

**DIRECTIVE N° 01/FIU/2018 OF 16/02/2018 OF THE FINANCIAL
INVESTIGATION UNIT RELATING TO ANTI-MONEY LAUNDERING
AND COMBATING THE FINANCING OF TERRORISM**

TABLE OF CONTENTS

ACRONYMS:.....	4
CHAPTER ONE: GENERAL PROVISIONS	5
Article One: Purpose of this Directive	5
Article 2: Definitions of terms.....	5
CHAPTER II: REQUIREMENTS FOR CUSTOMER IDENTIFICATION.....	7
SECTION ONE: KNOW YOUR CUSTOMER REQUIREMENTS (KYC)	7
Article 3: Category of customers.....	7
Article 4: Customer identification requirements.....	7
Article 5: The identity of natural person	7
Article 6: Identification of legal person or legal arrangements	7
Article 7: Identification of third party	8
Article 8: Non-face-to-face customer identification	8
Article 9: Identification of occasional customers	8
Article 10: Special monitoring of certain transactions.....	8
Article 11: Declaration of cash transactions.....	8
Article 12: Minimum requirements for account opening.....	8
SECTION 2: Customer Due Diligence Requirements.....	9
Article 13: Basic Customer Due Diligence (BCDD)	9
Article 14: Enhanced Customer Due Diligence (ECDD).....	9
Article 15: Simplified Customer Due Diligence (SCDD).....	10
Article 16: Due diligence related to a political leader.....	10
Article 17: Apply CDD Measures to potential customer	10
Article 18: Apply CDD requirement to existing customer.....	10
Article 19: Cross-Border Correspondent Financial Institution Services.....	11
Article 20: New technologies	12
Article 21: Reliance on intermediaries and third parties on CDD function	12
Article 22: Wire transfers	13
Article 23: Sanction for non-compliance with wire transfer requirement.....	14
Article 24: Risk assessment.....	14
CHAPTER III: AWARENESS AND SUSPICIOUS TRANSACTIONS REPORTING REQUIREMENTS	14
Article 25: Declaration of suspicious transactions.....	14
Article 26: Special attention to the customers from high risk countries	15
Article 27: Suspicious Transactions Report form.....	15
Article 28: Reporting Staff.....	15
Article 29: Independent audit function.....	15

Article 30: Suspicious transactions indicators and examples	16
Article 31 : Staff Training and Awareness Programmes.....	16
Article32: Monitoring of Foreign Branches, Subsidiaries and offices.....	16
Article33: Supervision of reporting entities	17
CHAPTER IV: RECORD KEEPING REQUIREMENTS	17
Article 34: Records keeping management.....	17
Article 35: Importance of record keeping	17
Article 36: Keeping records of information obtained through customer due diligence	17
Article 37: Period of record keeping.....	17
CHAPTER V: MISCELLANEOUS AND FINAL PROVISIONS.....	18
Article 38: Threshold for casinos and dealers in precious metals and precious stones.....	18
Article 39: Obligations for reporting entities	18
Article 40: Obligations for disciplinary or supervisory authorities of reporting entities	18
Article 41: Transitional provision.....	19
Article 42: Repealing provision.....	19
Article 43: Commencement.....	19
APPENDIXES	20
APPENDIX 1: CASH TRANSACTION REPORT.....	20
APPENDIX 2: MINIMUM ACCOUNT OPENING REQUIREMENTS	21
APPENDIX 3: SUSPICIOUS TRANSACTION REPORTING FORMAT	23
APPENDIX 4: INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS	26

ACRONYMS:

AML/CFT	: Anti-Money Laundering and Combating the Financing of Terrorism
BCDD	: Basic Customer Due Diligence
CDD	: Customer Due Diligence
ECDD	: Enhanced Customer Due Diligence
FATF	: Financial Action Task Force
FIU	: Financial Investigation Unit
KYC	: Know Your Customer
ML	: Money Laundering
MOU	: Memorandum of Understanding
NGOs	: Non- Governmental Organizations
RDB	: Rwanda Development Board
SCDD	: Simplified Customer Due Diligence
STR	: Suspicious Transaction Report
TIN	:Tax Identification Number
UBO	: Ultimate Beneficial Owner

DIRECTIVE N° 01/FIU/2018 OF 16/02/2018 OF THE FINANCIAL INVESTIGATION UNIT RELATING TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM.

Pursuant to Organic Law N° 01/2012/OL of 02/05/2012 instituting the penal code, especially in Articles 652, 653, 654, 655, 657 and 658;

Pursuant to Law N° 47/2008 of 09/09/2008 on prevention and penalizing the crime of Money Laundering and Financing Terrorism, especially in Articles 3, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 28 and 42;

Pursuant to the Presidential Order N° 27/01 of 30/05/2011 determining the organization, function and mission of the Financial Investigation Unit as amended to date, especially in Article 12;

Having reviewed the Directive N° 001/FIU/2015 of 30/12/2015 of the financial investigation unit relating to identification of customers, suspicious transactions reporting and record keeping requirements for reporting entities;

After consideration and approval by the Advisory Board of the Financial Investigation Unit in its session of 13/02/2018;

The Financial Investigation Unit hereafter shortened and referred to as the “FIU” decrees:

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Directive

This Directive aims at establishing requirements for identification of customers, suspicious transaction reporting, record keeping as well as risk assessment that reporting entities shall comply with within the framework of preventing and combating the crime of money laundering and financing of terrorism.

Article 2: Definitions of terms

1. **Beneficiary institution:** refers to the institution which receives the wire transfer from the ordering institution directly or through an intermediary institution and makes the fund available to the beneficiary;
2. **Correspondent financial institution service:** is the provision of financial services by one financial institution (the correspondent financial institution) to another financial institution (the respondent financial institution);
3. **Cross-border wire transfer:** refers to any wire transfer where the ordering reporting entity and beneficiary institutions are located in different countries. This term also refers to any chain of wire transfer in which at least one of the institutions involved is located in a different country;

4. **Customer:** individual, legal entity or legal arrangement that holds an account or has a business relationship with the reporting entity. In the case of a bank account, customer means natural person, legal entity or legal arrangement who:
 - a) opens a bank account or in the name of whom a bank account is opened;
 - b) has the power to sign on that account;
 - c) deposits, transfers or receives money by using that account;
 - d) is authorized to exercise transactions on that account.
5. **Domestic wire transfer:** refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in Rwanda. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of Rwanda, even though the system used to transfer the payment message may be located outside Rwanda;
6. **Legal arrangement:** refers to express trusts or other similar legal arrangements;
7. **Non-face to face:** identification of an individual when that individual is not present. The individual's information has to be consistent and/or corresponds with that is recorded;
8. **Occasional customer:** occurring or appearing of a customer at irregular or infrequent basis, who appears now and then;
9. **Originator:** the originator is the account holder, or where there is no account, the (natural or legal) person that places the order with the financial institution to perform the wire transfer;
10. **Political leader:** any person entrusted with prominent public functions in the Republic of Rwanda or in another country including that person's family members or other persons who are person's close associates or have business or financial relationship with him or her. In Rwandan context, a political leader is considered as any person who declares his/her assets to the Office of Ombudsman.
11. **Reporting entity:** natural or legal person set forth in law on prevention and penalizing the crime of Money Laundering and Financing Terrorism;
12. **Respondent bank:** refers to bank or reporting institution outside Rwanda to which correspondent banking services in Rwanda are provided;
13. **Suspicious transaction or activity:** transactions where there are reasonable grounds to suspect that the transaction or activity is related to money laundering or terrorism financing offences;
14. **Ultimate Beneficial Owner (UBO):** any person owning more than 25% of the capital of a company. It also refers to natural person(s) who ultimately owns or controls a customer and/ or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimately effective controls over a legal person;

- 15. Wire/fund transfer:** for the purposes of this Directive, wire transfer and funds transfer refer to any transaction carried out on behalf of an originator person through a licensee by electronic means for availability to a beneficiary person at another financial institution. The originator and beneficiary may be the same person;

CHAPTER II: REQUIREMENTS FOR CUSTOMER IDENTIFICATION

SECTION ONE: KNOW YOUR CUSTOMER REQUIREMENTS (KYC)

Article 3: Category of customers

Reporting entities shall classify their customers as follows:

- 1) Resident and non-resident;
- 2) Companies (sole proprietorship, partnership and corporate);
- 3) Cooperatives;
- 4) Non-Governmental Organisation (Local and Foreign);
- 5) Public institutions;
- 6) Public enterprises;
- 7) Clubs;
- 8) Other customers that may be determined.

Article 4: Customer identification requirements

The reporting entities shall identify their customers in the following cases:

- 1) Prior to establishing business relationship;
- 2) When they execute occasional transactions exceeding the threshold set under article 9 of this Directive;
- 3) When they receive a wire transfer that does not contain full information about the originator;
- 4) When they have suspicion of money laundering or terrorism financing;
- 5) When they have doubts about the veracity or adequacy of previously obtained customer identification data.

Article 5: The identity of natural person

The identity of natural person shall be verified by the presentation of valid official identification document with the bearer's photograph.

Article 6: Identification of legal person or legal arrangements

Legal person or legal arrangement shall be identified with any valid document, in particular their registration certificate. Reporting entities shall take any reasonable measure to verify the identity of their customers identified as a legal persons or legal arrangements.

Article 7: Identification of third party

Any person known to act on behalf of a customer shall present evidence of authority to act on his/her behalf, as well as his/her official identification document in conformity with the Article 5 of this Directive.

Article 8: Non-face-to-face customer identification

The customer identification procedures for non-face-to-face verification must be as severe as those for face-to-face verification. Reasonable steps must also be taken to avoid fraud by single or multiple false applications.

Article 9: Identification of occasional customers

Occasional customers shall be identified as described in Law on prevention and penalizing the crime of Money Laundering and Financing Terrorism for the case of transactions involving an amount exceeding Ten Million (10,000,000) Rwandan Francs or its equivalent in foreign currency.

This identification shall also be requested for any transaction amount of which is less than this threshold if it comprises a part of or the whole of transactions which are or seem to be linked and the total of which exceeds the threshold.

Article 10: Special monitoring of certain transactions

Reporting entities are required to pay special attention to all complexes, unusual patterns of transactions, especially large transactions, which have no apparent economic or visible lawful purpose. They shall examine the background and purpose of such transaction, establish the findings in writing, and transmit the report to the Financial Investigation Unit.

Article 11: Declaration of cash transactions

Reporting entities shall report to the FIU using the format set out in Appendix (1) of this Directive, all cash transactions equal to or exceeding fifty million Rwandan francs (FRW 50,000,000) or its equivalent in foreign currency, except where the sender and the recipient are banks or other financial institutions.

Reporting entities shall indicate to the FIU all transactions equivalent to the amount less than the threshold indicated in paragraph 1 of this Article, if they are part of a whole of transactions which are or seem to be linked and the total of which would exceed the threshold.

Article 12: Minimum requirements for account opening

Reporting entities shall, where applicable, put in place requirements for opening account. The list of minimum requirements for account opening is set out in Appendix (2) of this Directive.

SECTION 2: Customer Due Diligence Requirements

Article 13: Basic Customer Due Diligence (BCDD)

Reporting entities shall apply basic CDD measures before a business relationship is entered into. The basic CDD measures entail:

- 1) identifying the customer and verifying the customer's identity using reliable, independent source documents, data, or information;
- 2) identifying the ultimate beneficial owner (UBO) and taking reasonable measures to verify the identity of the UBO such that the reporting entity is satisfied that it knows who the UBOs are;
- 3) identifying any third parties on whose behalf the customer is acting;
- 4) determining the purpose and intended nature of the business relationship;
- 5) keeping the CDD information up-to-date and monitoring the business relationship and transactions undertaken throughout the course of the relationship to assure that they are consistent with the institution's knowledge of the customer and the UBO.

Reporting entities shall refuse to open an account, establish a business relationship or conduct the transaction, and consider making a STR when they are unable to comply with the CDD requirements.

Article 14: Enhanced Customer Due Diligence (ECDD)

Reporting entities shall perform Enhanced Customer Due Diligence (ECDD) if and when a business relationship or a transaction by its nature entails a higher risk of Money Laundering or Financing of Terrorism. EDD shall be performed prior to the business relationship or the transaction as well as throughout the course of the business relationship. Enhanced Customer Due Diligence (EDD) measures shall be undertaken when:

- 1) establishing business relations;
- 2) carrying out occasional transactions by wire transfers;
- 3) there is a suspicion of money laundering or terrorist financing;
- 4) the reporting entity has doubts about the veracity or adequacy of previously obtained customer identification data;
- 5) the customer is not a resident/not established in the country;
- 6) the customer is not physically present for identification;
- 7) the customer is a legal person, trust, or comparable entity intended as a private assets holding;
- 8) the customer is a body corporate or comparable entity with shares in bearer form or nominee shareholders;
- 9) the customer is a natural person, legal person, trust, or comparable entity that originates in a country or jurisdiction that does not apply or insufficiently applies the internationally accepted AML/CFT standards;

- 10) the customer is a political leader or politically exposed person; and
- 11) entering into correspondent banking relations.

Article 15: Simplified Customer Due Diligence (SCDD)

Reporting entities shall apply simplified CDD measures to customers identified as low risk customers. These customers consist primarily of financial and non-financial institutions that fall under the scope of the law on prevention and penalizing the crime of money laundering and combating terrorist where the following one or many of the following criteria is met:

- 1) a regulated institution supervised by the National Bank of Rwanda;
- 2) a foreign financial institution that is subject to international AML/CFT standards;
- 3) a public company that is subject to statutory disclosure requirements and whose shares are traded on an official stock exchange;
- 4) a public company wholly owned by the Government;
- 5) public legal persons;

Article 16: Due diligence related to a political leader

A reporting entity, in addition to performing normal due diligence measures to a political leader shall:

- 1) have appropriate risk management systems to determine whether the potential customer, existing customer or beneficial owner is a political leader;
- 2) obtain senior management approval for establishing for political leader, or continuing for existing customers, business relationships with such a customer;
- 3) take all reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as a political leader;
- 4) conduct appropriate monitoring of the business relationship with such a customer .

Article 17: Apply CDD measures to potential customer

Reporting entities shall not open an account, establish a business relationship or conduct the transaction with potential customers when a potential customer is unable to fulfill the requirement allowing the verification of his/her identity and shall immediately file a STR report.

Article 18: Apply CDD requirement to existing customer

Reporting entities are required to apply CDD requirements to existing customer on the basis of materiality and risk.

Reporting entities are required to conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

In assessing materiality and risk on the existing customer, reporting entities shall consider the following circumstances:

- 1) the nature and circumstances surrounding the transaction including the significance of the transaction;
- 2) any material change in the way the account, transaction or business relationship is operated; or insufficient information held on the customer or change in customer's information.

Reporting entities shall terminate the business relationship with existing customer when they have doubts about the veracity or adequacy of previously obtained customer identification data and when existing customers hold anonymous or accounts in fictitious names. Reporting entities shall immediately file a STR.

Article 19: Cross-Border Correspondent Financial Institution Services

Financial institutions that offer correspondent financial services to respondent financial institution are required to take the necessary measures to ensure that it is not exposed to the threat of money laundering and terrorism financing.

In relation to cross-border and correspondent financial institution services and other similar relationships, financial institution are required, in addition to performing the normal CDD procedures, take the following measures:

- 1) Gather sufficient information about a respondent institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the financial institution and the quality of supervision, including whether or not it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- 2) Assess the respondent financial institution's AML/CFT controls and ascertain that the latter are in compliance with FATF standards;
- 3) Obtain approval from senior management before establishing correspondent relationships;
- 4) Document the respective AML/CFT responsibilities of such financial institution.

In case a correspondent relationship involves the maintenance of payable through-accounts, the financial institution must be satisfied that:

- 1) its customer (the respondent bank or any other financial institution) has performed the normal CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution; and
- 2) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

Article 20: New technologies

Financial institutions shall have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes such as internationally accepted credit or debit cards and mobile telephone banking.

Financial institutions shall have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures shall be applied automatically when establishing customer relationships and conducting ongoing due diligence. Measures for managing the risks must include specific and effective CDD procedures that apply to non-face to face customers.

A financial institution that relies on a third party must immediately obtain the necessary information concerning property which has been laundered or which constitutes proceeds of, or means used to or intended for use in the commission of money laundering and financing of terrorist or any other unlawful act. Such financial institution must satisfy itself that copies of identification data and other relevant documentation relating the CDD requirements will be made available from the third party upon request without delay.

The Financial Institution must satisfy itself that the third party is a regulated and supervised institution and has measures in place to comply with requirements of CDD and reliance on intermediaries and other third parties on CDD as contained in this Directive.

Article 21: Reliance on intermediaries and third parties on CDD function

Financial institutions relying on intermediaries or other third parties which have no outsourcing or agency relationships, business relationships, accounts or transactions between financial institutions for their customers are required to perform some of the elements of the CDD process on the introduced business. The following criteria shall also be met:

- 1) Immediately obtain from the third party the necessary information concerning certain elements of the CDD process;
- 2) Take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
- 3) Satisfy themselves that the third party is regulated and supervised in accordance with AML/CFT and has measures in place to comply with the CDD requirements set out in the Directive; and
- 4) Make sure that adequate KYC provisions are applied to the third party in order to get account information for competent authorities.

The ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

Article 22: Wire transfers

Financial institutions conducting wire transfers of EUR/USD 1,000 or more shall obtain and maintain the following information relating to the originator of the wire transfer:

- 1) The name of the originator;
- 2) The originator's account number (or a unique reference number if no account number exists); and
- 3) The originator's address (the address can be substituted with a national identity number, customer identification number or date and place of residence or domicile).

For all wire transfers, the ordering financial institutions shall verify the identity of the originator in accordance with the CDD requirements contained in the Directive.

For cross-border wire transfers, the ordering financial institutions shall include the full originator information above in the message or the payment form accompanying the wire transfer.

If several individual cross-border wire transfers from a single originator are bundled in a batch-file for transmission to beneficiaries in another country, the ordering financial institution must only include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch-file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country.

For domestic wire transfers, the ordering financial institution shall either:

- 1) include the full originator information in the message or the payment form accompanying the wire transfer; or
- 2) include only the originator's account number or a unique identifier, within the message or payment form.

The second option must be permitted by the financial institution only if full originator information can be made available to the beneficiary financial institution and to the appropriate authorities within three (3) business days of receiving the request.

Each intermediary and beneficiary financial institution in the payment chain shall ensure that all originator information that accompanies a wire transfer is transmitted with the transfer.

Where technical limitations prevent the full originator information accompanying a cross-border wire transfer (during the necessary time to adapt payment systems), a record must be kept for six (6) years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

Beneficiary financial institutions shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. The lack of complete originator information is considered as a factor in assessing whether a wire transfer or related transactions are suspicious. They are therefore required to be reported to the FIU.

The beneficiary financial institution shall restrict or even terminate its business relationship with the financial institutions that fail to meet the above standards.

Cross-border and domestic transfers between financial institutions are, however, not intended to cover the following types of payments:

- 1) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction, such as withdrawals from a bank account through an ATM machine, cash advances from a credit card or payments for goods and services. However, when credit or debit cards are used as a payment system to effect a money transfer the necessary information must be included in the message; and
- 2) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

Article 23: Sanction for non-compliance with wire transfer requirement

Financial institution that do not comply with wire transfer requirements, may be subject to sanction including the suspension or withdraw of its operating license.

Article 24: Risk assessment

Reporting entities shall take appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographic areas, products and services, transactions or delivery channels.

Reporting entities shall maintain documents related to assessments referred to under paragraph one of this article.

Reporting entities shall ensure these assessments are at all times updated, and have appropriate mechanisms to provide risk assessment information to competent authorities.

CHAPTER III: AWARENESS AND SUSPICIOUS TRANSACTIONS REPORTING REQUIREMENTS

Article 25: Declaration of suspicious transactions

Require all reporting entities must report all transactions, including attempted transactions, when they suspect or have reasonable grounds to suspect that the funds are the proceeds of a criminal activity, are related to money laundering or are related or linked to, or to be used for terrorism, individual terrorist acts or terrorist organizations or those who finance terrorism.

These reports are confidential and cannot be communicated to the owner or the author of the transaction.

Article 26: Special attention to the customers from high risk countries

Financial institutions must conduct enhanced CDD for business relationship and transaction with any person from countries identified and listed by the FATF as not efficiently complying the FATF recommendations or having on going or substantial ML/TF risk.

Financial institutions must apply the following countermeasures for customer from countries identified and listed by the FATF as not efficiently complying the FATF recommendations or having on going or substantial ML/TF risk:

1. limit business relationship or financial transactions with identified countries or persons located in the country concerned;
2. review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;
3. conduct any other measures as specified by FIU.

Article 27: Suspicious Transactions Report form

Persons subject to the requirement to declare the suspicious transactions shall submit to the FIU the Suspicious Transactions Report (STR) in the format prescribed in Appendix (3) of this Directive.

The Suspicious Transactions Report (STR) shall be submitted to FIU in both hard and soft copies or in any other channel determined by the FIU.

Article 28: Reporting Staff

All reporting entities are required to appoint staff at managerial level in charge of handling Anti Money Laundering and Counter Financing Terrorism issues and to ensure compliance with the AML/CFT requirements.

The reporting staff must have the unlimited right to timely access to customer information, data, and CDD information, transaction records and other relevant information.

Article 29: Independent audit function

All reporting entities are required to have an adequately resourced and independent audit function to check and test the compliance with, and the effectiveness of the AML/CFT policies, procedures, and controls; and to assess whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.

The scope of independent audit shall include, at a minimum:

- 1) compliance with AML/CFT Law, its subsidiary legislation and instruments issued under the AML/CFT Law;

- 2) compliance with the reporting entity's internal AML/CFT policies and procedures;
- 3) Adequacy and effectiveness of the AML/CFT compliance programme; and
- 4) Reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

Reporting entities are required to ensure that independent audits are carried out at the institution level at least on an annual basis.

Article 30: Suspicious transactions indicators and examples

Indicators and examples of suspicious transactions provided in Appendix (4) of this Directive shall serve as guidance in identifying suspicious transactions.

Article 31: Staff Training and Awareness Programmes

Reporting entities are required to conduct awareness and training programmes on AML/CFT practices and measures for their staff. Such training must be conducted regularly and supplemented with refresher course. The training must include, in particular, information on current ML and TF techniques, methods and trends, all aspects of the AML/CFT law and obligations, and the requirements concerning CDD and suspicious transaction reporting.

The training conducted for staff must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting entities.

The reporting entities must make available its AML/CFT policies and procedures for all staff.

Article 32: Monitoring of Foreign Branches, Subsidiaries and offices

Reporting entities are required to closely monitor the reporting entities' foreign branches, subsidiaries and offices operating in jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF.

Reporting entities are required to ensure that their foreign branches, subsidiaries and offices apply AML/CFT measures consistent with the home country requirements. Where the minimum AML/CFT requirements of the host country are less stringent than those of the home country, the reporting entities must apply the home country requirements, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the FIU requirement the reporting entities are required to apply appropriate additional measures to manage the ML/TF risks, and report to FIU and their supervisor on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

Article 33: Supervision of reporting entities

The AML/CFT supervision shall be exercised by the authorities in charge of supervising reporting entities. Reporting entities which do not have supervisory authority shall be supervised by FIU.

Supervisory authorities shall develop and implement a formal AML/CFT supervisory framework, including setting the necessary activities for offsite surveillance and examination procedures for onsite visits for the reporting entities under their supervision.

The supervisory authorities shall impose administrative sanctions for the legal entities or persons they supervise who fail to comply with AML/CFT requirements. Sanctions may be applied not only to the legal persons, but also to their directors and senior management.

CHAPTER IV: RECORD KEEPING REQUIREMENTS

Article 34: Records keeping management

Reporting entities shall have in place an efficient record keeping framework that includes policies and procedures.

Records of a reporting entity shall be complete and reliable and be kept in a paper format or electronically.

Article 35: Importance of record keeping

Records shall be kept to permit reconstruction of individual transactions background (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for any analysis or investigation by competent authorities.

Article 36: Keeping records of information obtained through customer due diligence

Reporting entities shall keep all records obtained through CDD measures notably:

- 1) copies or records of official identification documents such as passports, identity cards, driving licenses or similar documents, certificate of incorporation;
- 2) account files and business correspondence
- 3) results of any analysis undertaken for a complex, unusual and large transaction;
- 4) Any other information that may help to trace the customer.

Article 37: Period of record keeping

Reporting entities shall keep records on the identification data obtained through or presented during the customer due diligence process within a period of at least ten (10) years after the end of the business relationship.

In the case of an occasional customer, the ten (10) year period specified in paragraph one of this Article shall start from the conclusion of the transaction.

Reporting entities shall maintain, for a period of at least ten (10) years counted from the conclusion of the transaction, all necessary records on transactions at the national or international level.

Persons required to exercise due diligence shall maintain account books and business correspondence for a period of at least ten (10) years after the end of the business relationship.

CHAPTER V: MISCELLANEOUS AND FINAL PROVISIONS

Article 38: Threshold for casinos and dealers in precious metals and precious stones

Casinos and dealers in precious metals and precious stones shall identify and verify the identity of customers.

Casinos shall report to the FIU using the cash transaction report format (Appendix 1) when their customers are engaged in cash transaction equal to or above three million Rwanda Francs (FRW 3,000,000) or its equivalent in foreign currency.

Dealers in precious metals and precious stones shall report to the FIU using the cash transaction report format (Appendix 1) when their customers are engaged in cash transactions equal to or above fifteen million Rwandan francs (FRW 15,000,000) or its equivalent in foreign currency.

Article 39: Obligations for reporting entities

Reporting entities shall develop policies and procedures and put in place mechanisms for efficient implementation of this Directive and the Law on prevention and penalizing the crime of money laundering and financing terrorism.

Article 40: Obligations for disciplinary or supervisory authorities of reporting entities

The disciplinary or supervisory authorities of reporting entities shall at all-time ensure that reporting entities under their supervision are compliant with the provisions of this Directive and the Law on prevention and penalizing the crime of money laundering and financing terrorism. The disciplinary or supervisory authorities of reporting entities impose to them disciplinary or administrative sanction for non-compliance as provided for in the Law on prevention and penalizing the crime of money laundering and financing terrorism.

For this purpose of meeting the requirements established under paragraph one of this Article, supervisory and disciplinary authorities must issue appropriate guidance to reporting entities under their supervision.

Article 41: Transitional provision

Unless specified otherwise in this Directive the guidelines, policies and procedures of reporting entities or any formal AML/CFT supervisory framework not contrary to this Directive shall continue to apply until their replacement or abrogation.

Article 42: Repealing provision

The Directive N° 001/FIU/2015 OF 30/12/2015 of the financial investigation unit relating to identification of customers, suspicious transactions reporting and record keeping requirements for reporting entities and any prior provision contrary to this "Directive" are hereby repealed.

Article 43: Commencement

This Directive shall come into force on the day of its signature

Done at Kigali, on 16/02/2018


RWANGOMBWA John
Governor of the National Bank of Rwanda and
Chairperson of the FIU Advisory Board



APPENDIXES

APPENDIX 1: CASH TRANSACTION REPORT

Name of the reporting entity							
Address & contact of Head Office							
a) Physical.....							
b) Postal.....							
.....							
c) Telephone.....							
.....							
d) E-mail.....							
.....							
e) Fax.....							
.....							
Item	Date of transaction	Full Name of person conducting transaction	Customer or Account Name	Passport/ID/ Certificate of Incorporation & Nationality	Description of the transaction	Currency	Amount

Information about the Reporting Officer	
Name.....	
Signature.....	Date.....
.....	

APPENDIX 2: MINIMUM ACCOUNT OPENING REQUIREMENTS

TYPE OF ACCOUNT	MINIMUM REQUIREMENTS	
	<u>RESIDENT</u>	<u>NON- RESIDENT</u>
1. Personal	1. Original and copy of ID/Passport/ National Driving license. 2. Quality Colored Passport size photo 3. Fill account opening application form 4. TIN number or certificate of incorporation (if applicable) 5. Not blacklisted 6. Electricity or Water Bill (where applicable) 7. Acceptance of terms and conditions	1. Original and copy of the passport/laissez -passer/ID where applicable 2. Quality Colored Passport size photo; 3. Fill account opening application form 4. Letter or contract from employer confirming employment, address and employment visa (if applicable) 5. Copy of TIN number or certificate of incorporation (if applicable); 6. Not blacklisted; 7. Acceptance of terms and conditions.
2. Sole Proprietorship	1. Original and copy of business license, Certificate of incorporation or business permit; 2. Tax identification number; 3. Full identification of signatories as individual (see n°1 above) 4. Reference letter (if applicable) 5. Electricity or Water Bill (where applicable) 6. Acceptance of terms and conditions	
3. Partnership	1. Certificate of incorporation; 2. Partnership deed stamped by RDB; 3. Board resolution clearly indicating the signatories to the account; 4. Fill account opening application form 5. Full identification of signatories as individuals (see n°1 above)	

4. Corporate	1. Memorandum or articles of association; 2. Certificate of incorporation; 3. Board resolution to open an account; 4. Fill account opening application form; 5. Full identification of signatories as individual (see n°1 above) 6. Reference letter (if applicable); 7. Electricity or Water Bill (where applicable) 8. Acceptance of terms and conditions.
5. Regulated Credit and financial institutions	1. Operating license; 2. Certificate of incorporation; 3. Articles of Association; 4. Board Resolution to open an account; 5. Fill account opening application form; 6. Full identification of signatories as individual (see n°1 above); 7. Full identification of two principle directors as individual (see n°1 above); 8. Electricity or Water Bill (where applicable); 9. Acceptance of terms and conditions; 10. Electricity or Water Bill (where applicable)
6. NGOs	1. Certificate of registration ; 2. Board resolution to open an account; 3. NGO Charter for foreign NGOs; 4. Full identification of signatories as individual (see n°1 above) 5. Full identification of two principle directors as individual (see n°1 above); 6. Electricity or Water Bill (where applicable) 7. Acceptance of terms and conditions.
7. Government organs	1. Council resolution by the governing body; 2. Ministerial order for public institutions (if applicable); 3. Appointment letter for signatories in case it is not mentioned in the letter of appointment by the governing body or council; 4. Full identification of signatories as individual (see n°1 above); 5. Electricity or Water Bill (where applicable)

8. Cooperatives , union and federation	1. Articles of association; 2. Board resolution to open an account; 3. Registration from Rwanda Cooperative Agency; 4. Temporary authorization from District-only when registration certificate is not yet out; 5. Full identification of signatories as individual (see n°1 above); 6. Electricity or Water Bill (where applicable) 7. Acceptance of terms and conditions.
9. Friendly groups /Clubs /Mutual fund / Chorus groups/	1. MOU creating the club; 2. Appointment letter of the governing body to open an account; 3. A reference letter(if applicable) 4. Full identification of signatories as individual (see n° 1 above); 5. Acceptance of terms and conditions.

APPENDIX 3: SUSPICIOUS TRANSACTION REPORTING FORMAT

Submit to: **Director, Financial Investigation Unit**

(Always complete the entire report, attach additional pages if necessary to explain the situation in full)

1. Tick appropriate box	a) Initial Report ... ☐ b) Amended Report ☐ c) Supplemental Report ☐
Part I. Information on the Reporting Entity submitting the report:	
2. Name of reporting entity.....	
3. Address & contact of Head Office.....	
a) Physical.....	
b) Postal.....	
c) Tel.....	
d) Email.....	
e) Fax.....	
4. Address & Contact of branch(es) where activity/transaction occurred	
a) Physical.....	
b) Postal.....	

c) Tel..... d) Email..... e) Fax.....	
Part II: Information about Person(s) or Entity engaging in Suspicious Transactions/Activities	
5. a) Surname (or name of Entity)..... b) First Name..... c) Middle name..... 6. Postal & physical address in country of residence 7. Date of Birth/Incorporation (DD/MM/YY) 8. Passport/ID No..... 9. Occupational or Business..... 10. Identity verified by (where applicable)..... a) Passport.....b) ID card.....c) Other..... d) Incorporation No.....e) Date & Place issued..... 11. Relationship to the reporting entity (e.g Accountant, Agent, Broker, Customer /Customer, Depositor, Director, Employee, Service Provider, Officer, Shareholder etc. Other (Specify).....	12. (i) Is/are the person(s) still affiliated with the reporting entity? No (if no specify) ☐ Resigned ☐ Suspended ☐ Terminated (ii) Date of resignation, suspension, termination (DD/MM/YY)...../...../.....
Part III: Information about Suspicious Activity	
13. Date of transaction or suspicious activity(DD/MM/YY): 14. Transaction type..... 15. a) Account name, where applicable.....	

b) Account number affected, where applicable..... 16. Amount involved (in FRW or in other currency)..... 17. Source of funds..... 18. Information on the destination of the funds..... 19. Description of the transaction/activity..... 20. Basis of suspicion..... 21. Has the suspicious activity had a material impact on or otherwise adversely affected the financial soundness of the reporting institution? Yes ☐ No ☐ If yes, describe impact..... 22. Has any law enforcement authority been notified in any manner? If so, indicate the following: a) Authority..... b) How it was notified..... 23. Has any other action been taken by the reporting entity.....?
Part IV: Please detail or list available documents:
Part V: Information about the Money Laundering Reporting Officer 24. Name..... 25. Position/title in the reporting entities..... 26. Signature.....Date.....
Part VII: For internal use only (by the Financial Investigation Unit) Report Number..... Report Date..... Action taken.....

APPENDIX 4: INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS

The following acts are the examples of indicators to identify Suspicious Transaction more of the aforementioned elements; the relevant reporting entities can use the indicators of Suspicious Transactions indicators, which include, among other things:

A. Transactions

1) Cash

- i. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
- ii. Transactions conducted in a relatively small amount but with high frequency (structuring).
- iii. Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
- iv. The foreign currency exchange or purchase in a relatively large amount.
- v. The purchase of travelers checks in cash in a relatively large amount.
- vi. The purchase of several insurance products in cash in a short period time or at the same time with premium payment entirely in a large amount and followed by policy disbursement prior to due date.
- vii. The purchase of securities by cash, transfer, or checks under other person's name.

2) Economically irrational transactions

- i. Transactions having no conformity with the initial purpose of account opening.
- ii. Transactions having no relationship with the business of the relevant customer.
- iii. Transaction amount and frequency are different from that of normally conducted by the customer.

3) Fund transfers

- i. Fund transfers to and from high-risk countries or offshore financial centers without any clear business purposes.
- ii. Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
- iii. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period.
- iv. Fund payments for export import activities without complete documents.
- v. Fund transfers from or to other high-risk countries.
- vi. Fund transfers from or to other high-risk parties.
- vii. Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
- viii. Fund transfers using the account of a reporting entity employee in an unusual amount.

B. Behaviors of the Customer

- 1) Unreasonable behavior of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).
- 2) Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
- 3) Customer/prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo.
- 4) Customer/prospective customer is unwilling or refusing to provide information/documents requested by the officials of the relevant reporting entity without any clear reasons.
- 5) Customer or his/her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/her transaction as a Suspicious Transaction.
- 6) Customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant reporting entity request information with respect to his/her transaction.

Additional Indicators to financial institutions

The following indicators are for your consideration if you are an institution that opens accounts and holds deposits on behalf of individuals or entities.

A: Personal transactions

Customer appears to have accounts with several financial institutions in one geographical area;

1. Customer has no employment history but makes frequent large transactions or maintains a large account balance;
2. The flow of income through the account does not match what was expected based on stated occupation of the account holder or intended use of the account;
3. Customer makes one or more cash deposits to general account of foreign correspondent bank (i.e., pass-through account);
4. Customer makes frequent or large payments to online payment services;
5. Customer runs large positive credit card balances;
6. Customer uses cash advances from a credit card account to purchase money orders or to wire/electronically transfer funds to foreign destinations;
7. Customer takes cash advance to deposit into savings or cheque account;
8. Large cash payments for outstanding credit card balances;
9. Customer makes credit card overpayment and then requests a cash advance;
10. Customer visits the safety deposit box area immediately before making cash deposits;

11. Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address;
12. Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount;
13. Customer deposits large endorsed cheques in the name of a third-party.

B: Corporate and business transactions

On opening accounts with the various businesses, a financial institution would likely be aware of those that are mainly cash based. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity. Below are some of the examples:

1. Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of salaries, invoices, etc;
2. accounts have a large volume of deposits in bank drafts, cashier's cheques;
3. money orders or electronic funds transfers, which is inconsistent with the customer's business;
4. accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity (for example, deposits that include a mix of business, payroll, and social security cheques);
5. accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity;
6. business does not want to provide complete information regarding its activities;
7. Financial statements of the business differ noticeably from those of similar businesses;
8. representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them;
9. deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations;
10. customer maintains a number of trustee or customer accounts that are not consistent with that type of business or not in keeping with normal industry practices;
11. customer operates a retail business providing cheque-cashing services but does not make large withdrawals of cash against cheques deposited;
12. customer pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments;
13. customer purchases cashier's cheques and money orders with large amounts of cash;
14. customer deposits large amounts of currency wrapped in currency straps;
15. customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere;
16. Customer makes a large volume of cash deposits from a business that is not normally cash-intensive.

Specific indicators of suspicious transactions in casinos

The following indicators of a suspicious transaction are for your consideration if you are an institution working as the Casino:

1. If the customer does not give required particulars or gives false particulars or is not willing to give the particulars at the time of depositing amount, giving coupon or withdrawal of amount through money or check during settlement,
2. If no source of the money is mentioned or becomes unable to provide satisfactory source.
3. If the customer games/gambles excessively an amount above the threshold indicated in the Article 27 of this Directive.
4. If any customer requests the Casino to pay the huge amounts he wins to another person.
5. If individual or organization involved in terrorist activities or criminal activities or any other person who is or is likely to be directly or indirectly associated with criminal activities comes to the Casino as a customer.
6. If the transaction appears in any manner suspicious or the gaming/gambling is carried out or appears to be carried out with the purpose of money laundering or encouraging terrorist or criminal activities.
7. If the amount that seems to be earned by doing illegal acts.
8. If any customer tries to influence any Casino officials through economic or any other bribery so as not to report the particulars of threshold transaction to the Financial Investigation Unit or if any customer does any illegal act.
9. Any other suspicious transaction.