

Islamic Government of Afghanistan



Da Afghanistan Bank

Responsibilities of Financial Institutions in the Fight Against Money Laundering and Terrorist Financing

Part A — General. §

1.1.1. Authority

This regulation on the responsibilities of financial institutions in the fight against money laundering and terrorist financing is pursuant to the authority granted to DAB by the Decree Law of the Islamic Republic of Afghanistan "Anti-Money Laundering and Proceeds of Crime," (AML Law) and the Decree Law of the Islamic Republic of Afghanistan "Combating the Financing of Terrorism" (CFT Law).

§ 1.1.2. Definitions.

- a) *Financial institutions* - financial institutions mentioned in this regulation include commercial banks, branches and representative offices of foreign banks, money service providers, foreign exchange dealers, payment systems operators, securities service providers, non-depository credit institutions (finance companies, leasing companies, mortgage companies), microfinance depository institutions (credit unions and cooperative banks), microfinance non-depository institutions, insurance companies, and private pension plans, to the extent that these institutions are required to be licensed, permitted, regulated, or supervised by Da Afghanistan Bank. For the purposes of this regulation, Da Afghanistan Bank is also considered to be a financial institution to the extent that it engages in commercial activities.
- b) *Large cash transaction* - a transaction in which one party receives, pays, or otherwise transfers cash, bullion, other precious metals, or precious stones, or any other monetary instrument with a value equal to or exceeding Afs 500,000. A large cash transaction also includes the completion of two or more such transactions by or on behalf of the same person during any two consecutive business days when the total value of the transactions is equal to or exceeds Afs 500,000.
- c) *Money laundering* - the offense against the laws of the Islamic Republic of Afghanistan as defined in Article 3 of the AML Law.

- d) *Occasional transaction* - any transaction that is initiated by a customer who is not a regular customer of the financial institution. In the case of depository institutions, all transactions initiated by customers who do not have a deposit account are to be considered occasional transactions.
- e) *Politically exposed person* - this term shall have the same meaning as given in Article 2 of the AM Law.
- f) *Suspicious transaction* - a transaction, or attempted transaction, or contact of any kind between parties with the intent to facilitate a transaction, regardless of amount or means of payment or ultimate completion of transaction, where any of the following circumstances exist: 1) there is no underlying legal or trade obligation, purpose, or economic justification; 2) the client is not properly identified; 3) the amount involved is not commensurate with the business or financial capacity of the client; 4) taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under law and regulations; 5) there are circumstances relating to the transaction which are observed to deviate from the profile of the client and/or the client's past transactions with the financial institution; 6) the transaction appears to be in any way related to an unlawful activity or offense that is about to be, is being, or has been committed; or 7) it is a transaction that is similar or analogous to any of the foregoing.
- g) *Terrorist financing* - the offense against the laws of the Islamic Republic of Afghanistan as defined in Article 3 of the CFT Law.

§ 1.1.3. General goals and objectives.

- a) This regulation aims at protecting financial institutions from being abused by criminals and terrorists, thereby protecting their reputations and minimizing operational risk. Financial institutions are expected to perform their duties in the fight against money laundering and terrorist financing, particularly in the provision of information that may lead to investigations and prosecutions of money launderers and terrorist financiers. In that way, the integrity and solvency of the financial system is fostered, contributing to the financial security of the country.
- b) The objectives of this regulation:
 - 1. Financial institutions will be required to have policies on customer acceptance that clearly identify when customers are to be rejected.
 - 2. Financial institutions will be required to identify their customers properly.
 - 3. Financial institutions will be required to submit reports to the Financial Intelligence Unit (FIU) on large cash transactions and suspicious transactions.
 - 4. Financial institutions will be required to retain records of transactions.
 - 5. Financial institutions will be required to have staff that have been trained sufficiently to carry out their duties under these regulations.

- c) Adherence by financial institutions to the standards set by this regulation will be monitored by DAB through on-site examinations and off-site analysis of data.

Part B — General obligations of financial institutions

§ 1.2.1. Internal controls and compliance.

Financial institutions must designate one individual as an "AML officer" having primary responsibility for development and implementation of the anti-money laundering measures contained in this regulation. A different individual must be designated as having responsibility for auditing the implementation by the AML officer of the policies and procedures developed. In particular, the system of internal controls must ensure that the necessary reports are filed with the FIU. This audit function should report directly to the Board of Supervisors or Board of Directors (if applicable) or to senior management, and its reports should include examples, if any, of the AML officer's failure to implement these measures.

§ 1.2.2. Cooperation with law enforcement.

Financial institutions shall cooperate and coordinate their anti-money laundering activities with FIU and cooperate with the FIU in any freezing or transferring the deposits of clients, according to the relevant provisions in law and regulations.

§ 1.2.3. Responsibilities of overseas branches of financial institutions licensed or permitted in Afghanistan.

The overseas branches of Afghanistan-licensed or permitted financial institutions shall abide by the provisions of laws governing anti-money laundering of the country or region where they are located, and provide cooperation and assistance to the anti-money laundering efforts of law enforcement officials of their host country, according to the laws of that host country.

§ 1.2.4. Responsibilities of professional associations of financial institutions.

The Afghanistan Bankers' Association, the Financial Companies Association of Afghanistan, the Union of Money Changers, and other financial self-disciplinary organizations shall draft working guidelines or codes of conduct for their members concerning anti-money laundering activities, in line with this regulation. They shall effectively discipline or suspend the membership of financial institutions that do not comply with these guidelines. These organizations are also expected to encourage information-sharing among their members concerning the details of customers or individual transactions that have been refused.

Part C - Customer acceptance, customer identification, monitoring of account activity, reporting, confidentiality, records retention, and staff training

§ 1.3.1. Customer acceptance policy.

Financial institutions must have a customer acceptance policy that clearly indicates situations when a customer will be rejected, and must be able to demonstrate to the satisfaction of DAB examiners that the policy has been implemented.

§ 1.3.2. Prohibition on anonymous accounts.

Financial institutions shall not open anonymous accounts or accounts with fictitious names. If the bank opens a numbered account, the identity of the client must be known to a sufficient number of staff to perform identification and subsequent monitoring of the account.

§ 1.3.3. Customer identification.

Financial institutions must set up a registration system for the identification of their clients and establish the identity of clients when performing any transaction for them. In all cases, if there is any doubt that the customer is not the beneficial owner of the funds, the financial institution is responsible for taking reasonable steps to identify the beneficial owner.

- a) *Identification of individuals* — When opening an account or handling any other transaction for an individual, financial institutions shall ask the potential customer to produce his personal, original national identity card or passport that is current and bears a photograph. The financial institution must attempt to verify the information submitted, and retain a copy of the identification document. In addition, the financial institution shall record the permanent address, telephone number (if any), approximate date of birth, place of birth, occupation, and name of employer (if applicable). The financial institution must make reasonable attempts to verify all of this information by means such as telephone calls, visits to the customer's home or place of work, or by any other appropriate and effective means. In cases where an account is opened by one individual (the agent) on behalf of another individual (the principal), the identification procedure must be performed on both the agent and the principal.
- b) *Identification of clients who are corporations, partnerships, organizations, charities, clubs, and associations (collectively, unit clients)* — When opening an account for a unit client, financial institutions shall ask the unit to produce valid registration documents, and these documents should be verified before the account is opened. Financial institutions also must take steps to verify the

identity of any agent that opens an account on behalf of a unit client, if that agent is not an officer of the client.

1. *Corporations and partnerships.* When opening accounts for corporations and partnerships, the following information should be obtained: name of entity, principal place of business operations, mailing address, contact telephone and fax numbers, taxpayer identification number or other official number, the original or certified copy of the Certificate of Incorporation and Articles of Association, the resolution of the Board of Directors to open the account, identification of those who have authority to operate the account, and the nature and purpose of the entity's business. The owners of the corporation or partnership must also be identified, whether they are individuals or other units.
2. *Other unit clients.* When opening accounts for other unit clients, the following information should be obtained: name of client, mailing address, contact telephone and fax numbers, official identification number, description of the purpose and activities of the unit, and a copy of the documentation confirming the legal existence of the unit. The principals of the unit must be identified as those exercising control or significant influence over the unit's assets. Financial institutions must take reasonable steps to identify and verify at least two signatories along with the unit itself.
3. *Single proprietorships.* Financial institutions must not open accounts in the name of unregistered single proprietorships. Instead, the account must be opened in the name of the proprietor as an individual, with proper identification of the individual as described in paragraph a) above.

§ 1.3.4. Regular reviews of customer identification.

Financial institutions must undertake regular reviews of their customers' identification records. These reviews should take place whenever there is a material change in the business relationship between the customer and the financial institution or transactions begin to deviate from the usual patterns.

§ 1.3.5. Monitoring of account activity.

Financial institutions must monitor customers' account activity, on a regular, reasonable schedule, to be able to establish patterns, the deviation from which may indicate suspicious activity.

§ 1.3.6. Reporting.

§ 1.3.6.1 What to Report

Suspicious and large cash transactions meeting the respective definitions in § 1.1.2 must be reported.

§ 1.3.6.2 When to Report

Large Cash Transactions shall be reported no earlier than the first business day of the month and no later than the fifth business day of the month following the month during which the transaction occurred. If no reportable transactions occurred during this period, then a 'NIL' report shall be prepared and submitted in accordance with the

instructions in § 1.3.6.3.

Suspicious Transactions shall be reported as soon as practical, but no later than one business day after initial formation of suspicion. The Suspicious Transaction Report shall be continually updated by the reporting entity as new information becomes available that either supports, refutes, or changes the original suspicion.

§ 1.3.6.3 How to Prepare Reports

Unless otherwise noted, all reports shall be submitted in electronic format.

Large Cash Transaction Reports (LCTR) shall be prepared in conformance with the specification published on the FIU's website (<http://www.fintraca.gov.af>) at the time of submittal. The specification was designed to facilitate direct extraction of reports from reporting entity databases and to eliminate the possibility of formatting errors. For those reporting entities that are not technically capable of direct extraction, a computer-based form is also supplied on the FINTRACA website. The form, once data is manually input by the reporting entity, will generate reports that conform to the specification. Instructions for preparation of a 'NIL' report are also posted on this site.

Suspicious Transaction Reports (STR) must be prepared in accordance with the specification published on the FINTRACA website (<http://www.fintraca.gov.af>) at the time of submittal. However, when time is critical, preliminary reports may be prepared and filed in any convenient format via any other available means facilitating rapid and secure transmittal of information including but not limited to telephone, courier, and secure electronic mail. Filing of a preliminary report does not release the reporting entity from the obligation to file a Suspicious Transaction Report. True and accurate copies of all documents required to support the suspicion must be included as attachments to the report. Reports must be placed for delivery on magnetic, optical, or USB-compatible storage media. Supporting documents may be in paper form if no alternative is available.

Report file names shall adhere to the following naming convention: three character identification code for reporting entity + '_' + Gregorian date of report submission in yyyy-mm-dd format + '_' + sequence number beginning with '1' for multiple reports submitted in a single day + '.xml' extension. For example, a report submitted by Da Afghanistan Bank on 5 December 2006 might be named as DAB_2006_12_05_1.xml

§ 1.3.6.4 How to Deliver Reports

The following modes of report delivery are acceptable:

- By courier. Reports may be delivered to the FIU during normal business hours or by special arrangement with the General Director. Courier must present documentation to prove that he represents the reporting organization indicated on the report. Reporting entities must ensure that delivered media are securely packaged and sealed to prevent tampering in-route.
- Electronic (preferred). Reports may be submitted by secure electronic mail. For this option, the reporting entity must sign an Electronic Signature Agreement with the FIU and must abide by the terms of the Agreement. A template agreement is posted at <http://www.fintraca.gov.af/reports.asp>. Reports that are not submitted in accordance with the terms of the Agreement will not be accepted.

§ 1.3.6.5 Validation of Reports

Delivered reports shall be validated against the report preparation specifications. Those reports that cannot be validated by the FIU will not be considered as having been received.

§ 1.3.6.6 Issuance of Receipts

In accordance with the law, FINTRACA shall issue receipts for documents actually received. Each receipt shall indicate the date and time of receipt, the name of the courier, the name of the submitting organization, and the name and signature of the receiving person. The receipt shall also contain a 'hash' calculation to ensure against future modification of submitted documents. A validation report shall be attached to each receipt issued. The validation report shall contain a list of identifiers corresponding to reports contained in the submitted document that have been validated by FINTRACA. The validation report shall also contain a list of identifiers corresponding to reports in the submitted document that could not be validated. All documents delivered by electronic mail in accordance with the Agreement referenced in § 1.3.6.4 shall be answered with a return receipt from FINTRACA, also in accordance with the Agreement, issued to the originating address.

§ 1.3.7. Confidentiality.

Financial institutions and their staff shall maintain confidentiality, and not disclose information concerning their anti-money laundering activities to their clients or to others, except to the FIU. The exception is that they may disclose to other financial institutions or to their professional associations information about potential clients or transactions that they have refused. In particular, financial institutions must not disclose to clients that they have filed suspicious transactions reports about their activity.

Financial institutions are advised to maintain signage in a prominent place or to hand out written notices to their customers that they are required to report all large cash transactions to the Financial Intelligence Unit. Staff may also orally advise each customer at the time the transaction is initiated.

§ 1.3.8. Records retention.

Financial institutions shall maintain account information and transactions records of clients in line with the following time specifications:

1. At least five years for account information, upon the cancellation of the account.
2. At least five years for transaction records, upon the recording of the transaction.

The records mentioned in the previous paragraph concern information about the account holder or initiator of transaction, the amount deposited or withdrawn from the account, the date and time of the transaction, the source and destination of the funds, the method of transmittal or funds withdrawal, etc.

Financial institutions with branches or sub-offices shall establish and maintain a centralized database of information from their branches and sub-offices on the identity of customers, principals, beneficiaries, agents, and beneficial owners, and on all large cash transactions and suspicious transactions.

§ 1.3.9. Staff training.

Financial institutions are responsible for training their staff in the requirements of this regulation and continually updating the skills of their staff as requirements and situations change. This training should include real-world examples of transactions that constituted money laundering and terrorist financing, and an awareness of the role that staff play in the overall process of detecting and punishing money launderers and terrorist financiers.

Part D - Special rules on politically-exposed persons, correspondent banking, occasional transactions, and cross-border and domestic wire transfers.

§ 1.4.1. Politically-exposed persons (PEPs).

Financial institutions must reject PEPs as customers if they know or reasonably suspect that the wealth of the PEP may have stemmed from bribery, extortion, or other illegal activities.

The opening of accounts or the handling of occasional transactions from PEPs must be approved by the financial institution's chief executive officer or general manager.

§ 1.4.2. Correspondent banking.

Financial institutions must not open correspondent accounts at other financial institutions that are unlicensed or otherwise unregistered or domiciled in countries that have been designated by the Financial Action Task Force as non-cooperative in the fight against money laundering and terrorist financing.

Similarly, financial institutions must not open correspondent accounts for other financial institutions that are unlicensed or otherwise unregistered or domiciled in countries that have been designated by the Financial Action Task Force as non-cooperative in the fight against money laundering and terrorist financing.

Financial institutions must apply due diligence to determine whether their customer is another financial institution and, if so, to ensure that such correspondent customers are in compliance with applicable anti-money laundering laws and regulations prior to opening an account. On-going enhanced monitoring must be applied to correspondent customers.

§ 1.4.3. Occasional transactions.

Financial institutions must not carry out occasional transactions in excess of Afs 500,000 on behalf of customers who refuse to identify themselves at all or refuse to disclose and document the source of their funds.

Identification of customers who initiate occasional transactions in an amount between Afs 500,000 and Afs 1,000,000 may consist of documentation and recording of name and address only. Identification of customers who initiate occasional transactions in an amount of Afs 1,000,000 and above should include the information required when opening an account as described in § 1.3.3 above, except that the Articles of Association and board resolution of a corporation are not required, and the financial institution is encouraged, but not required, to verify the identification documents supplied.

§ 1.4.4. Cross-border and domestic wire transfers.

All cross-border wire transfers must be accompanied by accurate information on the individual or unit initiating the transfer, including name, passport number or national identity card number, and account number. In addition, if the cross-border wire transfer exceeds Afs 1,000,000, the sender must provide documentation on the source of the funds. In the absence of an account number, a unique reference number shall accompany the transfer.

All domestic wire transfers must be accompanied by the same identifying information on the initiator, unless the financial institution has or will have access to identifying information on the beneficiary. In all cases, an account number or unique reference number shall accompany the transfer.

Part E - On-site supervision and enforcement.

§ 1.5.1. Periodic examinations of compliance with these regulations.

Examination personnel of the Financial Supervision Department of DAB will conduct reviews of financial institutions' compliance with these regulations as a part of their regularly-scheduled on-site examinations. Findings by the examiners that the institution's policies are inadequate or poorly implemented will result in a low rating for the "M" component of the "CAMELS" rating system for a bank, and the possibility of enforcement action against all types of financial institutions.

§ 1.5.2. Enforcement measures.

In cases where a financial institution is found to have committed any of the following acts, the Financial Supervision Department shall request it to correct the problem within a specified period of time, and issue enforcement actions that may include license revocation, fines, the requirement of an external audit, or the removal of administrators and the replacement with administrators acceptable to DAB, as outlined in Article 40 of the AML Law and Articles 46 through 52 of the Banking Law. Violations leading to enforcement actions include, but are not limited to:

- a) Failing to set up an internal control system for anti-money laundering activities
- b) Failing to designate an AML officer.
- c) Failing to identify customers properly.

- d) Disclosing to customers or potential customers that reports are being filed about them to the FIU
- e) Failing to maintain account information and transactions records on clients, and updating the information.
- f) Failing to report large cash transactions or suspicious transactions to the FIU, as required.

In addition, financial institutions that knowingly participate in money laundering or terrorist financing, and the administrators of these financial institutions, will be punished according to the provisions of Chapter IX of the AML Law.

Part F — Effective date of regulation. § 1.6.1.

Publication in the Official Gazette.

This regulation will become effective one calendar month following its publication in the Official Gazette.