INSTRUCTION OF BCTL N. 05/2017 OF 25 AUGUST ON CUSTOMER IDENTIFICATION, RECORD-KEEPING AND TRANSACTION REPORT[1]

Banco Central de Timor-Leste has the duty to assure compliance, by the financial institutions, with the provisions of Law nº 17/2011 of 28 December, on the Legal Regime for the Prevention and Combatting Money Laundering and the Financing of Terrorism, as amended.

Taking into consideration that a Bank or the banking system may be exposed to reputational, operational, legal and other risks related with money laundering activities and that the involvement of banking institutions in money laundering or the financing of terrorism is likely to seriously undermine their reputation and undermine the public's confidence in them and in the banking system.

Furthermore, considering that the effective knowledge and understanding by Banks of their customers and the business that they conduct with or through the banking institution is essential in preventing the banking system from being used for money laundering or the financing of terrorism, hence reducing the risk of the banking system becoming a vehicle for/or a victim of financial crime and suffering consequential damage, and protecting the reputation and integrity of the banking system.

In view of the best international practices and in the interest of protecting the Timorese banking system, the depositors and the institutions, enhancing a sound and safe financial and banking sector.

The Governing Board of Banco Central de Timor-Leste, in accordance with Article 27 paragraph 2 subparagraph c) of Law nº 17/2011 of 28 December and Article 31 paragraph 1 of Law nº 5/2011 of 15 June, hereby resolves to approve the following Instruction:

CHAPTER I
GENERAL REQUIREMENTS

SECTION I
GENERAL PROVISIONS

Article 1
Definitions

In this Instruction the terms below shall have the following meaning:

a). "Administrator" means any person who is an officer of a Bank, or other juridical person, including any member of the Governing Board or the Audit Committee and the Compliance Officer and further including any person who alone or together with one or more others has the authority to enter into commitments for the account of such juridical person;

b). "AML/CFT" means anti-money laundering/combating the finance of terrorism;

---

[1] This English version of the Instruction is provided to facilitate banks and the public to understand the content. Interpretations should be referenced to the official version which the Portuguese version.

c). "AML/CFT Law" means Law nº. 17/2011 of 28 December on the Legal Regime for the Prevention and Combatting Money Laundering and the Financing of Terrorism, as amended;

d). "Bank" means entities established under UNTAET Regulation nº. 2000/8 on Bank Licensing and Supervision including Other Deposit Taking Institution established pursuant to Public Instruction 06/2010 of 29 December, and their agents;

e). "Beneficial owner" means the natural person[s] who ultimately owns or control a customer and/or the natural person on whose behalf a transaction is being conducted including those persons who exercise ultimate effective control over a legal person or arrangement;

f). "Compliance Officer" means an officer who is responsible for ensuring that the Bank complies with its obligations in accordance with the present Instruction and the applicable laws and regulations;

g). "Correspondent banking" means the provision of banking services by one bank to another bank (the respondent bank);

h). "FATF" means the Financial Action Task Force, the inter-governmental body established in 1989, to which the Asia/Pacific Group on Money Laundering of which Timor-Leste is a member, is an associate member;

i). "Financial Information Unit" or "FIU" means the institution established under Article 4 of Law nº. 17/2011 of 28 December as amended;

j). "Legal arrangements" means express trusts or other similar legal arrangements such as fiduciary, nominee, etc;

k). "Numbered accounts" means accounts in which the name of the beneficial owner is known to the Bank but is substituted by an account number or code name in some documentation;

l). "Occasional transaction" means a single transaction, or a series of transactions that are, or appear to be linked to each other, where,

   i. the Bank does not have a business relationship with the customer, and

   ii. the total amount of money paid or received by the customer in a single transaction or series of transactions is greater than US$ 10,000.

m). "Payable through accounts" means correspondent accounts that are used directly by third parties to transact business on their own behalf;

n). "Politically Exposed Person" or "PEP" means; the natural persons, resident both inside or outside of Timor-Leste, who are or have been entrusted within the previous year with prominent political or public functions, as well as their close family members and persons known to have close corporate or commercial relationships with them. For the purposes of this Instruction:

   i. "Prominent political or public functions":

      (1). Heads of State, heads of Government and Government members;

      (2). Members of Parliament;

      (3). Members of superior courts and other high-level judicial bodies, whose decisions are final and binding, unless in exceptional circumstances;

      (4). Members of board of directors and boards of auditors of central banks;

      (5). Heads of diplomatic missions and consulates;

      (6). High-ranking Military and Police officers;

(7). Members of board of directors and boards of auditors of public companies and corporations wholly owned or controlled by the State, public institutes, public foundations, public establishments under whatever legal form;

(8). Members of executive boards of international organizations;

ii. "close family members":

(1). The spouse or the unmarried partner;

(2). The parents and offspring, their spouses or unmarried partners;

(3). The siblings;

o). "Qualifying Wire Transfers" are all wire transfers except for those that flow from a transaction carried out by a credit or debit or prepaid card for the purchase of goods or services (not including person to person transfers) so long as the card number accompanies all transfers flowing from the transaction; and bank-to-bank transfers and settlements where the both parties are acting on their own behalf;

p). "Senior management" means the most senior persons in each Bank who are responsible for the management and administration of the Bank;

q). "Shell bank" means a bank that has no physical presence in a country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision;

r). "Unusual transaction" means a transaction that appears to lack economic or commercial sense, or that involves large sums of money, particularly large cash deposits not consistent with the expected activity in an account.

Article 2
Scope

1. This Instruction shall apply to all Banks including branches of foreign entities licensed to operate in Timor-Leste.
2. This Instruction shall also be applicable to the foreign majority owned subsidiaries and branches of a Bank to the extent that local applicable laws and regulation so permit.
3. Notwithstanding the provision of the previous paragraph, in the event that the local laws and regulations prohibit compliance with these obligations, the Bank shall so advise the Central Bank.

SECTION II
PROHIBITION AND RESTRICTION

Article 3
Prohibition and restriction

Banks are prohibited from:

a). Keeping anonymous accounts or accounts in obviously fictitious names;

b). Dealing with unknown customers and those who refuse to provide the details required to enable compliance with this Instruction;

c). Allowing numbered accounts;

d). Entering into or continuing correspondent banking relationships with shell banks.

SECTION III
INTERNAL PROGRAMMES

Article 4
Internal policies and procedures

1. Every Bank shall develop internal policies and procedures to ensure compliance with this Instruction.
2. The policies and procedures referred to in the previous paragraph shall include, but not limited to, the following:
   a). Customer identification and verification;
   b). Customer acceptance;
   c). On-going monitoring and control of high-risk accounts;
   d). Reporting of suspicious transactions;
   e). Record-keeping.
3. Banks shall incorporate into their internal policies and procedures reasonable measures to identify and assess the risk of customers, especially in identifying the type of customers associated with a high risk of money laundering or financing of terrorism.
4. In determining the risk profile of a particular customer or type of customer, the Bank shall at a minimum take into consideration the following factors:
   a). the origin of the customer and location of business;
   b). background or profile of the customer;
   c). nature of the customer's business; and
   d). structure of ownership for a corporate customer.
5. Banks are required to establish adequate screening procedures into their recruitment policy to ensure high standards when hiring employees.

Article 5
Compliance measures

1. Every Bank shall appoint a Compliance Officer at Senior Management level, approved by the Central Bank, who is able to carry out his/her responsibilities effectively and become the point of contact for the Central Bank and the Financial Information Unit with regards to AML/CFT matters.
2. Compliance Officers shall have direct access to Senior Management and shall have full access to all customers' information and data in order to ensure compliance with the provisions established in this Instruction and the applicable laws and regulations.
3. Banks shall obtain the Central Bank's approval on the appointment or change in the appointment of the Compliance Officer.
4. Banks shall ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented to ensure the following:
   a). the Bank's compliance with the requirements of this Instruction and other applicable laws and regulations;

b). implementation of the anti-money laundering and combating financing of terrorism policies and programme;

c). proper channels of communication are in place to effectively communicate to all levels of employees the AML/CFT policies and procedures;

d). all employees are aware of the Bank's AML/CFT measures, including policies, control mechanisms and the channels of reporting;

e). the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the Bank's operational changes, including the introduction of new technology and processes;

f). the AML/CFT mechanism is continuously assessed to ensure that it is effective and sufficient to address any change in money laundering and financing of terrorism trends.

Article 6
Annual compliance report

1. Every Bank shall prepare an annual report with regards to the implementation of this Instruction which shall include, but not be limited to, the following:

   a). A description of the bank's systems, control objectives, controls and procedures to implement the AML/CFT regime in compliance with the AML/CFT Law and Instructions, particularly addressing the objectives and requirements in Article 4;

   b). The name, role and responsibilities of the Compliance Officer;

   c). The role and responsibilities of Internal Audit in reviewing the systems and procedures, including HR, with a summary of the audit programs relating to AML/CFT planned and achieved during the year;

   d). A description of the AML/CFT training programs provided for staff during the year.

2. The report referred to in the previous paragraph shall include an assertion signed by the Chairman of the Board of Directors, or by the chief executive officer in case of a branch of a foreign bank, that:

   a). The description of the systems and procedures in the report presents the Bank's systems and procedures as designed and implemented throughout the year;

   b). The controls related to the control objectives stated in the description of the Bank's systems and procedures were suitably designed throughout the period;

   c). The controls related to the control objectives identified in the report operated effectively throughout the year;

   d). The other information in the report fairly describes the subject matter and operated effectively throughout the year.

3. Each Bank shall require its external or internal auditors to form an opinion whether the description of the system and other information in the report fairly represents the system as designed and implemented; that the controls are suitably designed to meet the objectives of the AML/CFT regime; and that the controls operated effectively during the year.

4. The auditor shall issue an opinion that:

   a). Conveys reasonable assurance about the matters in the management assertion;

   b). Includes a description of the tests of controls and the results thereof;

   c). Draws attention to material shortcomings or weaknesses;

d). Draws attention to any limitations in the scope of the audit.

5. The report together with the assertion and auditor's opinion shall be submitted to the Central Bank within four months after the end of each financial year.

Article 7
Training programme

1. Banks shall provide regular training programmes on AML/CFT practices and measures for its staff, in particular, those staff that are directly dealing with customers and officers in-charge of processing and accepting new customers as well as staff responsible for monitoring transactions.
2. Banks shall make their staff aware that they may be held personally liable for any failure to observe the AML/CFT requirements.
3. Banks are required to make an allocation in their annual operating expenses budget to support an ongoing AML/CFT staff training programme.

CHAPTER II
CUSTOMER DUE DILIGENCE

Article 8
General requirements

1. Banks, in conducting a customer due diligence process, shall at all times obtain a copy of the documents and data to evidence the customer due diligence process has taken place.
2. Banks shall take reasonable and appropriate measures to ensure that the records of existing customers, including customer profiles, remain up to date and relevant throughout the business relationship.
3. Banks shall draw the attention of the customer to the need to update the information in his/her other accounts, if any.
4. The Central Bank may, from time to time, determine the circumstances under which the obligations regarding the identification and verification of the identity of customers or the beneficial owners may be reduced or simplified.
5. Banks are required to identify and assess risks but shall apply a risk-based approach in managing the risks that have been identified.

Article 9
Customer identification

1. Banks shall identify their customers and beneficial owners and verify their identities by means of independent source documents, data or information when:
   a). establishing business relationship with any customer;
   b). carrying out occasional transactions in an amount equal to or above US$10,000, whether conducted as a single transaction or several transactions that appear to be linked;
   c). doubts exist about the veracity or adequacy of previously obtained customer identification data;
   d). there is a suspicion of money laundering or financing of terrorism.

2. The due diligence process required in the previous paragraph shall include the identification and verification of the effective beneficial owner(s), those with a controlling interest, and the natural persons who manage a legal person or other natural person.
3. Banks shall identify and verify the identity of their clients, by the following means:
   a). Identification of individuals and verification of their identity shall include the full name and national identification number;
   b). Identification of legal persons shall include verifying information concerning the corporate name, head office address, identities of directors, proof of incorporation or similar evidence of their legal status, legal form of organization of the legal person, and the form and powers of those who manage the legal person;
   c). Identification of relevant legal arrangements, including persons associated with the arrangements.
4. Banks shall collect information regarding the purpose and intended nature of the business relationship.
5. If there is doubt as to whether a customer specified in paragraph 1 above acts for his/her own account, Banks shall verify the identity of the person or persons on whose behalf the customer is acting and verify that he/she is authorized to do so.
6. Notwithstanding the requirements established in the previous paragraphs, Banks may verify the identity of a customer and any beneficial owner of the customer after establishing a business relationship with the customer if;
   a). this is necessary not to interrupt the normal conduct of business with regard to the customer; and
   b). any risk of money laundering or terrorist financing that may be caused by carrying out the verification after establishing the business relationship is effectively managed.
7. Banks that carry out verification after establishing a business relationship with a customer under the previous paragraph shall complete the verification as soon as reasonably practicable after establishing the business relationship but shall not exceed 3 business days.
8. If a bank is unable to comply with the requirements established in paragraphs 1 to 6 above, it:
   a). shall not open the account, commence a business relationship or carry out any occasional transaction with that customer; or
   b). if it has already established a business relationship with that customer, shall terminate the business relationship and consider making a suspicious transaction report.

Article 10
Minimum verification requirements

1. When Banks undertake the opening of deposit accounts, at least the following data should be collected in the respective forms for each of the account holders and their representatives, as well as any other person entitled to operate the account:
   a). In the case of a physical person:
      i). Full name and signature;
      ii). Date and place of birth;

iii). Nationality;

iv). Complete permanent address;

v). Occupation and employer, if any;

vi). Taxpayer number;

vii). Public office held, if any;

viii). Type, number, date and issuer of the identification document;

ix). Income;

x). Expected use of the account: amount, number, type, purpose and frequency of the transactions expected;

xi). E-mail address, landline and mobile telephone numbers.

b). In the case of a legal entity:

i). Corporate name;

ii). Corporate purpose;

iii). Address of the registered head office;

iv). Taxpayer number;

v). Company's registration number;

vi). Identity of the partners or shareholders who own or have voting rights in the legal person corresponding to at least 5% of the share capital;

vii). Identity of the legal person's management bodies;

viii). Identity of any persons exercising effective control of the legal person;

ix). Identity of the beneficial owners.

c). In case of accounts held by self-employed persons, the respective form for account opening must contain the tax identification number, name, registered head office or place of business and purpose, in addition to the information referred to in subparagraph a).

d). The requirements established in subparagraph b) points v. and vii. do not apply in case of entities listed on a recognised stock exchange.

2. The data referred to in the preceding paragraph shall be proved through the following means of verification:

a). For physical persons the data specified in points i) to iii) of subparagraph a) of the preceding paragraph shall be proved by:

i). For resident persons, through the presentation of two of the following documents: national identity card, voter registration card, passport, resident permit in the territory, in case of a foreign citizen;

ii). For non-resident persons, through the presentation of the passport and of the identity declaration duly certified by the Embassy or Consulate of its country of origin or residence or by a Timorese public authority.

b). The full address, occupation and employer may be evidenced by any document, mean or through any diligence considered suitable and sufficient to demonstrate the information provided;

c). With regard to legal entities:

i). The identification data referred to in points i) to iii) of subparagraph b) of paragraph 2 shall be demonstrated by an extract from the commercial

registry; and, in the case of non-residents, through a duly certified equivalent document;

ii). The identification data referred to in points iv) and v) of subparagraph b) of paragraph 2 can be proved by the presentation of a certificate from the tax authorities, certificate of commercial registry or similar document, and, in the case of non-residents, through a duly certified equivalent document;

iii). The identification data contained in points vi) and vii) of subparagraph b) of paragraph 2 can be demonstrated by simple written statement issued by the legal entity itself, containing the name or corporate name of the holders, signed, in the case of Public Limited Liability Companies, be signed by the Company's Secretary.

d). When a physical or a legal person is not resident in the national territory and has not proved all of the identification data required in paragraph 2 above, the Bank may request written confirmation of the veracity and timeliness of the information provided, to be issued by a credit institution where the person already holds a bank deposit account.

e). When the confirmation referred to in the preceding subparagraph takes place, the Bank shall notify the Central Bank of the details of the credit institution that provided the information and the Central Bank may, if it deems necessary, impose further requirements.

Article 11 Article 11

New technologies and non-face-to-face business relationship

1. Banks are required to have policies in place and take appropriate measures to manage and mitigate risks to prevent the misuse of technological developments in money laundering or terrorist financing schemes when:

   a). developing new products and new business practices, including new delivery mechanisms; and

   b). developing the use of new or developing technologies for both new and pre-existing products.

2. Banks that offer non-face-to-face business services shall pay special attention to the following when establishing and conducting business relationship:

   a). establishing appropriate measures for customer verification that shall be as effective as that for face-to-face customers;

   b). implementing a monitoring system and reporting mechanism to identify potential money laundering and financing of terrorism activities.

3. The measures that the Bank may use to verify non-face-to-face customers shall include, but not limited to:

   a). requisition of additional documents to complement those which are required for face-to-face customers;

   b). developing independent contact with the customer; or

   c). verification of customer information publicly available.

4. The Bank shall ensure the certification of copies obtained when dealing with non-face to face relationships.

Article 12

Enhanced due diligence

1. Banks shall conduct enhanced customer due diligence on customers who pose higher risk including, but not limited to, the following:
   a). High net worth individuals;
   b). Politically exposed persons;
   c). Complex legal arrangements;
   d). Non-resident customers;
   e). Intensive cash based businesses;
   f). Individuals and entities from locations known for their high rates of crime such as drug producing, trafficking, smuggling, etc;
   g). Businesses/activities identified by the FATF as of higher money laundering and financing of terrorism risk; and
   h). Countries or jurisdictions with inadequate AML/CFT laws and regulations as highlighted by the FATF.
2. Notwithstanding the requirements established in the previous paragraph, Banks may classify a customer or transaction as high risk, when:
   a). following the initial acceptance of the customer the Bank determines the pattern of account activity does not conform to the bank's understanding of the customer;
   b). the customer refuses, without good reason, to provide the information requested and to cooperate with a Bank's customer due diligence process;
   c). the Bank has cause to believe that the customer has been refused banking services by another Bank for reasons related to the implementation of money laundering and terrorist financing requirements.
3. Without prejudice to any requirement to adopt higher standards for certain transactions or for certain classes of persons, the due diligence process established in the previous paragraphs shall include, but not be limited to, the following:
   a). Obtaining more detailed information from the customer and the beneficial owner and through publicly available information take all reasonable and appropriate measures to establish the source of wealth or funds and the purpose of the transaction; and
   b). Obtaining approval from the Senior Management of the Bank before establishing or continuing the business relationship with the customer.
4. Banks shall conduct enhanced on-going due diligence on customers referred to in paragraph 1 above throughout their business relationships with such customers.
5. The Central Bank may from time to time review the type of customers referred to in the paragraph 1 above.

Article 13
Ongoing customer due diligence

1. Banks shall exercise ongoing due diligence with respect to the business relationship with customers and closely examine the transactions carried out in order to ensure that they are consistent with their knowledge of the customer, his/her commercial activities and risk profile and, where required, the source of his/her funds.
2. Banks shall operate a system to detect unusual transactions in all their customers' accounts and procedures to assess whether these unusual transactions give rise to suspicions that should be reported to the FIU.

3. Banks shall conduct regular reviews on existing records of customers, especially when:
   a). a significant transaction is about to take place;
   b). there is a material change in the way the account is operated;
   c). the customer's documentation standards change substantially; or
   d). it discovers that the information held on the customer is insufficient.
4. In circumstances other than those mentioned in the previous paragraph, a Bank, based on its risk assessment, may require additional information consistent with the Bank's current customer due diligence standards from those existing customers that are considered to be of higher risk.

CHAPTER III
CORRESPONDENT RELATIONSHIPS

Article 14
General requirements

1. Banks are prohibited from establishing or maintaining business relationships with banks or financial entities that are domiciled or are subsidiaries of entities based in a country or territory that does not have effective consolidated supervision.
2. Banks are prohibited from establishing or maintaining commercial relationships with respondent financial institutions in a foreign country if they permit their accounts to be used by shell banks.
3. Banks are required to obtain approval of Senior Management before establishing a new correspondent banking relationship.

Article 15
Correspondent banking

Banks shall take the following measures before establishing a cross-border correspondent banking relationship:

a). assess the suitability of the respondent bank by taking the following steps:
   i). gather adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including the following, where applicable;
      (1). Know your customer policy;
      (2). Information about the respondent bank's management and ownership;
      (3). Major business activities;
      (4). Its geographical presence or jurisdiction country of correspondence.
   ii). based on publicly available information, evaluate the respondent institution's reputation and the nature of supervision to which it is subject;
   iii). assess the respondent bank's AML/CFT systems and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates; and
   iv). in the case of a payable-through account, the Bank shall ensure that the respondent institution:
      (1). has verified the customer's identity;

(2). has implemented mechanisms for ongoing monitoring with respect to its clients; and

(3). is capable of providing relevant identifying information on request.

b). clearly understand and document the respective AML/CFT responsibilities of each bank.

CHAPTER IV
WIRE TRANSFERS

Article 16
Obligations of Banks

1. Banks shall not execute, intermediate, or receive a wire transfer unless the wire transfer complies with the provisions of this Instruction.
2. Ordering Banks shall include required and accurate originator information, and required beneficiary information, on all wire transfers and related messages.
3. Intermediary Banks in the payment chain for processing wire transfers shall ensure that:
   a). all originator and beneficiary information remains with the wire transfer or related message throughout its processing;
   b). effective risk-based policies and procedures are in place for determining (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required beneficiary information; and (ii) the appropriate follow-up action.
4. Beneficiary Banks shall:
   a). take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information;
   b). verify the identity of the beneficiary, if the identity has not been previously identified;
   c). maintain records concerning the identity of the beneficiary;
   d). have effective risk-based policies and procedures for determining (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required beneficiary information; and (ii) the appropriate follow-up action.
5. In the processing of wire transfers, Banks are required to take freezing action and shall prohibit conducting transactions with designated persons and entities, as per the obligations set out in Article 36 of the AML/CFT Law, relating to the prevention and suppression of terrorism and terrorist financing.

Article 17
Requirements for Wire Transfers

1. All Qualifying Wire Transfers shall always contain the following:
   a). the name of the originator;
   b). the originator account number, where such an account is used to process the transaction;
   c). the originator's address, or national identity number, or customer identification number, or date and place of birth;

d). the name of the beneficiary; and

e). the beneficiary account number where such an account is used to process the transaction.

2. Cross border wire transfers below [$1,000] shall apply simplified customer due diligence measures unless there is a suspicion of money laundering or terrorist financing.

3. No Wire Transfer may be originated for a customer unless proper due diligence process has been completed in accordance with this Instruction.

4. In the absence of an account, a unique transaction reference number shall be included which permits traceability of the transaction.

5. The requirement established in paragraph 1 above in respect of originator information may be waived where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, provided that the originator's account number or unique transaction reference number is included as described in paragraph 3 above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

CHAPTER V
RECORD KEEPING

Article 18
Record-keeping

1. Banks shall maintain records, in an appropriate record keeping system, that are readily available to the Central Bank and other competent authorities determined by law, containing the following information:

   a). copies of documents evidencing the identities of customers, beneficial owners or agents, customer due diligence, account files, business correspondence and documents relating to transactions for at least ten 10 years after the transaction has been completed or the business relationship with the customer has ended;

   b). copies of all reports sent to the FIU for the period at least five years after transmission to the FIU;

   c). copies of all reports and data provided to foreign FIUs and/or entities; and

   d). copies of the feedback provided by the FIU regarding the reports on suspicious transactions submitted for five years after the receipt of such feedback.

2. Notwithstanding the requirements established in the previous paragraph, records that are subject to on-going investigations or prosecution in court shall be retained beyond the stipulated retention period until such records are no longer needed.

3. Banks shall ensure that the retained documents and records are able to create an audit trail of individual transactions that are traceable by Central Bank, the FIU and law enforcement agencies as determined by law.

CHAPTER VI
REPORTING OF TRANSACTIONS

Article 19
Suspicious transaction reporting

1. Banks shall immediately submit a suspicious transaction report to the Financial Information Unit, using the form in Annex 1 of this Instruction signed by the Compliance Officer, where there is reason to suspect that a transaction may involve proceeds from an unlawful activity or the customer is involved in money laundering or the financing of terrorism.
2. Banks shall also consider making a suspicious transaction report to the FIU when unable to complete a transaction or attempted transactions, or customer due diligence, regardless of whether the relationship has commenced or not.
3. Banks shall give full cooperation to the FIU in providing such additional information and documentation as it may request and to respond promptly to any further enquiries with regards to any suspicious transaction report.
4. Banks shall establish a reporting system for the submission of suspicious transaction reports to the Financial Information Unit including a mechanism for submitting reports from its branches.
5. Bank shall ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.
6. Banks shall undertake reasonable measures to ensure that all their employees involved in conducting or facilitating customer transactions are aware of the reporting procedures required in this Article.
7. In submitting a suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality and no person shall disclose the fact that a suspicious transaction report or related information has been or is being filed to the FIU and/or the Central Bank.
8. Banks shall immediately submit a suspicious transaction report to the FIU when it suspects or has reason to suspect that a transaction or series of transactions is being conducted in a manner to avoid the cash transaction reporting requirements of this Instruction, under Article 20.

Article 20
Cash transaction report

1. Banks shall report to the FIU, in a format to be determined by the Central Bank, any cash transaction in an amount equal to or above US$ 10,000, whether conducted as a single transaction or several transactions that appear to be linked.
2. Cash transactions shall include but not limited to checks, traveler's cheques, money/postal orders, bank drafts or other monetary instruments in any currencies.
3. Banks shall ensure that they have systems in place in order to comply with the requirements established in this Article.
4. Notwithstanding the requirements established in the previous paragraphs, Banks are not required to report the following transactions:
   a). Transactions on behalf of Banks;
   b). Transactions with the Central Bank.

Article 21
Other reports

1. Banks shall report to the Central Bank the names of customers whose applications for opening an account with the Bank have been refused.

2. Banks shall immediately report to the Central Bank any law enforcement inquiry relevant to money laundering or terrorist financing being conducted in the Bank or a company under its control.
3. Banks shall immediately report to the Central Bank any transaction declined by the Bank pursuant to this Instruction.

CHAPTER VII
TRANSITIONAL AND FINAL PROVISIONS

SECTION I
TRANSITIONAL PROVISION

Article 22
Transitional provisions

2. The implementation of the requirements established in CHAPTER VIArticle 20 of this Instruction shall be effective from 1 January 2018.

SECTION II
FINAL PROVISIONS

Article 23
Final provisions

Banks which at the time the present Instruction enters into force allow confidential numbered accounts or anonymous accounts to exist in their bank shall, within 30 calendar days, cease the operation of those accounts.

Article 24
Repeal

The following are repealed and superseded by this Instruction:

a). Public Instruction no. 02/2004 on the Prevention of Money Laundering, Customer Identification and Record-Keeping;

b). Chapter VI of Public Instruction no. 06/2010 on the Licensing and Supervision of Other Deposit Taking Institutions (ODTIs);

c). Section 1, Section 2 number 1 paragraph f) and Section 2 number 2 paragraph e) of Instruction no. 03/2003 on the Opening and Maintenance of Deposit Accounts.

Article 25
Compliance measures

1. Banks, any of their administrators, and their staff, shall be subject to the administrative sanctions established in Articles 31 and 32 of the AML/CFT Law if the Central Bank determines that the provisions of this Instruction have been violated.
2. The administrative sanctions set out in the previous paragraph shall not restrict the general powers of the Central Bank to issue written warnings, suspend or dismiss

administrators, revoke the license of a Bank, or exercise any other powers conferred by legislation.

Article 26
Entry into force and Publication

1. This Instruction shall enter into force from the date of its publication.
2. In accordance with Article 66 paragraph 1 of the Organic Law of the Central Bank, this Instruction shall be published in the Official Gazette.

Adopted in 28th of March 2017

Governor,

Abraão de Vasconselos

REPORTING ENTITY REFERENCE NUMBER	

SUSPICIOUS TRANSACTION REPORT

The obligation to file a Suspicious Transaction Report is required under article 23 of Law 17/2011 dated 28 December, amended by Law no. 5/2013/III of 14 August, on the Legal Regime to Prevent and Combat Money Laundering and the Financing of Terrorism.

Please send the completed form to the following address:

UNIDADE DE INFORMAÇÃO FINANCEIRA

Att. Executive Director
Banco Central de Timor-Leste
Avenida Xavier do Amaral No. 9
Dili, Timor-Leste

The completed Form can be sent also to UIF Fax: **+670 3311172**

Fields marked with an asterisk (*) are mandatory and must be completed by Reporting Officer prior to submission of the STR to UIF. The ones that are also marked "if applicable" must be completed if they are applicable to you or the transaction being reported. For all other fields, you have to make reasonable efforts to obtain relevant information.

PART A: INFORMATION ON CUSTOMER

a) Account holder

1. Name (*)				
2. ID No/Passport No/Business Reg. No. (*)	New			
	Old			
3. Gender (*)	☐ Male	☐ Female	4. Country *)	
			5. Nationality	
6. Business/Employment (*)			7. Occupation *)	
8. Other Occupation (*)				
9. Name of Employer (*)				
10. Address (*)				

c) Person conducting transaction

11. Name (*)				
12. ID No/Passport No/Business Reg. No. (*)	Old			
	New			
13. Gender (*)	☐ Male	☐ Female	14. Country (*)	
			15. Nationality (*)	
16. Other Occupation (*)				
17. Name of Employer (*)				
18. Address (*)				

PART B: TRANSACTION DETAILS

19. Customer Identification Number (*)		

20. Account Number (*)		21. Account Type (*)	
22. Date Account Opened (*)		23. Account Status (*)	
24. Balance (*)			
25. Branch (*)		26. Town	

a) Introducer/Guarantor

27. Name (*)			
28. Type of Identification (*)	Choose an item.	Please specify if others	
29. ID No/Passport No/Business Reg. No. (*)	New		
	Old		
30. Gender (*)	☐ Male ☐ Female	31. Country *)	
		32. Nationality (*)	

b) Transaction

33. Frequency (*)	☐ Single ☐ Multiple	34. Date of Transaction (*)	Click to enter a date.
35. Total Amount in (*) USD			
36. Amount of Foreign Currency Involved (*)		37. Type of Currency (*)	
38. Type of Transactions (*)	Choose an item.		
39. Purpose of Transaction			

PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION

40. Grounds for suspicion [Please mark (√) where relevant]

☐ Reactivated Dorman Account	☐ Regular / Unusual Offshore / Activity
☐ Large / Unusual Cash Deposit / Withdrawal	☑ Large / Unusual Inward / Outward Remittance
☐ Activity Inconsistent with Customer Profile	☐ Others. _____

(Please specify)

41. Give details of the nature and the circumstances surrounding it (*)

42. List of attachment (if any)	
43. Date of Reporting (*)	Click here to enter a date. *dd/mm/yyyy*

PART D: FOR THE UNIDADE DE INFORMAÇÃO FINANCEIRA USE ONLY

44. Receiving Officer		45. Date Received	Click to enter a date. *dd/mm/yyyy*

Attention: Article 25 of Law 17/2011, amended by Law no. 5/2013/III, strictly prohibits you to disclose or otherwise provide information you have submitted or is being submitted to the UIF and information regarding the investigation for the crime of money laundering and the financing of terrorism. It is a serious offence for the non-compliance with this obligation pursuant to the requirements established in Articles 31 and 32 of the said Law.

Sexta-Feira, 25 de Agosto de 2017 **Série II**, N.° 34A

JORNAL da REPÚBLICA

$. 0.75

PUBLICAÇÃO OFICIAL DA REPÚBLICA DEMOCRÁTICA DE TIMOR - LESTE

Número Extraordinário

SUMÁRIO

INSTRUÇÃO DO BCTL N.° 05/2017 RELATIVA À IDENTIFICAÇÃO DOS CLIENTES, À CONSERVAÇÃO DE DOCUMENTOS E À COMUNICAÇÃO DE OPERAÇÕES

Compete ao Banco Central de Timor-Leste assegurar o cumprimento, pelas instituições financeiras, das disposições da Lei n.° 17/2011, de 28 de dezembro, que aprova o Regime Jurídico da Prevenção e do Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, na sua atual redação.

Considerando que um Banco ou o sistema bancário podem ficar expostos a riscos de reputação, operacionais, legais e a outras formas de riscos decorrentes de atividades de branqueamento de capitais, e que o envolvimento de instituições bancárias em práticas de branqueamento de capitais ou financiamento do terrorismo pode afetar seriamente a sua reputação e prejudicar a confiança do público nessas instituições e no sistema bancário.

Considerando ainda que o efetivo conhecimento por parte dos Bancos acerca dos seus clientes e das atividades de negócios que os mesmos efetuam com ou através deinstituições bancárias é essencial para prevenir a utilização do sistema bancário para atividades de branqueamento de capitais ou financiamento do terrorismo, reduzindo assim o risco do sistema bancário ser utilizado como veículo ou como vítima de crimes financeiros com as resultantesconsequências negativas, e protegendo a reputação e a integridade do sistema bancário. No quadro das melhores práticas internacionais e com o intuito de proteger o sistema bancário de Timor-Leste, os depositantes e as instituições, no sentido de proporcionar um setor financeiro e bancário fiável e seguro.

O Conselho de Administração do Banco Central de Timor-Leste, de acordo com o artigo 27.°, n.° 2, alínea c) da Lei n.° 17/2011, de 28 de dezembro, e o artigo 31.°, n.° 1, da Lei n.° 5/2011, de 15 de junho, resolve aprovar a seguinte Instrução:

CAPÍTULO I
REQUISITOS GERAIS

SECÇÃO I
DISPOSIÇÕES GERAIS

Artigo 1.°
Definições

Para efeitos da presente Instrução, entende-se por:

a). "Administrador", qualquer dirigente de um Banco, ou de outra entidade jurídica, incluindo qualquer membro do Conselho de Administração ou do Conselho Fiscal e o Responsável pela Conformidade, incluindo ainda qualquer pessoa que individualmente ou em conjunto com uma ou mais pessoas possui poderes para assumir compromissos em nome da referida entidade jurídica;

b). "ABC/CFT", anti-branqueamento de capitais /combate ao financiamento do terrorismo;

c). "Lei ABC/CFT", a Lei n.° 17/2011, de 28 de dezembro, que aprova o Regime Jurídico da Prevenção e do Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, na sua atual redação;

d). "Banco", as entidades estabelecidas ao abrigo do Regulamento n.° 2000/8, da UNTAET, sobre o Licenciamento e Supervisão Bancária, incluindo Outras Instituições Recetoras de Depósitos estabelecidas ao abrigo da Instrução Pública n.° 06/2010 de 29 de dezembro, e os respetivos agentes;

e). "Beneficiário efetivo", a pessoa singular que é a proprietária última ou que detém o controlo final de um cliente e/ou a pessoa singular por conta da qual é efetuada uma operação. Inclui também as pessoas que controlam efetivamente uma

pessoa coletiva ou uma entidade sem personalidade jurídica;

f). "Responsável pela Conformidade (*Compliance Officer*)", o quadro responsável por assegurar que o Banco cumpre as suas obrigações no que diz respeito à observância da presente Instrução e das leis aplicáveis;

g). "Banca correspondente", a prestação de serviços bancários por um banco a outro banco (o "banco cliente");

h). "GAFI", o Grupo de Ação Financeira Internacional, um organismo intergovernamental criado em 1989, do qual o Grupo Ásia-Pacífico contra o Branqueamento de Capitais, que integra Timor-Leste, é membro associado;

i). "Unidade de Informação Financeira" ou "UIF", a instituição estabelecida ao abrigo do artigo 4.º da Lei n.º 17/2011, de 28 de dezembro, na sua atual redação;

j). "Entidades sem personalidade jurídica (*legal arrangements*)", fundos fiduciários explícitos (*express trusts*) ou outras entidades sem personalidade jurídica semelhantes como, por exemplo, fideicomisso, agente designado, etc;

k). "Contas numeradas", contas bancárias cujo nome do beneficiário é conhecido pelo banco, mas em que o mesmo nome é substituído por um número ou um código de conta bancária em alguma da documentação;

l). "Operação ocasional", uma operação única ou uma série de operações que estão, ou aparentam estar associadas entre si, sempre que:

i. o Banco não tenha uma relação de negócio com o cliente, e

ii. o montante total pago ou recebido pelo cliente numa operação única ou numa série de operações seja superior a US$ 10,000.

m). "Contas correspondentes de transferência (*payable through accounts*)", contas de correspondência utilizadas diretamente por terceiros para transacionar operações por conta própria;

n). "Pessoas politicamente expostas" ou "PPE", as pessoas singulares, residentes em Timor-Leste ou no estrangeiro, que desempenham, ou desempenharam no último ano, altos cargos de natureza política ou pública, bem como os membros próximos da sua família e pessoas que reconhecidamente tenham com elas estreitas relações de natureza societária ou comercial. Para efeitos da presente Instrução, entende-se por:

i. "Altos cargos de natureza política ou pública":

(1). chefes de Estado, chefes de Governo e membros do Governo;

(2). deputados;

(3). membros de tribunais superiores e de outros órgãos judiciais de alto nível, cujas decisões não possam ser objeto de recurso salvo em circunstâncias excecionais;

(4). membros de órgãos de administração e fiscalização de bancos centrais;

(5). chefes de missões diplomáticas e de postos consulares;

(6). oficiais de alta patente das Forças Armadas e forças policiais;

(7). membros de órgãos de administração e de fiscalização de empresas públicas e de sociedades anónimas de capitais exclusiva ou maioritariamente públicos ou controladas pelo Estado, institutos públicos, fundações públicas e estabelecimentos públicos, qualquer que seja o modo da sua designação;

(8). membros de órgãos executivos de organizações de direito internacional;

ii. "Membros próximos da família":

(1). o cônjuge ou unido de facto;

(2). os pais, os filhos e os respetivos cônjuges ou unidos de facto;

(3). os irmãos;

o). "Transferências eletrónicas qualificadas", todas as transferências eletrónicas, excluindo as que resultem de uma operação realizada através de cartão de crédito ou de débito ou de cartão pré-pago para a aquisição de bens ou serviços (não incluindo transferências entre pessoas), desde que o número do cartão acompanhe todas as transferências resultantes da operação, e excluindo transferências e liquidações entre instituições financeiras, em que ambas as partes atuam por sua conta;

p). "Administração", os quadros superiores em cada Banco responsáveis pela gestãoe administração do Banco;

q). "Banco de fachada", um banco constituído e com licença bancária num país onde não tem qualquer presença física e que não se encontra integrado num grupo financeiro regulado e sujeito a uma efetiva supervisão consolidada;

r). "Operação anómala", uma operação que aparentemente não apresente uma causa económica ou comercial ou que envolva montantes elevados, sobretudo grandes depósitos em numerário inconsistentes com a atividade esperada numa conta.

Artigo 2.º
Âmbito

1. A presente Instrução aplica-se a todos os Bancos e a todas as sucursais de entidades estrangeiras com licença para operar em Timor-Leste.

2. A presente Instrução aplica-se também às sucursais e filiais maioritárias de um Banco situadas no estrangeiro, na medida em que as leis e os regulamentos locais aplicáveis o permitam.

3. Sem prejuízo do disposto no número anterior, caso as leis e os regulamentos locais proíbam a execução dessas obrigações, o Banco deve informar o Banco Central.

SECÇÃO II
PROIBIÇÃO E RESTRIÇÃO

Artigo 3.º
Proibição e restrição

Os bancos ficam proibidos de:

a). Manter contas anónimas ou contas sob nomes manifestamente fictícios;

b). Manter relações com clientes desconhecidos e com clientes que se recusem a fornecer as informações necessárias para o cumprimento da presente Instrução;

c). Autorizar contas numeradas; e

d). Estabelecer ou manterrelações bancárias correspondentes com bancos de fachada.

SECÇÃO III
PROGRAMAS INTERNOS

Artigo 4.º
Políticas e procedimentos internos

1. Cada Banco deve criar políticas e procedimentos internos com vista a assegurar a execução da presente Instrução.

2. As políticas e os procedimentos referidos no número anterior devem incluir, mas não exclusivamente, o seguinte:

   a). identificação e verificação do cliente;

   b). aceitação do cliente;

   c). monitorização e controlo permanentes de contas de alto risco;

   d). comunicação de operações suspeitas;

   e). conservação de documentos.

3. Os Bancos devem incluir nas respetivas políticas e procedimentos internos medidas razoáveis no sentido de identificar e avaliar o risco dos clientes, nomeadamente na identificação do tipo de clientes associados a um elevado risco de branqueamento de capitais ou de financiamento do terrorismo.

4. De modo a determinar o perfil de risco de um determinado cliente ou tipo de cliente, o Banco deve considerar, no mínimo, os seguintes fatores:

   a). a origem do cliente e o local de atividade;

   b). os antecedentes ou o perfil do cliente;

   c). a natureza da atividade do cliente; e

   d). a estrutura da propriedade de um cliente empresarial.

5. Os Bancos devem adotar procedimentos de seleção adequados na respetiva política de recrutamento, a fim de assegurar a contratação de funcionários de acordo com critérios exigentes.

Artigo 5.º
Medidas de conformidade

1. Cada Banco deve nomear um Responsável pela Conformidade ao nível dos quadros superiores, aprovado pelo Banco Central, apto a exercer tal função com eficácia e a servir de ponto de contacto para o Banco Central e a Unidade de Informação Financeira em matérias relacionadas com ABC/CFT.

2. O Responsável pela Conformidade deve ter contacto direto com os quadros superiores de gestão do Banco e deve ter pleno acesso a todas as informações e dados dos clientes, no sentido de assegurar a execução das disposições previstas na presente Instrução e das leis e regulamentos aplicáveis.

3. Os Bancos devem obter a autorização do Banco Central para a nomeação, ou alteração na nomeação, do Responsável pela Conformidade.

4. Os Bancos devem definir e documentar claramente as funções e responsabilidades do Responsável pela Conformidade, com o intuito de assegurar o seguinte:

   a). a conformidade do Banco com os requisitos da presente Instrução e de outras leis e regulamentos aplicáveis;

   b). a adoção de políticas e programas de anti-branqueamento de capitais e de combate ao financiamento do terrorismo;

   c). a existênciade canais de comunicação adequados para a eficaz comunicação das políticas e procedimentos em matéria de ABC/CFT a todo e qualquer funcionário;

   d). a sensibilização de todos os funcionários para as medidas do Banco em matéria de ABC/CFT, incluindo políticas, mecanismos de controlo e canais de comunicação;

   e). a identificação dos riscos de branqueamento de capitais e de financiamento do terrorismo associados a novos produtos ou serviços ou decorrentes das alterações operacionais do Banco, incluindo a introdução de novas tecnologias e novos processos;

   f). a avaliação contínuado mecanismo de ABC/CFT, de modo a assegurar a sua eficácia e razoabilidade para

fazer face a qualquer alteração nas tendências de branqueamento de capitais e financiamento do terrorismo.

Artigo 6.º
Relatório anual de conformidade

1. Cada Banco deve elaborar um relatório anual relativo à aplicação da presente Instrução, que deve incluir, mas não exclusivamente, o seguinte:

   a). uma descrição dos sistemas, dos objetivos de controlo e dos controlos e procedimentos do banco para a execução dos mecanismos de ABC/CFT de acordo com a lei e as Instruções em matéria de ABC/CFT, em especial no que diz respeito aos objetivos e requisitos previstos no artigo 4.º;

   b). o nome, a função e as responsabilidades do Responsável pela Conformidade;

   c). a função e as responsabilidades da Auditoria Interna na verificação dos sistemas e procedimentos, incluindo os recursos humanos, com um resumo dos programas de auditoria em matéria de ABC/CFT programados e concluídos ao longo do ano;

   d). uma descrição dos programas de formação em matéria de ABC/CFT destinados ao pessoal ao longo do ano.

2. O relatório mencionado no número anterior deve incluir uma declaração assinada pelo Presidente do Conselho de Administração, ou pelo diretor executivo (no caso de uma sucursal de um banco estrangeiro), a indicar que:

   a). a descrição dos sistemas e procedimentos do Banco apresentadano relatório obedece à sua conceção e implementação ao longo do ano;

   b). os controlos associados aos objetivos de controlo mencionados na descrição dos sistemas e procedimentos do Banco foram adequadamente projetados ao longo do período;

   c). os controlos associados aos objetivos de controlo identificados no relatório foram executados com eficácia ao longo do ano;

   d). as restantes informações do relatório descrevem suficientemente o assunto e revelaram a sua eficácia ao longo do ano.

3. Cada Banco deve solicitar, aos seus auditores internos ou externos, a emissão de um parecerindicandose a descrição do sistema e outras informações no relatório representam suficientemente o sistema concebido e implementado;se os controlos concebidos são adequados para a concretização dos objetivos dos mecanismos de ABC/CFT e se os controlos foram executados com eficácia ao longo do ano.

4. O auditor deve emitir um parecer que:

   a). transmita uma garantia razoável acerca dos assuntos referidos na declaração do Presidente do Conselho de Administração;

   b). inclua uma descrição dos testes de controlo e dos respetivos resultados;

   c). chame a atenção para as insuficiências ou debilidades materiais;

   d). chame a atenção para qualquer limitação no âmbito da auditoria.

5. O relatório, a declaração do Presidente do Conselho de Administração e o parecer do auditor devem ser enviados ao Banco Central no prazo de quatro meses após o término de cada exercício financeiro.

Artigo 7.º
Programa de formação

1. Os Bancos devem ministrar programas de formação regulares ao seu pessoal em matéria de práticas e medidas de ABC/CFT, em especial ao pessoal envolvido nas relações diretas com clientes e ao pessoal responsável pelo tratamento e aceitação de novos clientes, bem como ao pessoal responsável pela monitorização de operações.

2. Os Bancos devem sensibilizar os seus funcionários para o facto de poderem ser responsabilizados por qualquer incumprimento dos requisitos em matéria de ABC/CFT.

3. Os Bancos devem reservar uma dotação no respetivo orçamento anual de despesas operacionais para a realização de um programa de formação contínuoao seu pessoal sobre oABC/CFT.

CAPÍTULO II
DEVER DE DILIGÊNCIA RELATIVO À CLIENTELA

Artigo 8.º
Requisitos gerais

1. Os Bancos, ao realizarem o processo de diligência relativo aos seus clientes, devem obter sempre uma cópia dos documentos e dos dados que comprovam a realizaçãodo referido processo.

2. Os Bancos devem tomar todas as medidas razoáveis e adequadas para assegurar que as fichas dos clientes já existentes, incluindo o perfil do cliente, se mantêm atualizadas e relevantes durante a relação de negócio.

3. Os Bancos devem informar o cliente para a necessidade de proceder à atualização das informações nas suas outras contas, caso existam.

4. O Banco Central pode, periodicamente, determinar as condições em que as obrigações respeitantes à identificação e verificação da identidade dos clientes ou dos beneficiários efetivos podem ser reduzidas ou simplificadas.

5. Os Bancos têm a obrigação de identificar e avaliar os riscos e devem aplicar uma abordagem baseada no risco na gestão dos riscos que identifiquem.

Artigo 9.º
Identificação dos clientes

1. Os Bancos devem identificar os seus clientes e beneficiários efetivos, bem como verificar as respetivas identidades, através de documentos, dados ou informações de origem independente, sempre que:

   a). estabeleçam relações de negócio com qualquer cliente;

   b). executemoperações ocasionais de montante igual ou superior a US$ 10,000, quer seja no âmbito de uma única operação ou através de várias operações que aparentem estar relacionadas entre si;

   c). subsistam dúvidas quanto à veracidade ou à adequação dos dados de identificação do cliente previamente obtidos;

   d). exista uma suspeita de branqueamento de capitais ou de financiamento do terrorismo.

2. O processo de diligência, exigido no número anterior, deve incluir a identificação e verificação do(s) beneficiário(s) efetivo(s) das entidades que detêm uma participação de controlo e das pessoas singulares que exercem o controlo ou a gestão da pessoa coletiva ou de outra pessoa singular.

3. Os Bancos devem identificar e verificar a identidade dos seus clientes através dos seguintes meios:

   a). a identificação de pessoas singulares e a verificação das respetivas identidades devem incluir o nome completo e o número de identificação nacional;

   b). a identificação das pessoas coletivas deve incluir a verificação de informações relativas à denominação social, à morada da sede social, à identificação dos titulares dos órgãos sociais, ao certificado de constituição ou prova semelhante da respetiva personalidade jurídica, à forma jurídica da pessoa coletiva, bem como à forma e poderes das pessoasque exercem a gestão corrente da pessoa coletiva;

   c). identificação das entidades sem personalidade jurídica relevantes, incluindo as pessoas relacionadas com essas entidades.

4. Os Bancos devem obter informações sobre o objeto e a natureza pretendida da relação de negócio.

5. Nos casos em que existam dúvidas sobre se o cliente referido no n.º 1 supra age por conta própria, os Bancos devem verificar a identidade da pessoa ou pessoas em nome ou por conta de quem o cliente atua e verificar se está autorizado para o efeito.

6. Sem prejuízo dos requisitos enunciados nos números anteriores, os Bancos podem verificar a identidade de um cliente e de qualquer beneficiário efetivo do cliente após o estabelecimento de uma relação de negócio com o cliente, caso:

   a). tal seja necessário para a continuação das relações normais de negócio com o cliente; e

   b). seja efetivamente gerido qualquer risco de branqueamento de capitais ou de financiamento do terrorismo que possa eventualmente decorrer da ação de verificação, após o estabelecimento da relação de negócio.

7. Os Bancos que realizam a ação de verificação após o estabelecimento de uma relação de negócio com um cliente, nos termos do número anterior, devem concluir a verificação num prazo razoável, sem nunca ultrapassar o prazo de 3 dias úteis a contar da data do estabelecimento da relação de negócio.

8. Se um banco for incapaz de cumprir os requisitos previstos nos n.ºs 1 a 6 supra, o mesmo:

   a). não deve abrir a conta, não deve iniciar uma relação de negócio nem realizar qualquer operação ocasional com esse cliente; ou

   b). no caso de já existir uma relação de negócio com esse cliente, deve cessar a mesma e considerar a possibilidade de fazer uma comunicaçãode operação suspeita.

Artigo 10º

1. Sempre que os Bancos procedam à abertura de contas de depósito, devem ser recolhidos nas respetivas fichas, pelo menos, os seguintes elementos referentes a cada um dos titulares das contas e aos seus representantes, bem como a outras pessoas com poderes para a movimentação das mesmas:

   a). No caso de pessoas singulares:

   i. Nome completo e assinatura;

   ii. Data e local de nascimento;

   iii. Nacionalidade;

   iv. Morada completa;

   v. Profissão e entidade patronal, quando aplicável;

   vi. Número de identificação fiscal, quando aplicável;

   vii. Cargos públicos que exerçam;

   viii. Tipo, número, data e entidade emitente do documento de identificação;

   ix. Rendimentos;

   x. Uso expectável da conta: montantes, número, tipo, objetivo e frequência das transações esperadas;

   xi. Endereço de correio eletrónico, número de telefone e de telemóvel.

b). No caso de pessoas coletivas:

i. Denominação social;

ii. Objeto social;

iii. Endereço da sede social;

iv. Número de identificação fiscal;

v. Número de registo;

vi. Identificação dos titulares de participações sociais ou direitos de voto, correspondente a, no mínimo, 5% do capital social da pessoa coletiva;

vii. Identificação dos titulares dos órgãos de gestão da pessoa coletiva;

viii. Identificação de qualquer pessoa que exerça um controlo efetivo sobre a pessoa coletiva;

ix. Identificação dos beneficiários efetivos.

c). No caso de contas tituladas por empresários em nome individual, a respetiva ficha de abertura de conta deve conter o número de identificação fiscal, a denominação, a sede ou estabelecimento principal e o objeto da atividade, para além dos elementos de identificação referidos no parágrafo a).

d). Os elementos referidos nas alíneas v. e vii do parágrafo b) não se aplicam a entidades que se encontrem admitidas à cotação numa bolsa reconhecida.

2. Os elementos de identificação referidos no número anterior devem ser comprovados através das seguintes formas:

a). Para pessoas singulares, os elementos de identificação referidos nas alíneas i) a iii) do parágrafo a) do número anterior, devem ser comprovados:

i. Quanto aos residentes, mediante a apresentação de dois dos documentos de identificação seguintes: bilhete de identidade, cartão de eleitor, passaporte, ou autorização de residência em território nacional quando cidadão estrangeiro;

ii. Quanto aos não-residentes, mediante a apresentação do passaporte e de declaração de identidade devidamente certificada pela Embaixada ou Consulado do seu país de origem ou residência ou, por uma entidade pública Timorense.

b). A morada completa, a profissão e entidade patronal podem ser comprovadas através de qualquer documento, meio ou diligência considerado idóneo e suficiente para a comprovação das informações prestadas.

c). No que respeita às pessoas coletivas:

i. Os elementos de identificação previstos nas alíneas i) a iii) do parágrafo b) do número 2, devem ser comprovados mediante certidão do registo comercial, e, no caso de não-residentes, através de um documento equivalente e devidamente certificado;

ii. Os elementos de identificação previstos nas alíneas iv) e v) do parágrafo b) do número 2, podem ser provados mediante a apresentação de um certificado das autoridades fiscais, certidão do registo comercial, ou, ainda, no caso de não residentes, através de um documento equivalente e devidamente certificado;

iii. Os elementos de identificação previstos nas alíneas vi) e vii) do parágrafo b) do número 2, podem ser comprovados mediante simples declaração escrita emitida pela própria pessoa coletiva, contendo o nome ou a denominação social dos titulares, que deverá ser assinada e, no caso de sociedades anónimas, deverá ser assinada pelo secretário da sociedade.

d). Quando a pessoa singular ou coletiva não seja residente em território nacional e não tenha comprovado algum dos elementos de identificação exigidos no número 2, pode o Banco solicitar confirmação escrita da veracidade e atualidade das informações prestadas, a emitir por uma instituição de crédito onde a pessoa já seja titular de uma conta de depósito bancário.

e). Caso o Banco leve a cabo a confirmação referida no parágrafo anterior, deve notificar o Banco Central desse facto, bem como, dos detalhes da instituição de crédito que prestou a informação, e o Banco Central pode, caso entenda necessário, impor requisitos adicionais.

Artigo 11.º
Novas tecnologias e relações de negócio sem a presença física do cliente

1. Os Bancos devem adotar políticas e tomar medidas adequadas no sentido de gerir e mitigar os riscos para prevenir a utilização abusiva dos desenvolvimentos tecnológicos em esquemas de branqueamento de capitais ou de financiamento do terrorismo que possam resultar:

a). do desenvolvimento de novos produtos e novas práticas comerciais, incluindo novos mecanismos de distribuição; e

b). da utilização de novas tecnologias ou em fase de desenvolvimento relacionadas com novos produtos e produtos preexistentes.

2. Os Bancos que disponibilizem serviços comerciais sem a presença física do cliente, ao estabelecerem e conduzirem relações de negócio devem prestar especial atenção ao seguinte:

a). adotaras medidas adequadas para a verificação dos clientes, com uma eficácia igual à aplicada para os clientes presenciais;

b). implementação de um sistema de monitorização e de um mecanismo de comunicação para a identificação de potenciais atividades de branqueamento de capitais e de financiamento do terrorismo.

3. As medidas que o Banco possa utilizar para a verificação de clientes não presenciais devem incluir, mas não exclusivamente:

   a). documentação adicional em complemento à documentação exigida para os clientes presenciais;

   b). estabelecimento de contacto independente com o cliente; ou

   c). verificação das informações do cliente publicamente disponíveis.

4. O banco deve assegurar aexistência de uma certificação das cópias obtidas quando em presença de relações de negócio à distância.

Artigo 12.º
Dever de diligência reforçado

1. Os Bancos devem aplicar medidas de diligência reforçadas relativamente aos clientes de risco mais elevado, incluindo, mas não exclusivamente, os seguintes:

   a). indivíduos com elevado património líquido;

   b). pessoas politicamente expostas;

   c). entidades sem personalidade jurídica complexas;

   d). clientes não residentes;

   e). atividades que envolvam transações em numerário de forma intensiva;

   f). indivíduos e entidades oriundos de locais conhecidos pelas suas elevadas taxas de criminalidade (p. ex., produção e tráfico de estupefacientes, contrabando, etc.);

   g). atividades identificadas pelo GAFI como de risco mais elevado de branqueamento de capitais e de financiamento do terrorismo; e

   h). países ou jurisdições com leis e regulamentos inadequados em matéria de ABC/CFT, conforme salientado pelo GAFI.

2. Sem prejuízo dos requisitos enunciados no número anterior, os Bancos podem classificar um cliente ou uma operação como de alto risco, sempre que:

   a). na sequência da aceitação inicial do cliente, o Banco considere que o padrão da atividade da conta não se coaduna com o conhecimento que o banco tem sobre o cliente;

   b). o cliente se recuse, sem justificação aceitável, a fornecer informações solicitadas pelo Banco e a colaborar no processo de diligência relativo à clientela instituído pelo Banco;

   c). o Banco suspeite que o cliente tenha recusado serviços bancários de outro Banco em virtude da implementação de requisitos sobre branqueamento de capitais e financiamento do terrorismo.

3. Sem prejuízo da adoção de medidas mais exigentes em relação a certas transações ou categorias de pessoas, o processo de diligência previsto nos números anteriores deve incluir, mas não exclusivamente, o seguinte:

   a). a obtenção de informações mais detalhadas do cliente e do beneficiário efetivo e, através de informações publicamente disponíveis, aplicandotodas as medidas razoáveis e adequadas com vista a determinar a origem do património ou dos fundos e o objetivo da operação; e

   b). a obtenção da autorização da administração do Banco para iniciar ou continuar a relação de negócio com o cliente.

4. Os Bancos devem exercer,de forma contínua, uma diligência reforçada relativamente aos clientes mencionados no n.º 1 supra, ao longoda relação de negócio com tais clientes.

5. O Banco Central pode, periodicamente, rever a classificação do tipo de clientes mencionados no n.º 1 supra.

Artigo 13.º
Dever de diligência contínuorelativo à clientela

1. Os Bancos devem exercer um dever de diligência contínuorelativamente às relações de negócio com os clientes e analisar cuidadosamente as operações efetuadas, de modo a assegurar a sua consistência com os conhecimentos que têm sobre o cliente, as suas atividades comerciais e o seu perfil de risco e, se necessário, analisar a origem dos seus fundos.

2. Os Bancos devem utilizar um sistema que detete operações anómalas em todas as contas dos seus clientes e adotar procedimentos que permitam aferir se tais operações anómalas podem ser consideradas suspeitase, como tal, serem reportadas à UIF.

3. Os Bancos devem efetuar revisões periódicas das fichas dos clientes já existentes, nomeadamente sempre que:

   a). esteja eminente a realização de uma transação significativa;

   b). existam alterações significativas à forma como a conta é movimentada;

   c). os padrões da documentação do cliente se alterem substancialmente; ou

   d). se descubra que as informações existentes sobre o cliente são insuficientes.

4. Em circunstâncias diferentes das mencionadas no número anterior, um Banco, com base na sua avaliação dos riscos, pode, nos termos das normas vigentes do Banco em matéria de dever de diligência relativo à clientela, solicitar informações adicionais sobre os clientes já existentes que sejam considerados de risco mais elevado.

CAPÍTULO III
RELAÇÕES CORRESPONDENTES

Artigo 14.º
Requisitos gerais

1. Os Bancos ficam proibidos de estabelecer ou manter rela-

ções de negócio com bancos ou entidades financeiras que se encontrem domiciliados ou sejam filiais de entidades sediadas num país ou território que não disponha de umaefetiva supervisão consolidada.

2. Os Bancos ficam proibidos de estabelecer ou manter relações de negócio com instituições financeiras clientes num país estrangeiro, caso estas autorizem a utilização das suas contas por bancos de fachada.

3. Os Bancos devem obter autorização da administração antes de estabelecerem novas relações bancárias correspondentes.

Artigo 15.º
Banca correspondente

Os Bancos devem adotar as seguintes medidas antes de estabelecerem relações transfronteiras entre bancos correspondentes:

a). avaliar a idoneidade do banco cliente através das seguintes ações:

i. recolha de informação adequada sobre o banco cliente, de modo a compreender plenamente a natureza da sua atividade, incluindo o seguinte, se aplicável:

(1). A política de conhecimento dos seus clientes (*know your customer*);

(2). informações sobre os gestores e sobre os detentores da participaçãode capital ou de direitos de voto ou de controlo efetivo do banco cliente;

(3). principais atividades de negócio;

(4). a respetiva presença geográfica ou o país do banco correspondente.

ii. a partir de informações publicamente disponíveis, avaliar a reputação da instituição cliente e a natureza da supervisão a que está sujeita;

iii. avaliar os mecanismos adotados pelo banco cliente em matéria de ABC/CFT, verificar a sua adequabilidade e eficácia, com base nas medidas de ABC/CFT adotadas no país ou na jurisdição onde o banco cliente opera; e

iv. no caso de contas correspondentes de transferência (*payable-through accounts*), o Banco deve assegurar que a instituição cliente:

(1). verificou a identidade do cliente;

(2). adotou mecanismos de monitorização contínua relativamente à sua clientela; e

(3). se encontra habilitada a fornecer os dados adequados sobre a identificação dos seus clientes, quanto tal lhe for solicitado.

b). compreender e documentar claramente as respetivas responsabilidades de cada banco em matéria de ABC/CFT.

CAPÍTULO IV
TRANSFERÊNCIAS ELETRÓNICAS

Artigo 16.º
Obrigações dos Bancos

1. Os Bancos não devem executar, intermediar ou receber transferências eletrónicas, salvo se estas obedecerem às disposições da presente Instrução.

2. Os Bancos ordenantes devem incluir a informação necessária e exata sobre o ordenante, bem como a informação necessária sobre o beneficiário, em todas as transferências eletrónicas e mensagens associadas.

3. No processamento das transferências eletrónicas, os Bancos intermediários na cadeia de pagamento devem assegurar:

a). que todas as informações sobre o ordenante e o beneficiário na transferência eletrónica ou na mensagem associada se mantêm ao longo do processamento da transferência eletrónica;

b). a adoção de políticas e procedimentos eficazes baseados no risco a fim de determinar: i) quando executar, rejeitar ou suspender uma transferência eletrónica à qual falte a informação necessária sobre o ordenante ou o beneficiário; e ii) as ações adequadas para o seu acompanhamento.

4. Os Bancos beneficiários devem:

a). adotar medidas razoáveis para identificar as transferências eletrónicas transfronteiras às quais falte a informação necessária sobre o ordenante ou o beneficiário;

b). verificar a identidade do beneficiário, caso não tenha havido uma identificação prévia;

c). conservar documentação sobre a identidade do beneficiário;

d). adotar políticas e procedimentos eficazes baseados no risco a fim de determinar: i) quando executar, rejeitar ou suspender uma transferência eletrónica à qual falte a informação necessária sobre o ordenante ou o beneficiário; e ii) as ações adequadas para o seu acompanhamento.

5. No processamento das transferências eletrónicas, os Bancos devem adotar medidas de congelamento e proibir a realização de operações com pessoas e entidades designadas, em conformidade com as obrigações previstas no artigo 36.º da Lei ABC/CFT, relacionadas com a prevenção e supressão do terrorismo e do financiamento do terrorismo.

Artigo 17.º
Requisitos respeitantes às transferências eletrónicas

1. Todas as transferências eletrónicas qualificadas devem conter sempre o seguinte:

a). o nome do ordenante;

b). o número de conta do ordenante, se essa conta for utilizada para o processamento da operação;

c). a morada do ordenante, ou o número do documento de identidade nacional, ou o número de identificação de cliente, ou a data e o local de nascimento;

d). o nome do beneficiário; e

e). o número de conta do beneficiário, se essa conta for utilizada para o processamento da operação.

2. As transferências eletrónicas transfronteiriçasde montante inferior a US$ 1,000 podem ficar sujeitas a medidas de diligência simplificada, salvo se existir suspeita de branqueamento de capitais ou de financiamento do terrorismo.

3. Não pode ser iniciada qualquer transferência eletrónica para um cliente sem que odevido processo de diligência, nos termos desta Instrução, se encontre completo.

4. Na ausência de uma conta, deve incluir-se o número de referência único da operação que permite a rastreabilidade da operação.

5. O requisito enunciado no n.º 1 supra, relativamente à informação sobre o ordenante, pode não ser aplicável quando diversas transferências eletrónicas transfronteiriças individuais provenientes de um único ordenante são agregadas num lote de transferências para transmissão aos beneficiários, desde que incluam o número de conta do ordenante ou o número de referência único da operação (conforme descrito no n.º 3 supra) e o lote de transferências contenha a informação necessária e exata sobre o ordenante, bem como todas as informações sobre o beneficiário, totalmente rastreáveis no país beneficiário.

CAPÍTULO V
CONSERVAÇÃO DE DOCUMENTOS

Artigo 18.º
Conservação de documentos

1. Os Bancos devem conservar documentos, através de um sistema adequado de conservação de documentos, facilmente acessíveis ao Banco Central e a outras autoridades competentes designadas por lei, contendo as seguintes informações:

a). Cópias de documentos comprovativos das identidades dos clientes, beneficiários efetivos ou agentes, das diligências efetuadas, da documentação relativa às contas, da correspondência comercial e da documentação relativa às transações,por um período de, pelo menos, dez [10] anos desde a data da realização das transações ou após o termo da relação de negócio com o cliente;

b). Cópias de todos os relatórios enviados à UIF durante, pelo menos, cinco anos após a data de envio à UIF;

c). Cópias de todos os relatórios e dados facultados às UIF e/ou entidades estrangeiras; e

d). Cópias da informação recebida da UIF no que diz respeito às comunicaçõessobre operações suspeitas submetidas, durante um período de cinco anos após a receção da referida informação.

2. Sem prejuízo dos requisitos enunciados no número anterior, a documentação que seja objeto de investigações contínuas ou de ação judicial deve ser conservada para além do período de conservação estipulado, até tal documentação deixar de ser necessária.

3. Os Bancos devem assegurar que a documentação e registos conservadossão suscetíveis de criarem um registo das operações individuais que sejam rastreáveis pelo Banco Central, pela UIF e pelas autoridades policiais e judiciárias, conforme estipulado por lei.

CAPÍTULO VI
COMUNICAÇÃO DE OPERAÇÕES

Artigo 19.º
Comunicação de operação suspeita

1. Os Bancos devem enviar imediatamente uma comunicação de operação suspeita à Unidade de Informação Financeira, utilizando o formulário constante do Anexo 1 à presente Instrução e assinado pelo Responsável pela Conformidade, quandoexistirem motivos para suspeitar que uma operação possa envolver proventos resultantes de uma atividade ilícita ou que o cliente esteja envolvido em atividades de branqueamento de capitais ou de financiamento do terrorismo.

2. Os Bancos devem também considerar a possibilidade de fazer uma comunicação de operação suspeita à UIF no caso de não terem conseguido concluir uma operação ou tentativas de operação, ou o dever de diligência relativo à clientela, independentemente da relação ter sido iniciada ou não.

3. Os Bancos devem assegurar a sua plena colaboração com a UIF quanto ao fornecimento de informações e documentação adicionais que lhe possam ser solicitadas, bem como responder prontamente a quaisquer pedidos de informação relativos a qualquer comunicaçãode operação suspeita.

4. Os Bancos devem adotar um sistema de comunicação para o envio de comunicaçõesde operações suspeitas à Unidade de Informação Financeira, incluindo um mecanismo para o envio de comunicações oriundas das suas sucursais.

5. Os Bancos devem assegurar que o mecanismo de comunicação de operações suspeitas funciona num ambiente protegido, a fim de preservar a confidencialidade e o sigilo.

6. Os Bancos devem aplicar medidas razoáveis no sentido de assegurar que todos os seus funcionários envolvidos na realização ou facilitação de operações do cliente conhecem os procedimentos de comunicação exigidos no presente artigo.

7. Ao apresentar uma comunicação de operação suspeita, devem ser tomados todos os cuidados com vista a assegurar o tratamento das comunicaçõescom o mais elevado grau de confidencialidade e ninguém deve divulgar o facto de que uma comunicaçãode operação suspeita, ou

informações associadas, vai ser ou foi enviada à UIF ou ao Banco Central.

8. Os Bancos devem comunicar de imediato à UIF sempre que suspeitem ou tenham razões suficientes para suspeitar que uma operação ou uma série de operações estão a ser conduzidas de forma a evitar o reporte de operações em numerário, conforme requerido por esta Instrução, no âmbito do seu artigo 20º.

Artigo 20.º
Comunicação de operações em numerário

1. Os Bancos devem comunicar à UIF, da forma estipulada pelo Banco Central, qualquer operação em numerário de montante igual ou superior a US$ 10,000, quer seja no âmbito de uma única operação ou através de várias operações que aparentem estar relacionadas entre si.
2. As operações em numerário devem incluir, mas não exclusivamente, cheques, cheques de viagem, ordens de pagamento/vales postais, cartas de crédito ou outros instrumentos monetários em qualquer moeda.
3. Os Bancos devem dispor de sistemas que permitam satisfazer os requisitos previstos no presente artigo.
4. Sem prejuízo dos requisitos enunciados nos números anteriores, os Bancos não são obrigados a comunicar as seguintes operações:
   a). Operações em nome de Bancos;
   b). Operações com o Banco Central.

Artigo 21.º
Outras comunicações

1. Os Bancos devem comunicar ao Banco Central os nomes dos clientes cujos pedidos de abertura de conta junto do Banco sejam recusados.
2. Os Bancos devem comunicar imediatamente ao Banco Central qualquer investigação policial sobre atividades de branqueamento de capitais ou de financiamento do terrorismo que esteja a decorrer no Banco ou numa sociedade sob o seu controlo.
3. Os Bancos devem comunicar imediatamente ao Banco Central qualquer operação recusada pelo Banco nos termos da presente Instrução.

CAPÍTULO VII
DISPOSIÇÕES TRANSITÓRIAS E FINAIS

SECÇÃO I
DISPOSIÇÃO TRANSITÓRIA

Artigo 22.º
Disposição transitória

Os requisitos enunciados no Artigo 20 da presente Instrução entrarão em vigor a partir de 1 de janeiro de 2018.

SECÇÃO II
DISPOSIÇÕES FINAIS

Artigo 23.º
Disposições finais

Os Bancos que, à data de entrada em vigor da presente Instrução, permitam a existência de contas numeradas confidenciais ou contas anónimas devem, num prazo de trinta 30 dias, encerrar as referidas contas.

Artigo 24.º
Revogação

A presente Instrução revoga e substitui os seguintes instrumentos:

a). Instrução Pública n.º 02/2004 referente à Prevenção de Atividades de Lavagem de Dinheiro,Identificação de Clientes eRegisto e Manutenção de Dados;

b). Capítulo VI da Instrução Pública n.º 06/2010 sobre o Licenciamento e Supervisão de Outras Instituições Recetoras de Depósitos (OIRD);

c). A Seção 1, Seção 2 número 1 parágrafo f) e Seção 2 número 2 parágrafo e) da Instrução n.º 03/2003 sobre a Abertura e Manutenção de Contas de Depósito.

Artigo 25.º
Medidas de conformidade

1. Os Bancos, qualquer dos seus administradores, e respetivo pessoal, ficam sujeitos às sanções administrativas previstas nos artigos 31.º e 32.º da Lei ABC/CFT, caso o Banco Central determine que as disposições da presente Instrução foram violadas.
2. As sanções administrativas estipuladas no número anterior não devem limitar os poderes gerais do Banco Central referentes à emissão de advertências por escrito, à suspensão ou demissão de administradores, à revogação de licenças bancárias ou ao exercício de quaisquer outros poderes conferidos por legislação.

Artigo 26.º
Entrada em vigor e publicação

1. A presente Instrução entrará em vigor na data da sua publicação.
2. De acordo com o artigo 66.º, n.º 1, da Lei Orgânica do Banco Central de Timor-Leste, a presente Instrução será publicada no Jornal da República.

Adotada em 28 de Março de 2017

O Governador

Abraão de Vasconselos

COMUNICAÇÃODE OPERAÇÃO SUSPEITA

A obrigação de apresentação de uma Comunicação de Operação Suspeita é exigida nos termos do artigo 23.º da Lei n.º 17/2011, de 28 de dezembro, que aprova o Regime Jurídico da Prevenção e do Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo.

Enviar o formulário preenchido para a seguinte morada:

Unidade de Informação Financeira

A/c. Diretor Executivo
Edifício do Banco Central de Timor-Leste
Avenida Bispo Medeiros
Díli, Timor-Leste

O formulário preenchido pode também ser enviado por fax para o número +670 331 3716

Todos os campos da comunicaçãoassinalados com asterisco (*) são de preenchimento obrigatório. Os campos assinalados com "se aplicável" devem ser obrigatoriamente preenchidos caso seja aplicável a si ou à operação comunicada. Nos restantes campos, deverá envidar esforços razoáveis para obter as informações.

PARTE A: INFORMAÇÕES SOBRE O CLIENTE

a) Titular da conta

1. Nome (*)			
2. N.º ID/N.º passaporte/N.º registo da sociedade (*)	Novo		
	Antigo		
3. Sexo (*)	☐ Masculino ☐ Feminino	4. País *)	
5. Negócio/Emprego (*)		6. Profissão *)	
7. Outra profissão (*)			
8. Nome da entidade patronal (*)			
9. Morada (*)			

b) Entidade que realiza a operação

10. Nome (*)			
11. N.º ID/N.º passaporte/N.º registo da sociedade (*)	Antigo		
	Novo		
12. Sexo (*)	☐ Masculino ☐ Feminino	13. País	
14. Outra profissão (*)			
15. Nome da entidade patronal (*)			
16. Morada (*)			

PARTE B: INFORMAÇÕES SOBRE A OPERAÇÃO

17. Número da conta (*)		18. Tipo de conta	
19. Data de abertura da conta (*)		20. Situação da conta	
21. Saldo (*)			
22. Sucursal (*)		23. Estado/cidade	

a) Apresentador/Fiador

24. Nome (*)			
25. N.º ID/N.º passaporte/N.º registo da sociedade (*)	Novo Antigo		
26. Sexo (*)	☐ Masculino ☐ Feminino	27. País	

b) Operação

28. Frequência (*)	☐ Única ☐ Múltipla	29. Data da operação *)	Clique para inserir data.
30. Montante total em (*) USD			
31. Montante de moeda estrangeira envolvida (*)		32. Tipo de moeda *)	
33. Tipo de operações (*)	Selecione um item.		

PARTE C: DESCRIÇÃO DA OPERAÇÃO SUSPEITA

34. Motivos de suspeição [Assinalar com (√) na caixa adequada]

☐ Conta inativa reativada

☐ Regular/offshore anormal /Atividade

☐ Depósito/Levantamento em numerário de montante elevado/ anormal

☐ ransferência feita/recebida de montante elevado/anormal

☐ Atividade inconsistente com o perfil do cliente

☐ Outros. _____

(Especificar)

35. Informação detalhada sobre a natureza da operação e as circunstâncias envolventes (*)

36. Data da declaração (*) Clique aqui para inserir data.

dd/mm/aaaa

PARTE D: RESERVADA EXCLUSIVAMENTE À UNIDADE DE INFORMAÇÃO FINANCEIRA

37. Responsável pela comunicação		38. Data de receção	Clique para inserir data.

dd/mm/aaaa

Atenção: o artigo 25.º da Lei n.º 17/2011, de 28 de dezembro, proíbe-o de divulgar ou de facultar informação que tenha prestado ou se prepare para prestar à UIF, bem como informações sobre a investigação pela prática dos crimes de branqueamento de capitais e financiamento do terrorismo. O incumprimento desta obrigação em conformidade com os requisitos previstos nos artigos 31.º e 32.º da referida lei é passível de sanções.