AML/CFT, and sanctions compliance summary Manual

October , 2016

ANTI-MONEY LAUNDERING AND
TERRORISM FINANCING COMPLIANCE MANUAL

Contents

Executive Summary

In 2001, the Lebanese Republic adapted the international agreement for fighting Money Laundering and Terrorist Financing. As a result on April 20, 2001, law 318 (amended by law 44 dated 24/11/2015) was issued requesting all financial institutions subjected to the provisions of the Banking Secrecy Law of September 3, 1956 to monitor their customer's operations, in order to avoid being involved in operations that might conceal the laundering of funds resulting from any of the offences specified by this Law.

Money laundering is the process of disguising or concealing illicit funds to make them appear legitimate. The crime of money laundering is defined as any person who:

1- Knowingly disguise or conceals the property or property interests obtained from a serious crime committed by themselves or;
2- Knowingly conceals, accepts, transports, stores, intentionally buys, or acts as a broker to manage the property or property interests obtained from a serious crime committed by others.

As per the Lebanese penal code, any person who undertakes money-laundering operations, or intervenes or participates in such operations, shall be punishable by imprisonment for a period of three to seven years, and by a fine of no less than twenty million Lebanese pounds.

Under the provisions of Law 44, illicit funds are defined as any asset resulting from the commission of any of the following offences:

1- The growing, manufacturing, or illicit trafficking of narcotic drugs and/or psychotropic substances according to the Lebanese laws.
2- The participation in illegal associations with the intention of committing crimes and misdemeanors.
3- Terrorism, according to the provisions of Lebanese laws.
4- The financing of terrorism or terrorist acts and any other related activities (travel, organizing, training, recruiting…) or the financing of individuals or terrorists organizations, according to the provisions of Lebanese laws.
5- Illicit arms trafficking.
6- Kidnapping using weapons or any other means.
7- Insider trading, breach of confidentiality, hindering of auctions, and illegal speculation.
8- Incitation to debauchery and offence against ethics and public decency by way of organized gangs.

9- Corruption, including bribery, trading in influence, embezzlement, abuse of functions, abuse of power and illicit enrichment.
10- Theft, breach of trust, and embezzlement.
11- Fraud, including fraudulent bankruptcy.
12- The counterfeiting of public and private documents and instruments, including checks and credit cards of all types and the counterfeiting of money, stamps and stamped papers.
13- Smuggling, according to the provisions of the customs law.
14- The counterfeiting of goods and fraudulent trading in counterfeit goods.
15- Air and maritime piracy.
16- Trafficking in human beings and smuggling of migrants.
17- Sexual exploitation, including sexual exploitation of children.
18- Environmental crimes.
19- Extortion.
20- Murder.
21- Tax evasion, in accordance with the Lebanese laws.

The Link Between Money Laundering and Terrorist Financing

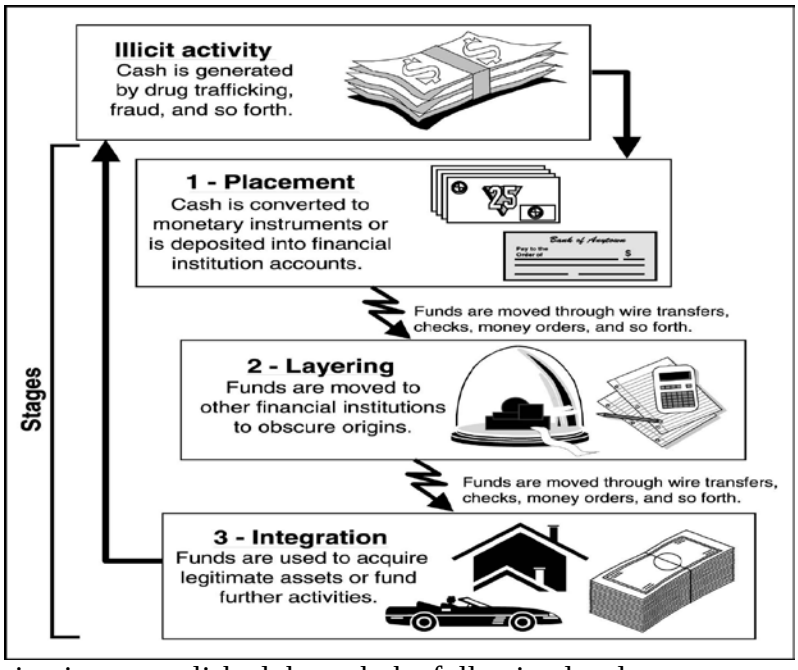
The techniques used to launder money are the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both whereas that of Money laundering is originated from criminal activities. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.
As stated under 44 mentioned above "The financing or contribution to the financing of terrorism, terrorist acts, or terrorist organizations, in accordance with the concept of terrorism as specified by the Lebanese Penal Code" is considered as money laundering predicate offenses, in this respect banks are requested to expand the scope of their AML framework to ensure that their activities are not used to finance terrorist activities.

AML/CFT Stages

Money laundering has three stages, as shown in figure 1:

- Placement: where illicit cash is converted into monetary instruments or deposited into financial system accounts.
- Layering: where the funds are moved to other financial institutions.
- Integration: where these funds are used to acquire assets or fund further activities.

Figure 1:



Terrorism financing is accomplished through the following levels:

- Collection: When the fund is collected.
- Transition: Transferring of fund from the collector to the user.
- Use of fund: The use of the collected money to execute the terrorist act.

On May 18, 2001, and under circular 83, the Central Bank of Lebanon established and published regulations setting out the rules & guidelines of the minimum control activities required to be adapted & performed by financial institutions.

Al-Mawarid Bank S.A.L (referred to as "the bank"), and in compliance with the Central Bank's regulations, adopts stringent measures that enable identifications and confiscation of any property, proceeds from, or instrumentalities used in or intended for use in the commission of any money laundering or terrorism financing offences, or property of corresponding value.

This Anti-Money Laundering and Terrorism financing manual identifies all related policies and procedures developed and adapted by the bank in compliance with the highest ethical and professional standards in addition to legal and regulatory requirements.

The manual covers:

- Guidelines on the bank's control activities for fighting Money Laundering and Terrorism financing;
- The bank's compliance structure, function, and reporting line;
- Account monitoring cycle, from the date an account is opened, covering the regular monitoring activities at the branches and the Compliance departments in addition to the reporting strategy to management and to external regulators mainly the Special Investigation Commission (Referred to in this document as SIC);

- All Central Bank regulatory circulars and internal circulars, related to Money Laundering.

All employees at the bank are required to strictly abiding by the policies and procedures stated in this manual- anyone who has been found to have assisted, been involved, or facilitated the commission of illegal activity, whether knowingly or by failure to comply with the bank's Anti-Money Laundering and Terrorism financing policies, may be subject to disciplinary action, including dismissal or legal persecution.

Compliance Policy

The board of Al Mawarid bank S.A.L is committed to utilize all its resources in order to ensure that the bank's services are not used for illegal activities or terrorism financing. In this respect, it is a must for the overall bank to abide by the policies listed below and the procedures stated within this manual in order to ensure full compliance with the local and International regulations:

1. The bank's anti-Money Laundering and terrorism financing prevention policies and procedures are based on Lebanese laws and Central Bank circulars, respecting the letter and the spirit of the FAFT and GAFI guidelines. The bank incorporates and abides by all policies set by the Central Bank, Bank Control Commission and the Special Investigation Commission related to fighting Money Laundering.
2. The bank should have an AML/CFT committee (referred to in this document as the Management Compliance Committee) whose functions and members are as defined in this document.
3. The bank should have an AML/CFT compliance unit (referred to in this document as the Compliance Unit) whose responsibilities are as defined in this document.
4. The bank shall appoint in each branch and in the back office departments, responsible for transfers and checks and lending monitoring, an AML/CFT officer (Referred to in this document as the compliance officer) whose responsibilities are as defined in this document.
5. Branch managers, branch tellers, and the bank's overall employees shall adopt the policies and procedures and responsibilities for "Fighting money laundering and terrorism financing prevention manual" as assigned in this document.
6. Any customer wishing to perform a transaction with Al-Mawarid Bank, with the exception of MoneyGram transactions, must have a single customer identification number (Customer ID). The definition of a customer ID must follow the bank's KYC policies and procedures to ensure the establishment of a complete customer file, related to every processed customer ID.
7. It is forbidden to perform any transaction for a non-customer, with the exception of MoneyGram money transfer, in which case a copy of the ID has to be obtained and the process steps outlined in this document executed.
8. It is forbidden to open anonymous/factious accounts. All account opened should follow the regular account opening procedure stated in this manual.
9. The name of all potential customers should be screened on the local SIC list in addition to all the international AML/CFT black lists (including OFAC, UN, EU and HRM) before initiating any business activity.
10. All customers must have a completed file, including information about their address, profession, income, and beneficial right owner before they obtain a customer ID number and a bank account number.
11. Customer files and database should be regularly updated as detailed in the guidelines.
12. Accounts related to exchange dealers should be approved by the Compliance committee, having the Compliance Unit approval as a must, before initiating any

business with the bank. Furthermore, exchange dealers accounts should be subject to the control procedures specified in this document where no accounts are opened unless for the purpose of shipment of the bank's excess bank notes.

13. Accounts related to offshore companies, non-profit organizations or financial institutions require prior approval from the Compliance department;
14. Accounts related to individuals or entities who are non-resident or of non-Lebanese origins (regardless if resident or non-resident) should be approved by the compliance department prior to initiating any business relationship;
15. No cash deposit is allowed on accounts related to offshore companies, non-profit organizations, non-residents, or foreign parties even in resident in Lebanon unless approved by the compliance department;
16. Cash withdrawals equal to or exceeding the equivalent of $10,000 related to offshore companies, non-profit organizations, non-residents (including Lebanese) and foreign parties (even if resident) need to be supported by a "cash withdrawal slip" with all the required clarification concerning the nature and purpose of such withdrawals;
17. Upon account opening, the bank should implement the risk-based approach strategy in determining the risks associated with the customer based on the business type, country risk, nature of requested service and expected account turnover, and relationship to the account beneficial right owner. A risk weight (Low, Medium, High) is set for each customer based on the performed risk assessment that will determine the level of customer due diligence required upon opening the account.
    The bank shall increase the KYC information level based on the determined risk weight and shall performs a periodical review of the relationship and apply a regular peer comparison among these accounts.
18. The bank has the right to request from its customers to present formal documents (Passport, Identification card, authorized signatories as specified by the bylaws for companies etc…) to validate their identity before executing transactions on their accounts.
19. Any customer that has a justified, high volume of transactions in relation to his business can be evaluated for exemption from the process steps outlined in this document.
20. Exemption from signing CTS is a process initiated by the branch, evaluated by AML/CFT compliance unit and submitted for analysis and approval by the Management Compliance Committee.
21. The Customer Exemption list should be reviewed on a yearly basis (maximum once per year), to re-evaluate the customers' eligibility for exemption during the coming period.
22. Transactions executed by CTS exempted customers should be monitored on a daily basis by the branches and the AML/CFT compliance unit. Individual or fragmented transactions exceeding the approved limits should be monitored, verified and reported in daily schedules.
23. Any transaction equal to or greater than $ 10,000 (or its equivalent in other currencies) must be executed according to the compliance process steps, outlined in this document.

24. Any transaction, including the ones mentioned below, which triggers suspicion, must be executed according to compliance process steps, outlined in this document:
    - ✓ Fragmented transactions that are equal to or greater than $ 10,000 (or its equivalent in other currencies) including foreign exchange transactions must be monitored and executed according to the compliance process steps, outlined in this document;
    - ✓ Customers making transferring or receiving sizeable amounts of money, that is considered unjustified compared to the customer's activities;
    - ✓ Customers making large or recurrent deposits unjustified by the customer's activities;
    - ✓ Customer's doing large cash deposits followed by electronic transfers or check withdrawals;
    - ✓ CTS exempted customers that witnesses change in the pattern of their cash deposits;
    - ✓ Cash deposits or incoming transfers followed by direct or multiple withdrawals;
    - ✓ Banking transactions that appear unusual considering the location of the branch;
    - ✓ Customers issuing/receiving checks or transfers to/from high risk jurisdictions.
25. Unusual transactions, including those defined under point 23 above, should be investigated in order to understand the reasons behind the operations. Reports and documents related to these investigations should be retained by the bank for a period of five years.
26. Customers, including numbered accounts, monthly transactions should be monitored at a consolidation level according to the compliance process steps, outlined in this document.
27. Related customers need to be defined on the system as group and their activities and account turnover need to be analyzed accordingly based on group level.
28. Transactions executed among accounts with direct/indirect relationship (companies, affiliates, family members, business partners, suppliers, customers, authorized signatories etc…) need to be assessed and monitor.
29. Customers' account activities are to be assessed on quarterly basis. Variations should be investigated and reported in case of doubt.
30. Transactions not in compliance with the account history or business activity need to be investigated and supported with a BRO/SOF form specifying the source of fund and ultimate beneficial right owner. In case of doubt, a suspicious transaction report should be prepared and sent to the AML/CFT compliance unit.
31. Daily Credit Card activities should be monitored in order to ensure that no fraudulent or other money laundering activities are available. Daily transactions should be compared to pre-defined limits and all excesses should be investigated and reported.
32. Daily Maintenances on Credit Card should be monitored to ensure that no internal fraudulent acts are performed.
33. Letter Of Credit should be reviewed for validation. An enhanced due diligence is required when executing letter of credits associated with high jurisdictions.

34. Any staff member that witnesses a doubtful transaction can trigger an investigation by completing the "Suspicious Transaction Form" and sending it to the AML/CFT compliance unit.
35. Any transfer/check equal to, or greater than $ 10,000 (or its equivalent in other currencies), received by Correspondent Accounts lacking appropriate justification should be blocked and escalated to the assigned compliance officer for investigation.
36. All MoneyGram transactions over $ 9,999.99 have to be approved by the MoneyGram center in Denver, USA to ensure compliance.
37. Fragmented MoneyGram transactions must be monitored even if the transaction amount is below $10,000, in compliance with MoneyGram Anti-Money laundering requirements.
38. The bank should maintain, for a period of at least five years, a record including all the information accompanying a cross-border wire transfer received from an ordering financial institution, where limitations prevent this information from being transmitted.
39. The bank must retain information on the customer, at least for five years after closing the account or ending the business relation, particularly the customer's full name, residential address, occupation and financial status, in addition to copies of all documents used to verify the above-mentioned information. It must also retain copies of all operations-related documents, for at least five years after performing the operation.
40. The bank should take sufficient measures to prevent the misuse of technological developments for money laundering or terrorist financing purposes.
41. E-banking activities need to be monitored continuously for unusual activities such as repetitive transaction requests that are not in compliance with the customer's activities.
42. The bank shall not open or maintain any relationship with shell banks.
43. The bank can maintain a relationship only with banks that are approved by the bank's Assets Liability committee.
44. Accounts related to Politically Exposed Persons (PEP), Embassies and Non-Governmental Organizations and Charities require prior approval before initiating any business relationship. An enhanced due diligence is required on such kind of customers upon opening the account and on-going.
45. The bank should maintain a clear record, if available, for transactions associated with Exchange Dealers equal to or greater than $ 10,000 (or its equivalent in other currencies). All such transactions should be supported by a special form signed by the customer stating its source of fund and purpose.
46. The bank should maintain a record of all accounts opened or maintained through power of attorney. The reasons supporting such legal commitment should be clearly explained and validated. Transactions executed on such accounts should be closely monitored.
47. Accounts held as dormant for a period of one year or above should be blocked on the system. Releasing a dormant account should be supported by a special form signed by the customer, branch supervisors and managers.

48. The AML/CFT compliance unit is required to monitor customers' transactions to ensure compliance with the bank's overall Money Laundering detection procedures.
49. The AML/CFT compliance unit is required to issue a periodic report to the Management Compliance Committee reflecting the bank's overall compliance with AML policies and stating all noted gaps in addition to the necessary recommendations.
50. The AML/CFT compliance unit shall issue monthly reports listing all cases investigated by the Unit. Should the investigation of the AML/CFT compliance unit show suspicious, such cases are to be escalated immediately to the Management Compliance Committee.
51. Doubtful transactions shall be analyzed by the AML/CFT compliance unit. Results shall be reported to the Management Compliance Committee.
52. The Management Compliance Committee shall hold periodic meetings during which:
    - ✓ Compliance policies and procedures are reviewed and modified when appropriate;
    - ✓ The Compliance Unit reports related to the bank's overall compliance with the policies and regulations related to Anti-Money Laundering- shall be discussed.

    Urgent meetings are to be held by the committee upon receiving a doubtful transaction report from the AML/CFT compliance unit.
53. The Management Compliance Committee is responsible of reporting all cases deemed suspicious, to the Special Investigation Commission at the Central Bank.
54. Periodical and surprise audit reviews are performed on the branches to ensure their application of the compliance methodology. Any violations found are reported to the Management Compliance Committee.
55. AML/CFT compliance unit has clear instructions to report any fraudulent check or credit card users to Management Compliance Committee that will report the case to Special Investigation Commission when necessary. Furthermore, the Compliance Unit needs to notify the bank's Chairman/General manager immediately when having a doubt that any transaction is related to money laundering or terrorism financing.
56. The AML/CFT compliance unit should maintain an internal list of all accounts under monitoring and perform daily and monthly reviews on their transaction and report when necessary to the Management Compliance Committee.
57. An enhanced due diligence should be performed on all Correspondent/Respondent Banks to ensure their compliance with fighting money laundering policies. Furthermore, the bank's AML/CFT questionnaire should be filled and signed by the Respondent bank's AML/CFT officers and sent to Al Mawarid Bank accompanied with their respective AML/CFT policy manual and their annual reports.
58. The bank must be fully informed of the laws and regulations governing its correspondent banks and must deal with the latter in conformity with the laws, regulations, procedures, sanctions and restrictions adopted by international legal organizations or by the sovereign authorities in the correspondents' home countries. In this respect, the bank must ensure, upon executing any cross-border operation, not to process any transaction related to a sanctioned entity or sanctioned trading business activity, tax evasion, or any other act that is considered illegal by its correspondent banks.

59. The bank shall not deal with entities or individuals subjected to international sanctions related to money laundering or terrorism financing including sanctions issued by OFAC, EU, HMT and UN;
60. The Organization Development Department must conduct semi-annual training on anti-money laundering detection techniques for all branch managers, supervisors and tellers, Correspondent Accounts Department and the AML/CFT compliance unit, as well as all back office staff of the bank.
61. It is strictly forbidden for any employee to draw the attention of any customer who is under investigation from the bank or the Special Investigation Committee unless the bank was formally notified from SIC that the banking secrecy on the account was disabled. Any employee who acts against the bank's policy in this matter will be subject to serious disciplinary action.
62. It is strictly forbidden for any employee to inform or even imply to a customer on ways to avoid signing CTS or other required forms or provide additional information supporting specific transactions.
63. The bank shall enforce, for employees' recruitment, the highest standards of honesty and integrity.

References used in this document:

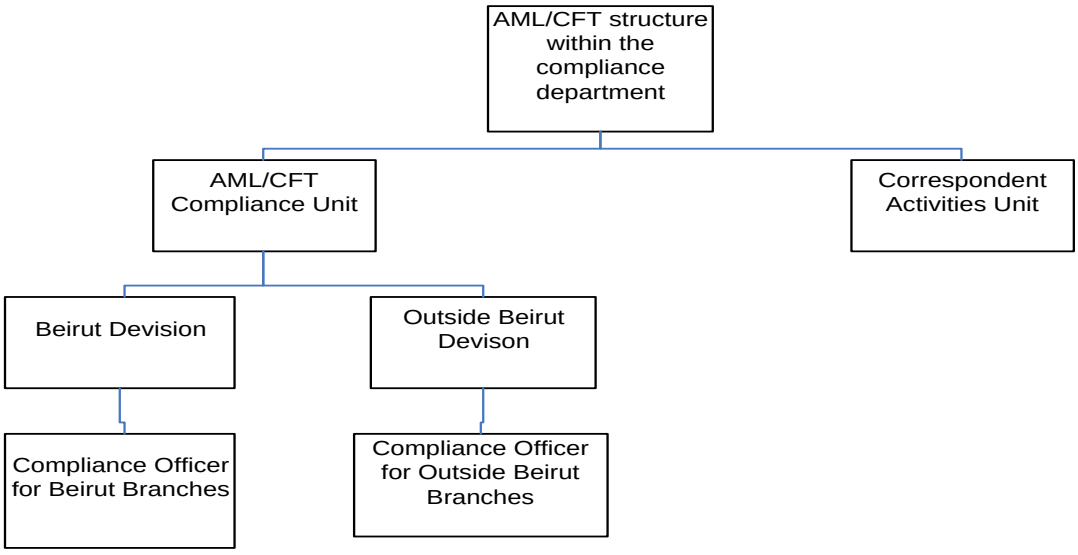
- BDL circular 83: "Control of Financial and Banking Operations for Fighting Money Laundering".
- BDL circular 126 "The relationship between banks and financial institutions and their correspondents".
- Law 44: "Fighting money laundering".
- Bank Secrecy Act/ Anti-Money Laundering examination Manual.
- MoneyGram "Anti-Money Laundering Compliance and Terrorist Financing Prevention Manual".

Compliance structure and functions

Objective: *Identify the parties involved in fighting Money Laundering and Terrorist Financing and define their needs and technical expertise.*

Based on The Central Bank's circular no. 83 article 10 "All banks and financial institutions operating in Lebanon must establish a unit to ascertain compliance with the laws, regulations and procedures in force, hereafter named "the AML/CFT Compliance Unit" and must appoint in each branch of the bank/financial institution an officer responsible for the control of operations".
Furthermore, banks must establish a special committee consisting of the Director General or any of his/her assistants, the Head of the Risk, the Director of Operations, the Head of the Internal Audit Unit, the Director of Branches, and the Head of the AML/CFT department.

Based on the above the bank established its Management Compliance Committee and AML/CFT compliance unit structured as follows:



Technical Expertise:

It is the obligation of all Compliance Officers involved in account monitoring, customer transaction review, analysis and reporting, to be familiar with all Fighting Money Laundering and terrorism financing control procedures set by the Central Bank of Lebanon and the bank's management.

All Compliance Officers should attend yearly training about the latest fighting money laundering techniques whether provided internally or by external parties.
It is the obligation of the management to ensure that all required training is provided to the Compliance officers. Furthermore, technical methods should be applied to assess the level of knowledge available among the staff involved in fighting suspicious activities.

Functions:

Management Compliance Committee:

As defined under BDL circular # 83, the members of the Management Compliance Committee are: The general manager of any of his assistants, Risk manager, Operation manager, Internal Audit manager, Branches manager, and Central Compliance manager. Whereas the committees' functions as defined under the mentioned circular are as follows:

- To prepare a procedure guide for implementing the provisions of the Law on Fighting Money Laundering and the provisions of these regulations.
- To prepare a form for customer recognition (KYC: Know Your Customer) and for controlling financial and banking operations to avoid involvement in money laundering and terrorism financing operations.
- To ascertain the proper implementation and effectiveness of the procedures and regulations on fighting money laundering and terrorism financing operations.
- To review periodically the above-mentioned procedures and regulations, and to develop them in line with up-to-date methods of fighting money laundering.
- To prepare a staff training program on the methods of controlling financial and banking operations, in accordance with the control procedure guide, and with other legal and regulatory texts in force.
- To review the reports submitted by the "Compliance Unit" and the "Internal Audit Unit" on adopted procedures, unusual operations and high-risk accounts regarding cash deposits and withdrawals, transfers, and the link between these operations and economic activities.
- To comment on the reports above and to present their assessment to the Board of Directors.
- To monitor the adequacy of exemption procedures whereby some well-known customers are exempted from filling the cash transaction slip, and also to determine the exemption ceiling and modify it according to developments in the customer's economic situation.

AML/CFT Compliance Unit:

The AML/CFT compliance Unit is made of the following divisions:
Monitoring Beirut branches: for monitoring the accounts related to Beirut branches and the private banking;
Monitoring outside Beirut branches: for monitoring the customers of outside Beirut branches;

Branch compliance officers: this division includes the compliance officers of all the branches.

The function of the AML/CFT compliance unit as defined under BDL circular # 83 and implemented by the bank is as follows:

- To ascertain that concerned officers are complying with the procedure guide on the implementation of legal and regulatory texts for fighting money laundering and terrorism financing;
- To review periodically the effectiveness of the procedures and regulations on fighting money laundering, and to propose amendments to the Compliance committee for taking appropriate decisions with the approval of Management;
- Review customer files and ensure the presence of all required documents including the KYC and BRO forms properly filled and signed by the account holder;
- Perform automatic screening for the customers' names on the Anti-Money laundering list received from SIC as well as the world check (including OFAC, EU, UN, and HRM) and inform the Compliance manager and Internal Audit about all noted cases;
- Give clearance on opening accounts related to offshore companies, non-profit organizations, non-resident accounts, and accounts related to foreign individuals or entities;
- Give clearance for accepting cash deposits from offshore companies, non-profit organizations, non-resident accounts, and accounts related to foreign individuals or entities;
- To review the daily/weekly reports received from the concerned departments and branches about cash operations and fund transfers.
- Ensure customer proper risk weight classification based on the risk-based-approach criteria and verify that the required due diligence as per the risk classification was properly performed;
- Perform quarterly review of the customer's risk weight classification, investigate variation and execute the necessary changes accordingly;
- Perform quarterly peer to peer comparison of the customer's and investigate noted variation;
- To monitor, on a consolidated basis, the customer's accounts and operations (on and off balance sheet) at the Head Office and at all branches in Lebanon and abroad;
- To investigate unusual operations, and to prepare periodical (at least, monthly) reports on operations that appear involving suspicious operations risks and submit them to the "Management Compliance Committee";
- All reports done by the Compliance unit should be maintained for a period of five years to be provided to the Special Investigation Commission when requested;
- To review Correspondent Banks' files and ensure presence and completeness of adequate AML control procedures implemented by them;
- To approve the account opening of all exchange dealers and monitor their transactions;
- Monitor the accounts of exchange dealers, if available, on a consolidated basis;
- Perform enhanced review on all activities executed through the correspondent bank to

ensure that they comply with the rules and policies applied by this last;
- To set the agenda for all the Management Compliance Committee meetings.
- To notify the bank's chairman/general manager directly in case of doubt in the involvement of any account concerning in money laundering or terrorism financing act.

Regarding each of the Divisions established within the Compliance Unit:

- To ascertain that operations control standards are implemented by the Head Office and the branches under its supervision, to ensure their compliance with AML/CFT regulations;
- The division supervising outside Beirut branches should coordinate with the division of Beirut branches when it comes to high risk accounts;
- To prepare a monthly report on the compliance of the Head Office and branches with AML/CFT requirements, and to keep this report with the Senior Management.

Correspondent Activities Unit:

For the purpose of complying with BDL circular 126 concerning the relationship with our correspondent banks, the bank has established a new Unit within the compliance department that deals with the following:

- Monitoring and providing clearance on transfers associated with high risk countries, offshore companies, non-profit organizations, private banking customers defined to be under monitoring by the Compliance department;
- Handling enquiries received from the correspondent banks concerning specific transactions or customers;
- Reviewing the overall transfers activities to identify any unusual transactions, investigate and report results to the compliance;
- Follow up on the latest international regulations, including international sanctions, and ensure bank's full compliance w.r.t to the cross-border activities performed with our correspondent banks;
- Follow up on all the transactions performed by the respondent banks and ensure full compliance with the applied AML/CFT policies and standards.

It is worth mentioning that the role of this Unit is independent from the role of the compliance officers assigned with the transfers departments and it doesn't replace the tasks assigned for the later.

AML/CFT branch Compliance Officers:

The function of the Compliance Officers at the branches as defined under BDL circular # 83 and implemented by the bank is as follows:

- Reports directly to the head of the AML/CFT compliance Unit concerning all matters related to law 44 and BDL circular 83;

- Ascertain that the branch's employees are complying with the procedure guide on the implementation of legal and regulatory texts for fighting money laundering and terrorism financing, and that the KYC forms are properly filled.
- Provide the AML/CFT compliance committee with recommendations concerning any required changes in the applied AML/CFT policies and procedures.
- Ensure screening of the names of all new customers on the SIC-AML/CFT list that includes all the names escalated from the Special Investigation commission.
- Control cash operations, transfers, and any other account-related operations, in particular those carried out through ATMs, and all other operations carried out electronically (non face-to-face banking);
- Perform when necessary the required customer due diligence based on the risk weight identified using the risk-based-approach;
- Notify the Compliance Unit through monthly reports about any suspicious operations, and about the extent of compliance of the branch with the required procedures;
- Analyze the account activities of all CTS exempted customers and ensure that regular visits are done to these customers to validate the nature of their work and to confirm that the source of funds is in compliance with the account turnover, as recommended by the Management Compliance Committee when required.
- Ensure that customers (Not exempted) are filling and signing cash transaction slip (CTS), which must include the amount involved, the source and destination of funds, and the beneficial right owner, when making a cash deposit exceeding the sum of ten thousand US dollars or its equivalent, or when carrying out multiple operations involving lower amounts but totaling more than USD 10,000 or the equivalent.
- Coordinate with the tellers on preparing schedules for transactions that exceeded the limit specified for exempted customers, and to take the necessary technical measures to maintain these schedules, in order to make them available upon request by the internal audit officers or bank auditors, or to the Special Investigation Commission.
- Ensure that no cash deposit is accepted from Offshore companies, non-profit organizations, non-resident customers, or foreign accounts (including residents) unless there is a clearance from compliance;
- Ensure that offshore companies, non-profit organizations, non-residents, and foreign customers are filling the “cash withdrawal slips” on all withdrawals exceeding the sum of ten thousand US dollars or its equivalent, or when carrying out multiple operations involving lower amounts but totaling more than USD 10,000 or the equivalent;
- Prepare, when necessary, a detailed study concerning offshore companies, non-profit organizations, non-residents, and foreign customers requesting an approval to perform cash deposit and send it to the AML/CFT compliance department and ensure proper implementation concerning the compliance recommendations;
- Bestow careful attention to checks endorsed to a third party and to bank checks that are not deposited by the first beneficiary, as well as to traveler's checks and coordinate with the required departments about checks issued by institutions in foreign countries, in addition to those in which the identity of the account holder is not specified.
- Coordinate with the relevant departments to ensure that the nature and source of fund

and the relationship between the initiator and the beneficial of all incoming or outgoing transfers that are equal to or exceed US$10,000 are properly explained, documented and in compliance with customer's business.

- Perform close monitoring concerning all transactions executed on customer accounts, exceeding or equal to US$10,000 or its equivalent in other currencies that are not in compliance with customer business or transaction history and request the customer to fill the BRO/SOF form when required to validate the source of fund for such transactions.

Branch Cashier:

The functions of the Cashier at the branches as defined under BDL circular # 83 and implemented by the bank are the following:

- Request from customers (Not exempted) to fill and sign a cash transaction slip (CTS), which must include the amount involved, Beneficial owner and the source and destination of funds, when making a cash deposit exceeding the sum of ten thousand US dollars or its equivalent, or when carrying out multiple operations involving lower amounts but totaling more than USD 10,000 or the equivalent.
- To coordinate with the branch compliance officer on preparing schedules for transactions that exceed the ceiling specified for exempted customers, and to take the necessary technical measures to maintain these schedules, in order to make them available upon request, to the internal audit officers or bank auditors, or to the Special Investigation Commission.
- Apply due care concerning setting the clearing date for all checks deposited in the accounts in order to ensure that it can't be withdrawn before being collected from the issuing bank.
- Upon accepting any cash deposit through delegation, the Branch cashier need to ensure that there is a written delegation signed by the account holder;
- Ensure that no cash deposit is accepted from Offshore companies, non-profit organizations, non-resident customers, or foreign accounts (including residents) unless there is a clearance from compliance;
- Request from offshore companies, non-profit organizations, non-residents, and foreign accounts to fill a "cash withdrawal slips" on all withdrawals exceeding the sum of ten thousand US dollars or its equivalent, or when carrying out multiple operations involving lower amounts but totaling more than USD 10,000 or the equivalent;
- Notify the branch compliance officer immediately when detecting cash deposit activities done on any account by an exchange company;
- Report to the Compliance Unit, through the branch compliance officer, about any doubtful cash deposit or suspicious checks that may involve money laundering or terrorism financing operations.

Branch Customer Service Officer:

The functions of the branch customer service officers concerning their role in fighting money laundering and terrorism financing, as defined under the bank's policies, are the following:

- To ensure completeness and accuracy of the KYC and BRO documents filled and signed by the customer;
- To ensure customer files completeness concerning all required legal documents especially in connection with accounts opened for institution and companies;
- To screen the names of all new customers on the SIC-AML/CFT list that contains all the names escalated from the Special Investigation Commission;
- Assess the legality of the power of attorney used for account opening and understand the relationship between the account holder and the proxy holder.

The Branch Manager:

The functions of the branch manager in connection to AML control acts as stated under BDL circular 83 are the following:

- To review account opening operations, to approve the exemption of certain customers from filling cash transaction slips, and to determine the ceilings of exemption, based on relevant criteria. The branch manager must also submit the names of exempted customers and the ceilings of exemption to the "Management Compliance Committee" for consideration.
- Coordinate with the Credit manager concerning the debtor accounts and their respective activities.
- To coordinate with the credit department on performing periodical visits, in person or by entrusting someone else, the debtor customers in order to understand their business and to prepare reports about creditor and debtor customers when in doubts that the movements in their accounts may conceal suspicious money laundering or terrorism financing operations, and to submit copies of these reports to the Compliance Unit.

Compliance Officers at the Back office (Operation departments):

Correspondent Account Department:

The Compliance Officer at the Correspondent Account department is responsible for the following functions:

- Monitor all outgoing/Incoming transfers especially those equal to or greater than US$ 10,000 and coordinate with the branches/Customer Accounts to verify the nature of

the transfer, source of funds, relationship between the initiator and the beneficiary, and whether the transaction is in compliance with the customer's business.

- Monitor all checks drawn on foreign banks or endorsed to third parties especially those equal to or greater than US$ 10,000, and coordinate with the branches to verify the nature of these checks, source of fund, beneficial owner, relationship between the customer and the beneficiary, and whether this is in compliance with customer's business.
- Escalate to the Correspondent Activities Unit within the Compliance department all transactions related to high risk accounts (NGO, Offshore, Non-resident or foreign accounts in addition to other accounts suspected to be associated with Sanctioned countries), for clearance prior to execution;
- Verify that the check deposited in the accounts is not cleared before being collected from the issuance bank.
- Follow up on the files related to all Correspondent Banks in order to validate their legal existence and ensure the presence of strong control processes that assists in fighting money laundering.
- Maintain all records related to the results of their enquiries on Incoming/Outgoing transfers and checks for a period of five years.
- Provide the AML/CFT compliance unit with regular reports reflecting all transactions executed and monitored.

Customer Account Department:

It is the responsibility of the Compliance Officer at the Customer Accounts department to handle the following issues:

- Verify that a proper due diligence was executed concerning all incoming transfers especially those that are equal to or greater than US$ 10,000 by coordinating with the respective branch and Correspondent Account on identifying the nature of such transfers, source of fund, beneficial owner, relationship between the customer and the sender and whether this transaction is in compliance with customer's business.
- Escalate to the Correspondent Activities Unit within the Compliance department all transactions related to high risk accounts (NGO, Offshore, Non-resident or foreign accounts in addition to other accounts suspected to be associated with Sanctioned countries), for clearance prior to execution;
- Provide the AML/CFT compliance unit with regular reports reflecting all transactions executed and monitored.
- Maintain all records related to the results of their enquiries on Incoming/outgoing transfers for a period of five years.

Operations department:

The Operations department follows up on all transfers request through e-banking where the following due diligence is performed:

- Request the call Center to verify the request of all transactions equal to or exceeding $10,000 or tis equivalent;
- Escalate to the Correspondent Activities Unit within the Compliance department all transactions related to high risk accounts (NGO, Offshore, Non-resident or foreign accounts in addition to other accounts suspected to be associated with Sanctioned countries), for clearance prior to execution;
- For other transactions, request clarification from the customer that includes the purpose of the transfer;
- Request when necessary the required supporting document validating the requested transfer;
- Transfer the request to the Correspondent accounts for execution.

Credit Admin Department:

It is the responsibility of the Compliance Officer at the Credit Administration department to handle the following issues:

- Review all the KYC documents related to corporate lending customer to ensure its accuracy and proper identification of source of fund and beneficial right owner;
- Ensure, when required, that the customer due diligence including the customer's field visits were properly reported;
- Coordinate with the AML/CFT compliance unit within the Compliance department concerning any discrepancies noted within the KYC documents;
- Send the files of all new corporate lending customers to the Compliance department for their review.

Internal audit department:

The role of the internal audit department as defined under BDL circular #83 and as stated under the bank's policies in connection with fighting money laundering and terrorism financing are the following:

- Assess the account turnover of the overall bank customers and investigate the variations encountered.
- Ensure bank's overall compliance with the Fighting Money laundering and terrorism financing manual.
- Ensure branches' compliance in connection with filling and performing periodical updates for the KYC document.
- Notify the external audit periodically concerning the noted gaps.
- Notify the Compliance Unit about the gaps noted during their audit concerning the applied fighting money laundering and terrorism financing control procedures or when having doubt in specific account or when noting any issue that constitute a major risk for the bank.

AML-CFT IMPLEMENTED PROCEDURES

CUSTOMER KYC PROCESSES

Objective: *To obtain a reasonable knowledge about the identity of the bank's customer, to ensure compliance between the account turnover and the customer's business activity, and to acquire an acceptable level of assurance that the customer is not involved in any suspicious acts.*

Implementing an effective "know-your-customers" (KYC) standards is an essential part in reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing and other unlawful activities. Setting proper KYC policies and procedures contribute to the bank's overall safety and protect the integrity of the banking system as it minimizes legal and reputation risks resulting from inadequate KYC risk management programs.

Al-Mawarid bank has enhanced its KYC control techniques in order to ensure that all branches have a detailed knowledge of their customers and their respective business, sources of funds, beneficial right owner, and expected account turnover.
In this respect all branches are required to abide by the following procedure in order to minimize the risk of any party using the bank's services for unlawful acts:

New Customers:

Branch Level:

- All new customers are obliged to complete the following documents in order to open a new account at the bank:

1- *Know-your-customer* (known at the bank as the account opening form): A document that specifies the type of account being opened and provides detailed information about the customer's identity, address, working address, family status, source of fund, purpose of the account, expected account turnover, and yearly income. It is essential that the Customer Service Officer at the branch ensures that this document is completely filled and that the address, type of business and source of funds are clearly explained and not too general. Moreover, this document should be signed by the customer as a confirmation of his approval of the listed information.

2- *Economic right owner (beneficial right owner)*: The customer needs to specify in this document if he has the economic right of the money deposited in/withdrawn from his account. This document is highly important for analysing and understanding the

relationship between the transactions executed by the customer and the business activity. In case the transactions executed by the customer were not in compliance with the source of fund declared in the KYC, the Compliance Officer needs to refer back to the economic right to verify if the account is funded by the customer himself or a third party.

In case the customer declared that the economic right belongs to a third party, then detailed information about the third party should be provided, including name, address, business activity and source of fund.
It is worth mentioning that the beneficial owner of any account can't be an entity, it should be the person with the actual control on the funds deposited in the account.

3- *Contract*: a document that specify the bank's terms and conditions concerning its relationship with the customer.

4- *Copy of customer's personal identification documents*: In case the customer is a natural person: a passport, an identity card, an individual civil registration, or a residence permit is required.
In case the customer is a legal entity: duly registered documents regarding its bylaws, its registration certificate, the identity of the person empowered to sign on its behalf, and the identity of its legal representative are required.
Information stated in the customer's personal identification documents should be reconciled with those stated in the KYC form; any variation should be investigated and immediately adjusted.

5- *Specimen of Signature*: this document includes the signature that will be used by the customer on all documents signed at the bank in the future as a result this signature should be reconciled with that on the KYC and economic right forms.

6- *For legal entities (companies and institutions)*: duly authenticated documents regarding its by-laws, registration certificate, and ownership structure, a list showing the stocks or shares distribution (directly or indirectly), a list of the persons with authorized signatures, in addition to a copy of the identity of its legal representative and the directors and natural persons who hold, whether directly or indirectly, a percentage of shares enabling them to have effective control over the company.

7- *For foreign legal entities:* The documents mentioned under point 6 above needs to be authenticated from the Lebanese embassy and ministry of external affairs in the foreign country in addition to the ministry of external affairs in Lebanon. Furthermore, the documents need to be translated to Arabic by a notary public.

8- In case the operation is performed by correspondence: an official authentication of the customer's signature on the same document or on a separate certificate. The authentication of the signature of a customer residing abroad or the verification of its

identity may be done through a correspondent or affiliated bank, or through a branch or a representative office of the concerned bank, or through another bank whose authorized signatures can be verified, provided it is subject to a good control and adopts sufficient and effective AML/CFT procedures and provided the first account-related operation is connected to an account held by the customer at a bank that is also subject to a good control and implements sufficient and effective AML/CFT procedures.

9- In case the operation was done through a power of attorney document, the Compliance Officer needs to check the original power of attorney or a certified copy thereof and fill KYC and BRO forms for both involved parties in addition to acquiring all of the above stated documents. The relationship between the account holder and his authorized representative should be clearly and reasonably explained otherwise investigated and reported to the AML/CFT compliance unit.

   The branches should maintain a register for all accounts opened or executed through power of attorney and the records should be updated regularly and flagged on the system.

10- The name of the account holder (for individual), shareholders, board member and authorized signatories (for legal entities) in addition to the name of the holders of power of attorney connected to any of our accounts needs to be screened on the bank's SIC-AML/CFT lists same as for the account holder.

The branch CSO needs to see the original documents mentioned above and the copies are to be taken at the branch where they should be stamped by "original seen" and signed.

In addition to the above, the customer will be requested to provide the bank with a series of documents depending on the type of account being opened (loan, deposit etc…) and the Customer Type (individual, joint, company etc…)

- Based on the source of fund specified by the customer, the Country risk field is specified and inputted on the system. "Country risk" is used by the bank to specify the country originating the customer's source of fund in addition to the country where the customer's business is located.

- The "Residency Code" field is specified based on the country that the customer is taking as his main residence.
- The "Customer Type" field is used to specify the type of business the customer is performing.
- The "Additional customer information" field is used to input all the additional information provided by the customer in the KYC and BRO fields.

- The "Business monitoring field" specifies the risk level associate with the customer as defined in this document (refer to the risk-base-approach section in this document).
- The "Service monitoring field" specifies the risk associated with the service provided to the customer as defined in this document (refer to the risk-base-approach section in this document).

Due to the risks associated with specific accounts or type of business, branches are required to acquire an approval from the Compliance department on accounts related to offshore companies, non-profit organization, non-residents, foreign customers, and exchange companies prior to initiating any business relationship.
In this respect, and in addition to the regular requested legal documents, the branch is requested to provide additional information to ensure that the risks are properly mitigated (refer to the sections of the exchange dealers, offshore companies, and Non-profit organizations in this document).

All customer files should be reviewed by the Compliance Officer at the branch to ensure its completeness. The file should then be sent to the Compliance Department in a period not exceeding one week from its opening date.
The customer risk weight is determined based on the following factors:

- Country risk
- Business risk
- Service risk
- Expected Account turnover
- World check

The level of required customer's due diligence is performed based on the determined risk weight.

The results of the performed due diligence is sent to the AML/CFT compliance Unit within the Compliance department for their review and feedback.

When the branch fails to perform the required due diligence on the account holder, proxy holder or the actual beneficial owner or when the results are not satisfactory, the AML/CFT compliance Unit should be immediately notified and no account shall be opened, unless a clearance was given from the Compliance Committee. Besides, the bank should consider notifying the Special Investigation Commission (SIC) and the case.

Customer name screening:

Customer screening is divided into two categories: Screening on the local SIC-AML/CFT list that is done at the branch and the Compliance department and screening on the world check (refer to Appendix A for details about the lists) that is done automatically on a daily basis at the level of the Compliance department this screening includes screening new sanctioned

names among our customers lists as well as screening new customers among the existing sanction lists.
Names appearing on the local SIC-AML/CFT list are related to people being monitoring by the regulatory entity. In this respect, banks are requested to coordinate with SIC in case any of the related names maintain an account with them. Banks are not required to terminate any businesses relationship with the names listed on the SIC-AML/CFT list without prior confirmation from SIC.
As for the world check lists, they are related to people whose decisions related to freeze of fund, assets, business relationships with them, or people already convicted with anti-money laundering or terrorism financing acts.
In this respect, Al Mawarid bank S.A.L doesn't wish to establish any business activity with parties listed on the international black list or that of the special investigation commission. Accordingly, and in case any of the mentioned parties approached the bank for opening an account, or in case the bank detected that any of the customer is dealing with a sanctioned party, the business relationship will be set on hold and the case will be escalated to the AML/CFT compliance committee in order to set the required action plan for terminating the business relationship.

Screening process:

Before proceeding with the account opening procedure, the Compliance Officer at the branch needs to screen the customer's name, or in case of legal entities the names of shareholders, authorized signatories and board members, on the SIC-AML/CFT in addition to the international sanction lists that includes all the names escalated from the Special Investigation commission. In case we have power of attorney on the account then name of the proxy holder should be screened as well.

In case the name was available on the SIC list the branch needs to communicate the matter to the AML/CFT compliance unit and forward them the file without notifying the customer about anything. The AML/CFT compliance unit will inform the Internal Audit, Management Compliance Committee and the bank's chairman/General manager about the noted case where a letter will be sent from the bank's management to SIC notifying them about the new customer and act based on their recommendation. The branch is not authorized to close the account before receiving any confirmation from Compliance committee.
The AML/CFT compliance unit will flag this customer as "watch" on its records in order to monitor closely all future transactions.
In case the customer was listed on OFAC, EU or UN the account opening procedure shall be immediately stopped and no relationship is established with the mentioned party.

As a second control, on a daily basis a list of all newly opened IDs is uploaded to our screening system and all hits are reported to the AML/CFT compliance unit for assessment. In case the positive hit was related to the SIC-AML/CFT list then the AML/CFT officer will verify that it was reported by the branch compliance officer on the previous day otherwise escalate to the compliance committee as per the process stated above.

In case the positive hit was reported on any of the international black lists, the AML/CFT officer reports the case directly to the members of the AML/CFT compliance committee through the compliance manager. The risk associated with the mentioned account is assessed taking into consideration that Individuals or entities sanctioned by OFAC, UN, EU and HRM are considered by the bank as undesirable customers where no business relationship should be maintained with them. The branch will be notified about the committees decision and act accordingly. The account will be immediately closed and delivered to the customer at the level of the back office.
As stated above, and during the end of day process, new sanctions are automatically screened on the lists of our customers.
On a daily basis a compliance officer at the compliance department, review the hits provided by the system in order to assess whether they are related to any of our customers and report the issue to the Head of AML-CFT Unit and the Compliance manager. The compliance manager should immediately notify the compliance committee and the bank's chairman about any sanctioned customer where a decision is taken immediately to terminate the business relationship and close the account.

Legal compliance unit:

The Legal compliance unit within the compliance department is the entity responsible for reviewing the customer's file and coordinate with the AML/CFT Unit concerning any noted issues or discrepancies.
The mentioned unit should extract a daily report reflecting all newly opened accounts and ensure that their respective files are received in a period not exceeding one week from the date of opening. Once received, the Compliance Officer at the Unit needs to review the files to ensure completeness and accuracy of documents by verifying that the KYC, and BRO are clearly filled and signed by customers, and that the specimen of signature and the ID copy are available in addition to the all other required documents.

The Unit will validate the determined customer's risk weight and ensure the AML/CFT unit was notified about all the due diligences performed on those classified as high risk.

In case the customer was related to other accounts at the bank, either directly or indirectly, the related accounts need to be flagged on the system as group. In this respect, the Compliance unit shall identify the group code on the system and send it to the "Operations" department for execution on the system.

In case the account was opened in a geographical area that is different from the customer's work or living location, the Compliance Unit has the right to request the branch to enquire about such a matter.

Finally, the legal compliance unit will verify that the customer's name screening was performed at the branch level and through the daily automated screening processes.

In case the legal compliance noted discrepancy in the file that requires adjustment, it will be returned to the branch and flagged on the system as "Incomplete file" where they follow up till the reported discrepancies are cleared.

Incomplete files include the following:

- Missing specimen;
- Missing copy of customer's ID;
- Missing or unclear customer related information: personal details, residence details, job details, financial information, source of funds, Beneficial right owner;
- Missing legal documents (example: documents related to non-individual accounts, proxies etc…);
- Missing FATCA documents;
- Missing signature.

Once the file is controlled, and in case no issues or discrepancies were noted, it will be sent to the "Customer database maintenance" unit to input all the customer information stated in the KYC in addition to the customer final risk weight on the system and to flag it on the system as "Complete file". All inputted information is subject for review in order to confirm their accuracy. Once the information is controlled, the files will be sent for scanning and archiving.

Old Customers:

All customer accounts should be supported by an existing KYC. In this respect, the bank should perform a periodic review on all its files to verify the ones that requires renewal. The branches should be notified about the specific information required per file to execute the file update process. In this respect, file update starts by contacting the customers and requesting them to pass by the branch and renew the file.

The compliance department- Legal Unit should follow up with the branches on all accounts that require renewal or that are considered from compliance perspective as incomplete.

Files related to accounts classified as high risk/medium should be reviewed at least every 1-2 years respectively.

The following indicators require immediate update for the customer's file:

- Drastic change on the account turnover;
- Detection of doubtful transaction;

The Legal compliance Unit must on a periodical basis, at least quarterly, provide the branches with lists of the files that require renewal or those are incomplete and follow up with them in order to ensure full compliance.

The Legal compliance Unit

Any enquiry request received from the SIC should be communicated to the Internal Audit, Cards Unit and the AML/CFT compliance unit. The AML/CFT and Cards Units should verify whether the customer's name is reported on any of our systems.
In case the name subject for enquiry was the bank's customer, the account should be immediately reported to SIC through the bank's management and his name should be flagged on the AML/CFT compliance unit "watch" list for monitoring. All reported cases by SIC should be recorded on the SIC-AML/CFT list, it is the function of the Compliance Unit to ensure that the list is updated regularly.

Furthermore, on a weekly basis all existing customers are screened on the daily updated international black lists as a search for latest sanctions related to existing customers. Accounts with positives hits will be set on hold and the case will be escalated to the AML/CFT compliance committee as per the process explained above.

The department should maintain account "watch" list related to all closely monitored accounts including the following:

- Accounts reported by SIC.
- Accounts reported to SIC.
- Accounts under monitoring reported to the Management Compliance Committee.
- Customers classified according to the risk-base approach as highly risky.

The bank should maintain the documents related to the customer files for a period of at least 5 years after the date of business termination with the customer.

All files related to closed accounts are to be kept for a minimum period of 5 years. The files and all accompanying documents should be stamped "Closed". Finally, closed account should be blocked and closed on the system to reflect the existing facts.

CUSTOMER ENHANCED DUE DILIGENCE

Objective: *Assessing the value of information provided by the customer in connection with his KYC and BRO forms in connection with the account turnover to ensure that the bank possesses sufficient customer information...*

At account opening, the bank should obtain information sufficient to develop an understanding of normal and expected activity of the customer's occupation or business operations. In this respect, Customer Due Diligence is required in order to address various

concerns related to customer's overall risk weight such as high expected account turnover, or to ensure compliance between the available account turnover and the customer's source of fund.

The bank may determine that a customer poses a high risk because of his business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving high-risk jurisdictions (refer to the risk-base-approach section of this document). If so, the bank should consider obtaining, both at account opening and throughout the relationship, documents that will validate and explain the purpose of the account, source of funds and wealth and customer's occupation or type of business.

Customer Due Diligence is the responsibility of the branch's Compliance Officer and is performed based on customer's determined risk weight upon account opening, account analysis, or a request from the AML/CFT Compliance Unit or the compliance committee. It can take place when the account is initially opened and is usually requested when the declared source of fund implies high future turnovers, when the account is categorized among those classified to be of high risk, or when the information provided by the customer doesn't reconcile with the potential turnover.

Customer enhanced due diligence account for the following factors:

- Obtaining additional information on the customer by either requesting additional documents clarifying his/her net worth or business or by performing a market enquiry or media screening;
- Requesting documents validating the nature of the transactions performed on the account;
- Increase the frequency of file updates;
- Enquiry and media screening concerning the customer's suppliers and clients;
- Conduct customer site visits;

When the branch manager and compliance officer, performs a site visit to the customer, it is highly important that the purpose and the reason of this visit are not communicated to the customer in order not to raise any doubt. The bank's team should monitor the customer's business activity (example: number of customers visiting the field during the visit, type of activities performed etc...) and analyse the account turnover based on the information gathered to ensure compliance.
The team should acquire from the customer some documents that can validate the account turnover. These documents are to include updated financial statements, list of suppliers, copies of latest sales and purchasing invoices, list of suppliers and customers...

A field visit report should be prepared stating all noted facts and including the following:

- Date of field visit.
- Location.
- The customer's residence, place of employment, or place of business to the bank.
- Number of branches (local and foreign) and approximate number of employees.

- Description of the customer's primary trade area and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume, and total sales, and a list of major customers and suppliers.
- Explanations of changes in account activity.
- Name of major suppliers and customers with whom the bank's customer performs business with.

Customer enhanced due diligence should be implemented on all accounts falling under the high risk profile, including but not limited to: Private banking account, Financial institutions, Non-profit organization, and Offshore companies, PEP, and accounts related to non-residents who requires a compliance approval prior to initiating the business relationship.
The AML/CFT compliance unit should check the provided report and analyse the data to verify and validity its compliance with the customer's account turnover.
The Compliance Unit, shall collect additional data from our information reporting agencies and request the information department to conduct investigations with other banks, taking into consideration and respecting the banking secrecy laws.

In case the results were not satisfactory, no relationship should be established with new customers, as for existing ones, the Compliance Unit should consider prepare a Suspicious Investigation report and raise it to the Management Compliance Committee for review and recommendation.

CORRESPONDENT BANKS DUE DILIGENCE

Objective: *Ensure adequacy of the bank's systems to manage the risks associated with offering correspondent account relationships. Ensure the bank's compliance with statutory and regulatory requirements for correspondent accounts for foreign shell banks.*

Banks maintain correspondent relationships at other domestic and foreign banks to provide certain services that can be performed more economically or efficiently because of the other bank's size, expertise in a specific line of business, or geographic location. Such services may include deposit accounts, fund transfers or other minor services as foreign currencies exchange or facilitating secondary market loan sales.

It is essential for Al Mawarid Bank to ensure the physical presence of its correspondent bank and that it is not dealing with Shell Banks. The banks should verify that all its correspondent/Respondent banks have effective internal control procedures related to fighting Money Laundering and terrorism financing acts in order to minimize all risks that can result from such a relation.
Furthermore, the bank should ensure that its correspondent bank has reliable procedures applied for identifying their customers, understanding their source of fund and nature of business and validating their identity.

Because domestic banks must follow the same regulatory requirements, risks in domestic correspondent banks are minimal in comparison to other types of financial services; however transactions through the account, which may be conducted on behalf of the respondent's customer, may be high risk.
As for foreign banks, some institutions are not subject to the same or similar regulatory guidelines as the Lebanese banks; therefore, these foreign institutions may pose a higher money laundering risk to the bank. Without adequate controls, Al-Mawarid Bank may set up a correspondent account with a foreign financial institution and not be aware that this last is permitting some customers to conduct transactions anonymously through the bank's account (example: nested accounts).

In this respect, it is important that the bank's management (mainly represented by the Executive and ALCO committee) clearly state and define the following issues:

- Names of the approved correspondent banks that the bank is allowed to do business with.
- Intended use of the accounts, expected account activity and maximum allowed limit for the daily outstanding balance.
- Understand the foreign correspondent financial institution's relationship with other correspondent.
- Assess the risks posed by the foreign correspondent financial institution relationships.
- Establish criteria for opening and closing the foreign correspondent financial institution account.

In order to ensure physical presence and effective applied internal control procedures for fighting Money Laundering activities in the correspondent bank, the bank should ensure receiving the following documents:

1- Certifications/ License: Correspondent banks should be registered in their own country and maintain records identifying their main owners and top management. Names should be reconciled against the bank's applicable AML watch lists.
2- Address: The bank should maintain the correspondent bank's detailed address.
3- Swift initiation documents: swift initiation documents can be considered as an essential document that validates the existence of the correspondent bank.
4- AML/CFT policy manual: The bank should receive a copy about the correspondent bank's AML/CFT policy manual, review it and ensure that it complies with the bank's policies. Moreover, the bank should enquire about the AML/CFT officer assigned at the correspondent bank. The Compliance Manager has all the right to contact the AML/CFT officer of the correspondent bank for any clarification concerning the applied AML/CFT policies.
5- AML questionnaire: All correspondent banks are required to fill the bank's AML/CFT questionnaire that clarify and verify the correspondent bank's compliance with the required fighting money laundering and terrorism financing policies and regulations. Moreover, the questionnaire tends to reveal if the correspondent bank is subject to external review from its regulators and about whether it was ever directly

or indirectly involved in Money Laundering or terrorism financing cases. Moreover, the document tends to verify if the correspondent bank's employees are provided with regular training to ensure awareness about Anti money laundering and terrorism financing policies.

6- Annual report: The bank should acquire the correspondent bank's annual report including the audit report in order to verify that the bank is not violating serious policies and facing a going concern problem that will affect its relation with Al-Mawarid Bank.
7- Information concerning the products and services provided by the correspondent bank, in addition to information about their customers' base, industry, country of residency and operations.

The bank should review all acquired documents/information for reasonableness and accuracy in order to acquire assurance with respect to the following:

- That the correspondent bank is prohibited from dealing with shell banks;
- That the correspondent bank is not providing access to third parties on the bank's account without prior permission and;
- The risks associated with the correspondent bank's customers, products are services are clearly identified and mitigated.

The bank should evaluate the quality of the information received to ensure that sufficient internal controls are maintained by the correspondent bank. If the bank at any time knows, suspects, or has reasons to suspect that any information contained in any received document, or any information is no longer correct, the bank must request that the foreign bank verify or correct such information, or take appropriate measures to ascertain its accuracy.
It is the function of the Compliance Unit to ensure that the above set procedures is properly implemented, all noted gaps should be reported to the Management Compliance Committee.

RELATIONSHIP WITH SPECIFIC ENTITIES

EXCHANGE DEALER

Objectives: *Ensure that the bank's relationship with its respective Exchange dealers customers are not used directly or indirectly as a cover of illegal activities and money laundering acts.*

Based on the bank's internal policy, the relationship with exchange dealers is limited to the shipment of the bank's excess bank note services. Any Exception should be approved by the compliance committee and the AML/CFT compliance unit and should be subjected to the following conditions:

- No account can be opened at the bank in the name of an exchange company in case any of the shareholders, executive managers, authorized signatories, or any of their direct families (parents, wives, husbands, and children) has an account with the bank;
- It is strictly forbidden for the shareholders, executive managers, authorized signatories, or any of their direct families (parents, wives, husbands, and children), of an exchange company to execute transactions related to their exchange business on their personal accounts;
- When a bank accepts a check drawn on it by a money exchange institution, or when it executes a banking transaction requested by a money exchange institution in favor of one of its customers, whether directly or indirectly, and when the value of the check or transaction exceeds USD 10,000 or its equivalent, the said bank must receive a signed notification from the exchange institution specifying whether the transaction was carried out by the money exchange institution in exchange of funds received in cash or not, as well as about the source and destination of funds, and the identity of both the beneficiary and the beneficial owner;
- The bank can't exchange money with any exchange company unless it had an account at the bank;
- In case an exchange company requested a checkbook, the bank needs to ensure that all printed checks have the statement "Paid to first beneficiary";
- The bank can't accept any check deposit in the account of an exchange dealer unless it was issued to the first beneficiary;
- The bank should not execute and transfer transaction requested by an exchange company if the beneficiary was a third party;
- The bank can't accept cash deposits in its customer's account if their source was an exchange company;
- The bank can't accept any power of attorney from any of its customer in the favor of or to the favor of an exchange company;
- The bank can't execute any transfer exceeding $1500 requested by an exchange company on behalf of third parties;
- The bank can't open any fiduciary account in the favor of exchange company customers;
- When the exchange company requests to perform outgoing transfer against money collected from exchange transaction or against money transports, the bank need to ensure getting the form specified above supporting such transfer regardless the amount;
- The bank should notify the Central Bank in case the exchange company failed to provide with the transactions forms mentioned above.

It is important to ensure that the bank's services are not used by any exchange institution directly or indirectly to launder illicit money. In this respect, the bank should clearly identify all its exchange dealer customers and flag their transactions and monitor them to ensure safeguarding of transaction.

Furthermore, the AML/CFT Compliance unit should perform a customer due diligence on available Exchange Dealers' accounts held with Al-Mawarid bank S.A.L., the due diligence should include a field visit to the customer when required, acquisition of all legal documents

that validate the legal existence of the business, in addition to copy of the company's license. Moreover, the bank should acquire and review the Anti-Money laundering and terrorism financing policy manual applied by the exchange company. In case of absence of policy manual for fighting money laundering, the bank has the right to conduct meetings with key persons to ensure the presence of effective control procedures implemented to ensure protection from money laundering acts.
The bank should request from its exchange dealer customers to fill the AML/CFT questionnaire; for the purpose of analyzing the effectiveness of the control processes implemented by the exchange dealers.
Below is a list of the legal documents required from exchange companies:

- BDL license.
- Copy of the commercial certificate dated not more than three months.
- Copy of the commercial circular dated not more than three months.
- Copy of company's bylaws.
- Copy of the last board of directors and general assembly minutes of meeting.
- Copy of the last report issued by the special investigation commission on the company.
- Copies of the authorized signatories ID.
- Copy of the company's compliance officer's personal resume.
- All additional documents required from legal entities as stated under the "Customer KYC processes" section of this document.

In case of lack of cooperation, the bank has the right to terminate the relationship with the customer and report this matter to the Central Bank of Lebanon.

All noted gaps or suspicious activities should be investigated and reported to the Management Compliance Committee for feedback and recommendation.

FINANCIAL INSTITUTIONS

The bank is allowed only to deal with licensed financial institutions. In this respect, when opening any account for a financial institution the bank needs to perform the following due diligence on the account:

- Request the documents, stated under the KYC section for legal entities, in order to validate the company's legal existence.
- Ensure that the institution was licensed by the regulatory authority in the country of Operations.
- Ensue that the institution is not a shell company.
- Ensure that the company has assigned a dedicated Compliance officer and acquire copy of his C/V to validate his qualifications in AML/CFT area.

- Validate that the company has applied policies and procedures related to fighting money laundering and terrorism financing by acquiring copy of their AML/CFT manual and reviewing it to verify its effectiveness.
- Ensure that the company has defined a clear process in order to acquire information related to its customers, source of fund, and nature of business and to reconcile such information with their account behavior.
- In case of a Lebanese financial institution:
    - Ensure that the internal policy clearly restrict cash deposits activities of their customers' accounts.
    - Ensure that the company doesn't perform any of the activities related to exchange dealers including transport of money.
    - Ensure that the company doesn't perform any function other than the ones specified by the central bank for the financial institutions.
    - Ensure that the company's internal policies clearly states that no transfer above $1500 can be performed based on the request of any of its customers to a third party.

The bank should closely monitor the accounts of the financial institution in order to ensure compliance with the applied laws and regulations. In the review revealed gaps that constitute risks on the bank's operations, the Management Compliance Committee has the right to terminate the business relationship with the mentioned institution or temporary freeze it till the customer perform the required adjustments in their applied procedures in order to clear the noted gap.
Since Lebanese financial institutions are not allowed to accept cash deposits from their customers, the bank shall not grant any financial institution holding an account at Al-Mawarid Bank S.A.L a CTS exemption.

OFFSHORE COMPANIES

Objective: *Ensures that the risks associated with accounts of offshore companies and charities are adequate.*

Offshore companies are associated with several compliance risks as those related to tax evasion or sanctions. An offshore company might be involved in trading activities falling within the sanction programs and as a result subject the bank to violations of the international trading restrictions set on certain countries. In this respect, it is essential for the bank to implement an enhanced due diligence on its offshore companies to ensure that all risks are properly addressed.
Opening accounts for offshore companies at the bank requires prior approval from the compliance department. In order to open the account, all the necessary KYC information concerning the shareholders, beneficial right owner, and country of operations and nature of business should be obtained.

The following legal documents are required as well. In case of a foreign offshore company, the documents should be authenticated by the Lebanese commercial registry office, and translated into Arabic by a notary public:

- Duly authenticated documents regarding its by-laws,
- Articles of association,
- Registration certificate,
- Annual Ordinary General Assembly Meeting Minutes,
- Board of Directors Meeting Minutes,
- Ownership structure,
- A list showing the stocks or shares distribution (directly or indirectly),
- A list of the persons with authorized signatures,
- Copy of the identity of its legal representative and the directors and natural persons who hold, whether directly or indirectly, a percentage of shares enabling them to have effective control over the company,
- Nature of business and source of income.
- Shareholder's biography.

Having obtained the above information and legal documents, the file is escalated to the compliance department where the information and documents are reviewed for validity. The compliance department may further request proof of business, such as certification that verifies the company's country of operation.

For existing companies, information is required about their previous transactions, including documents such as bills of lading and signed contracts as proof of locations where the company is operating. In the case of new companies, the compliance department should review information such as the company's business assessments, feasibility studies, obtained contracts, and lists of potential clients.

In addition to the above, the department also conducts a name screening process on the names associated with the company, including its shareholders, authorized signatory/signatories and associated parties (major customers, suppliers,…), as well as the type of business and countries of operation, to ensure it is not operating on behalf of third parties or is related to countries and activities subject to sanctions.

Based on the provided case, the compliance department has the right to request proof of existence of the company such as a rent contract or registration of premises and offices either rented or owned, or a list of employees. If the head office or premises exist in Lebanon, the compliance department can also request a site visit.

Based on the compliance department's risk assessment, one of the following recommendations is issued:

1- Clearance to open the account.
2- In case of lack of enough information, or the need for additional documents, the compliance department my postpone the decision till additional information or documents are submitted,
3- Reject to open the account.

Following the account opening, continuous monitoring of the account is undergone at several levels of the control process whereby supporting documents are requested in order to validate information such as the purpose and destination of funds, and the country of operations. Transactions are also subjected to prior enhanced due diligence, including the request of supporting documents such as signed contracts.

NON PROFIT ORGANIZATION

Objective: *Ensures that the risks associated with accounts of non-profit organizations (NPO) and charities are adequate.*

NPOs are private nonprofit organizations that pursue activities intended to serve the public good. NPOs provide several social services in one or more of the communities that the NPO operates. An NGO can be any nonprofit organization that is independent from government.

NPOs can range from large regional, national, or international charities to community-based self-help groups. NPOs also include research institutes, churches, professional associations, and lobby groups. NPOs typically depend, in whole or in part, on charitable donations and voluntary service for support.

Risk Factors

Because NPOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NPO can be complex, making them susceptible to abuse by money launderers and terrorists. The U.S. Treasury issued guidelines to assist charities in adopting practices to reduce the risk of terrorist financing or abuse.

Risk Mitigation

To assess the risk of NPO customers, a bank should conduct adequate due diligence on the organization. In addition to the regular required customer identification procedure, due diligence on NPOs should focus on other aspects of the organization, such as the following:

- Purpose and objectives of their stated activities.
- Geographic locations served (including headquarters and operational areas).
- Organizational structure.
- Donor and volunteer base.
- Funding and disbursement criteria (including basic beneficiary information).
- Recordkeeping requirements.
- Its affiliation with other NPOs, governments, or groups.
- Internal controls and audits.

For accounts that bank management considers to be higher risk, strict documentation, verification, and transaction monitoring procedures should be established. NPO accounts that are at higher risk for AML/CFT concerns include those operating or providing services internationally, conducting unusual or suspicious activities, or lacking proper documentation. EDD for these accounts should include:

- Evaluating the principals.
- Obtaining and reviewing the financial statements and audits.
- Verifying the source and use of funds.
- Evaluating large contributors or grantors of the NPO.
- Conducting reference checks.

PERFORMING INVESTIGATION ON DOUBTFUL TRANSACTION

Objective: *Ensure that all suspicious cases are detected immediately and investigated in order to avoid having illicit money laundered through the services of Al Mawarid Bank.*

Transaction investigation can be triggered based on several factors:

- Transactions identified by the branch;
- Transactions identified by the AML-CFT unit when performing transaction of account monitoring/review;
- Regulatory instructions.

Doubtful transactions triggered at the branches should be reviewed and monitored by the branch compliance officer. The first action should be to perform additional investigation such as enquiring about details of the transaction such as the purpose, the relationship between our client and the parties involved in the transaction, the ultimate beneficial owner, and the source of funds. The branch can request from the customer additional documents validating the account turnover. In case the outcome of the investigation was negative, a "Doubtful transaction" slip is prepared signed and sent to the AML/CFT compliance unit. The branch should clearly states the reasons leading to the doubt and the investigation that was performed.

The AML/CFT compliance unit should apply the following approach to all doubtful cases raised whether triggered by the branch, SIC or by the department itself:

- The file of the customer subject to investigation should be requested in addition to the statement of all his accounts covering a period of minimum one year.
- The Compliance Unit shall review the file in details to understand the customer's source of funds in addition to the beneficial owner of the funds deposited in the account subject of the investigation. The department will request the opinion of the

branch manager concerning the customer under investigation and the information provided by the branch should be reconciled with that available in the file.

- All executed transactions performed by the customer are categorized according to their type and checked for compliance with customer's source of fund. Moreover, the variation in the account behavior compared to the nature of business of the customer should be closely monitored and reviewed.
- Analytical testing should be done to forecast an expected turnover of the account behavior, based on the declared source of fund and business type, and compared it with the actual transactions executed on the account.
- Customer's transactions should be checked in details to gather information about various parties that the customer may be dealing with, repetitive transactions done with specific parties should be subjected to further assessment where the bank should try to acquire further information about those parties, their relationship with our client, whether they are subject to any sanction in addition to the nature and purpose of the transactions executed with between them.
- The department should seek the help of the Information department to gather additional information about the customer subject of the investigation in order to assist in finalizing the decision.
- Media screening should be done as well on the customer to either identify information than can highlight additional risks associated with the customer or can validate the customer's business activities or financial situation.
- Based on the collected data the AML/CFT Compliance Unit can send the branch addition enquiries to answer or actions to take (such as performing a field visit to the customer's business).

Based on the above, and in case the Compliance department failed to validate the account turnover, a report needs to be prepared stating all the noted facts with the necessary recommendation and sent to the Management Compliance Committee for their review and feedback.

The Compliance Committee shall review the report received from the AML/CFT Compliance Unit and ask for a meeting to discuss all noted facts. Based on the recommendation of the committee one of the following decisions should be made:

- Request the Compliance Unit to investigate a specific item or area that was not covered in its report.
- Request the Information department to perform additional search about the customer.
- Request the branch to provide additional documents or information in order to validate the existence of his business.
- Confirm the doubt and report the account to the Special Investigation Commission for their feedback and recommendation without closing the account (due to the local policies).

Based on BDL circular 83, banks report to the Governor of the Central Bank for being the president of the Special investigation commission about noted suspicious case when any of the following applies:

- When it has persistent doubts about the credibility of the written statement submitted by the customer regarding the identity of the economic right owner, or when it discovers that false information has been given on the identity of the said owner.
- When it realizes that it was misled in the course of checking the customer's or the economic right owner's identity, while having persistent, serious and precise doubts about the information provided by the customer.
- When transferred amounts or checks are returned, whether directly or upon the request of concerned parties, particularly correspondent banks, either because of forgery or because of doubts that they involve suspicious operations.

The AML/CFT compliance unit should ensure that the decision of the Committee was followed and respected.

Any further information requested from the Special Investigation Commission should be reviewed by the members of the compliance committee before being sent.

CUSTOMER RISK-BASE APPROACH

Objective: *Ensure the adequacy of the bank's system to manage risks associated with customers whose profession or countries are classified as risky, and manage the ability to implement effective risk-based due diligence monitoring and reporting system.*

As stated under BDL circular 83 " Banks adopt a risk-based approach to classify customers and transactions in accordance with the level of risks, low, medium and high, while taking into account, for indicative purposes but not restrictively, the following risks: Customers, Country risk and Service risk".

Risk based approach start by performing a risk assessment that tends to assist the bank in identifying the threats associated with Money laundering and Terrorism financing. Once these threats are identified the bank can set risk mitigation criteria that tend to address these threats upon account opening.
In this respect, the bank has performed an internal risk assessment on the customer's portfolio and identified the following factors that affect the risk weight for each customer:

- Customer/Business risk
- Country risk
- service risk

Customer risk

Based on our performed risk assessment, the bank has defined the following type of customers that carries an increased ML/TF risk:

Description	Risk Weight
Politically exposed Person, Embassies Ambassadors, diplomatic representative and their staff	HIGH
Money service Businesses: Exchange dealers, money remitters, etc…	HIGH
Gaming and lottery businesses.	HIGH
Dealers in high value commodities: gold, jewels, antiques,	HIGH
Restaurants and night-clubs.	HIGH
Real Estate companies	HIGH
Car and Vehicle dealers	HIGH
Off-Shore Companies	HIGH
Customers dealing through intermediaries (proxies etc…)	HIGH
Gas stations	HIGH
Non-governmental organizations	HIGH
Insurance companies	HIGH
Petroleum Companies	HIGH
Bearer Shares Companies	HIGH
Credit Counter	HIGH
Financially exposed persons	HIGH
Firms with sleeping partners	HIGH
High net worth individual	HIGH
Customers involved in businesses with volatile source of fund: - Professional service providers (lawyers, custom officers). - Medical field. - Travel agencies	MEDIUM
Retail stores (volatile and cash intense businesses)	MEDIUM
Stock brokerage	MEDIUM
Telecommunication trading	MEDIUM
Salaried employees whose salary structures are well defined	LOW

Government Departments and Government owned companies, regulators and statutory bodies	LOW
OTHERS	LOW

In addition to the above, the following factors need to be accounted for when assessing the customer's risk:

- Account activities: the more complex the account activity the higher the risk. Accounts with volatile turnover especially those affected by seasonal factors or that involves high cash and checks activities, tend to be difficult to monitor as the account performance cannot be easily determined or analytically assessed. In this respect, the customer risk weight need to account for the overall account activities as additional enhanced due diligence is required by the bank.
- World check: Account screening is another important factor that can affect the customer's overall risk weight. Customer screening accounts for checking information of the customer on the international black list, local list, in addition to media screening and PEP list. Available information can automatically increase the customer's overall risk to high or even undesirable.

Country or Geographical risk

Country or geographical risk may arise because of the location of a customer, the original destination of the transactions of the customers, or because of the business activities of the entity itself, its location and the location of its organizational units.
The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing may include different criteria. Factors that may indicate a higher risk are:

- Countries or geographic areas subject to sanctions, embargoes or comparable restrictive measures issued, for instance, by the US treasury, FINCEN, United Nations, or the European Union.
- Countries or geographic areas identified by credible sources (e.g., the FATF, the IMF or the World Bank) as lacking an appropriate system of preventing money laundering and/or terrorism financing.
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity or known for tax avoidance.

In addition to the above, the following elements should be accounted for when setting the risk weight associated with each country:

- The strictness of laws on fighting money laundering and terrorism financing, and the

efficiency of the regulatory and judiciary authorities in charge of their implementation.

- The existence of banking secrecy.
- The situation of the country regarding corruption and organized crime.

In this respect, the bank will rely on the yearly report issued by the "US treasury- Bureau for International Narcotics and Law Enforcement Affairs", "The corruption perception index", in addition to the list of countries known to be as tax haven.

In this respect, the following countries were defined as low, moderately and high risky:

Country	Risk Level	Country	Risk Level
Afghanistan	High	Dominica	Medium
Albania	Medium	Dominican Republic	High
Algeria	Medium	Ecuador	Medium
Andorra	Low	Egypt	Medium
Angola	High	El Salvador	Medium
Anguilla	Low	Equatorial Guniea	Low
Antigua and Barbuda	High	Eritera	Low
Argentina	High	Estonia	Low
Armenia	Low	Ethiopia	Low
Aruba	High	Fiji	Low
Australia	High	Finland	Low
Austria	High	France	High
Azerbaijan	Medium	Gabon	Low
Bahamas	High	Gambia	Low
Bahrain	High	Georgia	Low
Bangladesh	Medium	Germany	High
Barbados	High	Ghana	Medium
Belarus	High	Gibraltar	High
Belgium	Low	Greece	High
Belize	High	Grenada	High
Benin	Medium	Guatemala	High
Bermuda	Low	Guernsey	High
Bolivia	High	Guinea	High
Bosnia and Herzegovina	Low	Guinea-Bissau	High
Botswana	Low	Guyana	Medium
Brazil	High	Haiti	High
British Virgin Islands	High	Holy See	Low
Brunei	Low	Honduras	Medium
Bulgaria	Low	Hong Kong	High
Burkina Faso	Low	Hungary	High
Burma	High	Iceland	Low
Burnudi	Low	India	High
Cabo Verdi	Low	Indonesia	High

Country	Risk Level	Country	Risk Level
Cambodia	High	Iran	High
Cameron	Low	Iraq	High
Canada	High	Ireland	High
Cayman Islands	High	Isle of Man	High
Central African Republic	High	Italy	High
Chad	Low	Jamaica	Medium
Chile	High	Japan	High
China, People Rep	High	Jersey	High
Colombia	High	Jordan	Medium
Comoros	Medium	Kenya	High
Congo, Dem Rep of	High	Korea, North	High
Congo, Rep of	High	Korea, South	High
Cook Islands	High	Kosovo	Medium
Costa Rica	High	Kuwait	Medium
Cote d'Ivoire	High	Kyrgyz Republic	Low
Croatia	High	Laos	Medium
Cuba	High	Latvia	High
Curacao	High	Lebanon	Low
Cyprus	High	Lesotho	Low
Czech Rep	Medium	Liberia	High
Denmark	Low	Liechtenstein	High
Lithuania	Low	Singapore	High
Luxembourg	Low	Slovakia	High
Macau	High	Solomon Islands	Low
Macedunia	Low	Solvenia	Low
Magascar	Low	Somalia	High
Malawi	Low	South Africa	High
Malaysia	High	South Sudan	High
Maldives	Low	Spain	High
Mali	Low	Sri Lanka	Low
Maltta	Medium	St. Kitts & Nevis	High
Marshall Islands	High	St. Lucia	High
Mauritania	Low	St. Vincent	High
Mauritius	Medium	St.Maarten	High
Mexico	High	Sudan	High
Micronesia FS	Low	Suriname	Low
Moldova	Medium	Swaziland	Low
Monaco	High	Sweden	Low
Mongolia	Medium	Switzerland	High
Montenegro	High	Syria	High
Montserrat	Low	Taiwan	Medium
Morocco	Medium	Tajikistan	Low
Mozambique	Low	Tanzania	Medium
Namibia	Low	Thailand	High

Country	Risk Level	Country	Risk Level
Nauru	Low	Timor-Leste	Low
Nepal	Low	Togo	Low
Netherlands	High	Tonga	Low
Netherlands Antilles	High	Trinidad and Tobago	Medium
New Zeland	Low	Tunisia	High
Nicaragua	Medium	Turkemistan	Low
Niger	Low	Turkey	High
Nigeria	High	Turks and Caicos	High
Niue	Low	Uganda	Low
Norway	Low	Ukraine	Medium
Oman	Low	United Arab Emirates	Medium
Pakistan	High	United Kingdom	High
Palau	Low	United States	High
Panama	High	Uruguay	High
Papua New Guinea	High	Uzbekistan	Medium
Paraguay	High	Vanuatu	High
Peru	Medium	Venezuela	High
Philippines	High	Vietnam	Medium
Poland	High	Yemen	Medium
Portugal	High	Zambia	Low
Qatar	Low	Zimbabwe	High
Romania	Medium	Libyan Arab Jamah	Low
Russia	High	American samoa	Low
Rwanda	Low	Yugoslavia	Low
Samoa	Medium	Virgin-Islans,Brit.	High
San Marino	Low	Panama Canal Zone	High
Sao Tome & Principe	Low	Palestine	High
Saudi Arabia	Medium	Guadeloupe	Low
Senegal	Medium	Puerto Rico	Low
Serbia	High	British Indian Oc	Low
Seychelles	High		
Sierra Leone	Low		

In addition to the country of business or origin, the bank should account for the risks associated with the geographical area of the branch where the account was or is being opened with respect to the customer's residence or business location. Deviations that are not supported by rational explanation shall be considered of high risk.

Transaction Product and service risk

Another important element that the ML/TF risk assessment should account for is those risks arising from the transactions, products, and services that the entity offers to its customers and the way these products are delivered to the customer where particular attention should be paid for the risks arising from the implementations of new technologies.

The bank should identify the level of risks involved in the service provided to its customers where applicable.

In this respect, the following services are to be accounted for when dealing with our customers:

- Customers involved in money market trading;
- Corporate customers mainly those benefiting from an overdraft facilities, facilities against cash collateral, of trade finance activities;
- International Correspondent banking services;

For existing customers, the bank can rely on the historical relationship in order to determine the risk factor related to the provided products and services by performing the following:

Based on the acquired information, the bank should set the level of risk involved with every customer and this risk and customer relationship shall be reviewed periodically.

As for the factors that accounts for the screening (Media, Local and International lists) it doesn't these factors will automatically affect the customer overall risk level regardless the determined score. For instance, a customer will be perceived as "Undesirable" in case he is listed on any of the international major lists (OFAC, EU, UN, HRM).

Once the identification and risk analysis processes are completed, the strategy of ML/TF risk management is applied to enable the entity to implement adequate policies and procedures for reducing the risks and bringing it down to an acceptable level, with a view to avoiding reputational risks, operational risks, risks of sanctions imposed by a regulatory body and other forms of risk.
In this respect, the bank shall perform the following controls activities based on the determined risk assessment,

Fill an enhanced KYC that includes additional information about the customer's business financial activities, his expected transactions and services performed with the bank, major entities performing business with through and reasons of such activities;

- Increase the level of awareness concerning the monitoring and control procedures required on such accounts;
- Request additional documents besides the KYC to validate the business existence and verify the accuracy of the information provided by the customer, only when required and based on the Compliance Unit recommendation;
- Request additional information on the customers from the Information department, when required;
- Identify the source of wealth;
- Obtain information about all associates having transaction authority over the account;
- Perform a field visit to the customer's business to validate its existence, understand the

business activity and determine the expected turnover in order to assess the expected account activities;
- Perform peer comparison analysis on the accounts to investigate noted variations.

The bank shall not restrict doing business with any business line or nationality/country, other than those restricted by the Lebanese laws or by the Compliance Committee, as long as the customers are showing full cooperation in providing the bank with the required documents and as long as the bank is complying with all the international rules and regulations when dealing with its correspondent banks.
Termination of business activity with any customer will be decided on a case by case basis and based on valid reasons that have nothing to do with suspicious acts or doubt in the customers activities knowing that such a decision is to be taken exclusively by the Compliance Committee after discussing it with the bank's Chairman/General manager.

When monitoring the activities of the above customers, the Compliance Unit should implement the control procedures mentioned under section "AML/CFT compliance unit-implemented control activities".

TRAINING AND QUALIFICATIONS

Training is considered an essential method for communicating the importance of anti-money laundering and terrorism financing efforts, as well as educating employees about what to do if they encounter potential money laundering.

Trains cover several aspects of the fighting money laundering and terrorism financing measures included but not limited to the following:
- Laws related to fighting money laundering and terrorism financing;
- Sanction programs;
- Customer due diligence procedures;
- Account monitoring and suspicious transaction reporting;
- Money laundering and terrorism financing method and real life cases.

In this respect, the bank shall abide by the following training program:
- All new employees shall attend an AML/CFT training session at the compliance department once joining the bank and before being assigned to any function;
- A yearly training shall be provided to all new employees related to the AML/CFT techniques and implemented controls;
- All customer contact staff and back office and audit team should attend at least one yearly AML/CFT training concerning the latest changes in the AML/CFT implemented laws and regulations;
- The branch compliance officers shall attend a quarterly workshops to be delivered by the head of the compliance department in collaboration with the head of AML/CFT Unit;

- The AML/CFT unit shall attend yearly workshops organized by the banking regulators in Lebanon;
- The Compliance team shall hold at least two internal meeting per month with the compliance manager to go through the implemented controls, reported issues, and the monthly key risk indicator reports;
- A quarterly meeting shall be held between the AML/CFT divisions and their respective branches in order to discuss the implemented processes, set improvement plans, and actions plans to handle noted discrepancies.

Finally, all the bank compliance officers, especially the members of the AML/CFT compliance Unit, must have sufficient experience in fighting money laundering and must hold specialized certificates such as the CAMS-Certified Anti-Money Laundering Specialist- and its staff must have the required skills.

CODE OF CONDUCT

Fighting money laundering and terrorism financing is the responsibility of every employee within Al-Mawarid Bank S.A.L. It is the bank's objective to operate within a clean environment where compliance risks are kept low and managed. In this respect, it is the obligation of all employees, regardless of the positions or function held within the bank, to maintain integrity and confidentiality when applying the policies and procedures related to fighting money laundering and terrorism financing.
The below guidelines are to be abides and respected by all members of Al Mawarid Bank's staff:

- Abide by all the procedure stated within this manual;
- Maintain confidentiality concerning all customer enquiries done by the Special Investigation committee or other regulatory entities. In this respect, it is strictly forbidden on any employee within the bank to inform our customers if they are being investigated or studied by the special investigation commission or if their name is listed on the SIC-AML/CFT list;
- Maintain confidentiality concerning customer enquiries performed by the AML/CFT Compliance Unit. In this respect, customers are not to be informed about any enquiring being done on them by the compliance team. Furthermore, it is strictly forbidden on any employee to forward any enquiry send by the compliance department to the customer;
- Tipping off our customers in order to avoid our regular applied controls procedure is completely prohibited. Examples of tipping off includes but not limited to the following:
    - Methods to avoid signing CTS;
    - Guidance to avoid transaction enquiries or in providing wrong explanation related to transaction enquiry;
    - Methods in hiding critical information that will affect the overall risk assessment of the customer or implicate a specific decision related to the account.

- It is completely prohibited to restrain from communicating any information related to specific customer or transaction that might implicate a specific decision or the customer's overall risk assessment;
- Restrain from communicating any information related to the members of the compliance team or committee including names, telephone extension;
- Conflict of interests resulting from a specific compliance issue related to any customer that has a direct or indirect relationship with any employee need to be immediately communicated to the organization development department and the head of the compliance department;
- No one other than the compliance team, and after acquiring the approval of the of general management, can provide any external regulatory party with information related to our customers conditioning that this information is requested in writing and addressed to the General management,

Any employee who fails in abiding any of the above points will be subjected to sever disciplinary action that can include immediate suspension from work.

As per the Lebanese Banking Secrecy law, Employees are requested to maintain confidentiality of information with respect to the bank's client even after terminating their relationship with Al Mawarid Bank S.A.L.

Finally, the bank shall perform regular background screening of prospective and current employees, especially for criminal history, which is essential to keeping out unwanted employees and identifying those to be removed.

AML-CFT Compliance committee
Al Mawarid Bank S.A.L

Appendix A

International black lists for customers' screening

Country	Source Name	Source Abbrev
United States	US-U.S. Office of Foreign Asset Control (OFAC) - SDN List	OFAC
International	UN-United Nations Sanctions List 1	UN
United States	US-U.S. Bureau of Industry and Security (BIS)- Denied Persons List	BIS
International	World Bank List of Debarred Firms	WBDL
International	Interpol	Interpol
United States	US-U.S. Federal Bureau of Investigation	FBI
United States	US-U.S. Debarred Parties	DTC
International	Police (Country Specific)	Police
Switzerland	CH-State Secretariat for Economic Affairs	SECO
International	EU-European Union List	EUList
Isle of Man	IM-Isle of Man Financial Supervision Commission	IoM-FSC
International	Mutual Legal Assistance (MLAT)	MLAT
Colombia	CO-Corte Suprema de Justicia, República de Colombia	Supr Court
United States	US-U.S. Department of State	US DoS
United States	US-U.S. Marshalls	US Marsh
United States	US-U.S. Immigration and Customs Enforcement (ICE)	US-ICE
Saudi Arabia	SA-Saudi Arabia Most Wanted	SaudInfo
United States	US-U.S. Securities and Exchange Commission	US-SEC
Israel	IL-Israeli Intelligence and Terrorism Information Center	IL-ITIC
Russian Federation	RU-Federal Security Service of the Russian Federation (FSB)	RU-FSB
United States	US-U.S. Department of Justice	US-DOJ
United States	US-U.S. Federal Trade Commission	US-FTC
Canada	CA-Royal Canadian Mounted Police	CA-RCMP
Canada	CA-British Columbia Financial Institutions Commission	CA-BC-FIC
Canada	CA-Manitoba Securities Commission	CA-MB-SC
Australia	AU-Australian Securities & Investments Commission	AU-ASIC
United States	US-United States Attorney - Southern District of California	US-AO-SDCA
United States	US-United States Attorney - Northern District of California	US-AO-NDCA

Country	Source Name	Source Abbrev
Pakistan	PK-Pakistan National Accountability Bureau	PK-NAB
United States	US-California Attorney General	US-CASA
United States	US-United States Attorney - District of New Jersey	US-AO-NJ
United States	US-United States Attorney - Southern District of Florida	US-ALSDFL
United States	US-United States Attorney - Southern District of Texas	US-AOSDT
United States	US-United States Attorney - District of Massachusetts	US-AO-DOMA
United States	US-United States Attorney - District of Columbia	US-AO-DODC
United States	US-United States Attorney - District of Connecticut	US-AO-DOCT
United States	US-United States Attorney - District of Arizona	US-AO-DOAZ
United States	US-United States Attorney - Western District of Texas	US-AO-WDTX
United States	US-United States Attorney - Northern District of Texas	US-AO-NDTX
Brazil	BR-Procuradoria Geral da República do Brasil	BR-MPF-PGR
United States	US-U.S. Courts	US-COURT
United States	US-United States Attorney - Northern District of Illinois	US-AG-NDIL
United States	US-United States Attorney - Central District of California	US-AG-CDCA
United States	US-United States Attorney - District of Nevada	US-AG-DNV
Russian Federation	RU-Ministry of the Interior of the Russian Federation	RU-MVDRF
United States	US-U.S. Central Intelligence Agency	US-CIA
United States	US-United States Attorney - District of Maryland	US-AO-DMD
United States	US-United States Attorney - Eastern District of Michigan	US-AO-EDMI
United States	US-United States Attorney - Eastern District of North Carolina	US-AO-EDNC
United States	US-United States Attorney - Western District of Pennsylvania	US-AO-WDPA
United States	US-United States Attorney - Middle District of Pennsylvania	US-AO-MDPA
United States	US-United States Attorney - Eastern District of Wisconsin	US-AO-EDWI
United States	US-United States Attorney - District of Oregon	US-AO-DOR
United States	US-United States Attorney - Eastern District of Texas	US-AO-EDTX
United States	US-United States Attorney - Western District of Kentucky	US-AO-WDKY
United States	US-United States Attorney - Western District of Missouri	US-AO-WDMO
United States	US-United States Attorney - Southern District of New York	US-AO-SDNY
United States	US-United States Attorney - Northern District of Indiana	US-AO-NDIN
United States	US-State of New York Banking Department	US-NY-BD

Country	Source Name	Source Abbrev
Mexico	MX-Procuraduría General de la República de Mexico	MX-PGRMX
United States	US-U.S. Drug Enforcement Administration	US-DEA
United States	US-United States Attorney - District of Rhode Island	US-AG-RI
United States	US-U.S.-China Economic and Security Review Commission	US-USCCC
United States	US-Arizona Corporation Commission Securities Division	US-AZ-CCSD
Russian Federation	RU-Office of the Prosecutor General of the Russian Federation	RU-GPO
Colombia	CO-Departamento Administrativo de Seguridad (DAS), República de Colombia	CO-DAS
Colombia	CO-Ejército Nacional de Colombia	CO-EJNA
Colombia	CO-Fiscalía General de la Nación, República de Colombia	CO-FGDLN
Colombia	CO-Policía Nacional de Colombia	CO-POL
United States	US-U.S. Department of Justice - Tax Division	US-DOJ-TAX
United States	US-United States Attorney - Northern District of Ohio	US-AO-NDHO
Hong Kong	HK-Securities and Futures Commission of Hong Kong	HK-HKSFC
United States	US-New York County District Attorney's Office	US-AO-DNYC
International	UN-United Nations Security Council Resolution 1737 (2006) - Iran Financial Sanctions	UN-SC-1737
India	IN-Indian Central Bureau of Investigation	IN-CBI
Japan	JP-Japanese National Police Agency	JP-NPA
Spain	ES-Guardia Civil española	ES-GCE
United States	US-United States Attorney - Eastern District of Virginia	US-AO-EDVA
United States	US-U.S. FBI Top 10 Fugitives and Most Wanted Terrorists	FBI-MW
Brazil	BR-Supremo Tribunal Federal do Brasil	BR-STF
Brazil	BR-Superior Tribunal de Justiça do Brasil	BR-STJ
United States	US-U.S. Coalition Against Insurance Fraud	US-CAIF
United States	US-United States Attorney - District of New Hampshire	US-AO-DNH
Brazil	BR-Federação Nacional dos Policiais Federais - FENAPEF (Brazil)	BR-FENAPEF
International	UN-United Nations International Criminal Tribunal for the Former Yugoslavia	UN-ICTY
Russian Federation	RU-Russia-Eurasia Terror Watch (RETWA)	RU-RETWA
United Kingdom	UK-Metropolitan Police	UK-MET
United States	US-U.S. Financial Crimes Enforcement Network, Section 311 - Special Measures	FinCEN 311
Germany	DE-Polizei Brandenburg (Germany)	Polizei LB
Italy	IT-Ministero dell'Interno (Italy)	IT-Interno
United Kingdom	UK-Her Majesty's Treasury Financial Sanctions	HMTreasury
United States	US-U.S. Postal Inspection Service	US-USPIS

Country	Source Name	Source Abbrev
Germany	DE-Der Generalbundesanwalt beim Bundesgerichtshof (Attorney General of Germany)	DE-GBA
China	CN-Ministry of Public Security	CN-MPS
International	Website	Website
International	Newspaper	Newspaper
Dominican Republic	DO-Dirección Nacional de Control de Drogas (Dominican Republic)	DO-DNCD
Peru	PE-Policía Nacional del Perú	PNP
Slovenia	SI-Republic of Slovenia, Ministry of the Interior Police	SI-Police
India	IN-Ministry of Home Affairs of India	IN-MHA
United States	US-U.S. Office of Foreign Asset Control (OFAC) - Parastatal Entities of Iraq	OFAC-IRAQ2
Canada	CA-Department of Justice Canada	CA-Justice
United States	US-United States Attorney - Western District of North Carolina	US-AO-WNC
International	UN - United Nations Security Council Resolution 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities	UN-SC-1267
International	UN-United Nations Security Council Resolution 1518 (2003) - Iraq	UN-SC-1518
International	UN-United Nations Security Council Resolution 1521 (2003) - Liberia	UN-SC-1521
International	UN-United Nations Security Council Resolution 1572 (2004) - Côte d'Ivoire	UN-SC-1572
International	UN-United Nations Security Council Resolution 1591 (2005) - Sudan	UN-SC-1591
Japan	JP-Ministry of Finance Japan	JP-MOF
Israel	IL-Israeli Ministry of Justice	IL-JUSTICE
France	Ministère de l'Economie	FR-MINEFE
Russian Federation	RU-Investigative Committee at the Public Prosecutor's Office of the Russian Federation	RU-SLEDCOM
Ukraine	UA-Office of the Prosecutor General of Ukraine	UA-GP
Venezuela	VE-Ministerio Público de Venezuela	VE-Fiscal
El Salvador	SV-Fiscalía General de la República, El Salvador	SV-Fiscal
United States	US-U.S. Department of Defense Military Commission Proceedings at Guantanamo Bay	US-Defense
Germany	DE-Federal Office for Protection of the Constitution	DE-FOPC
United States	US-U.S. Department of State, Narcotics Rewards Program	US-NARC
United States	US-U.S. Department of State - Iran and Syria Nonproliferation Act	US-ISNA
United States	US-U.S. Department of State - Executive Order 12938	US-EO12938
United States	US-U.S. Department of State - Chemical and Biological Weapons Sanctions	US-CBWS
United States	US-U.S. Department of State - Sanctions for the Transfer of Lethal Military Equipment	US-STLME
United States	US-U.S. Department of State - Executive Order 13382	US-EO13382

Country	Source Name	Source Abbrev
New Zealand	NZ-New Zealand Police List	NZ-POLICE
Peru	PE-Ministerio del Interior de Perú	PE-MinInt
United States	US-U.S. Defense Logistics Agency	US-DLA
United States	US-U.S. OFAC - Palestinian Legislative Council List	US-PLC
International	EU-European Union Banned Airlines	EU-BA
United States	Consolidated Sanctions List	Sanctions
Israel	IL-Ministry of Defence - Terrorism List	IL-MODTL
Mexico	MX-Secretaría de Seguridad Pública de Mexico	MX-SSP
Panama	PA-Policia Nacional de Panamá	PA-POLICE
United States	US-U.S. Department of State - Iran, North Korea, and Syria Nonproliferation Act	US-INKS
Guatemala	GT-Ministerio de Gobernación de Guatemala	GT-MINGOB
United Kingdom	UK-UK Home Office Proscribed Terrorist groups	UK-PROTER
Canada	CA-Special Economic Measures against Burma	CA-SPMEBU
Canada	CA-Special Economic Measures against Iran	CA-SPMEIR
Canada	CA-Special Economic Measures against Zimbabwe	CA-SPMEZW
United Kingdom	UK-Crown Prosecution Service	UK-CPS
Spain	ES-National Police of Spain (Cuerpo Nacional De Policía)	ES-POLICE
Colombia	CO-Armada Nacional de Colombia	CO-ARMADA
Spain	ES-La-Moncloa	ES-LM
Paraguay	PY- Secretaría Nacional Antidrogas	PY-SENAD
Egypt	EG-Stock Exchange	EG-SE
Russian Federation	RU-Federal Antimonopoly Service of the Russian Federation	RU-FAS
Canada	CA-Special Economic Measures	CA-SEM
Spain	ES-Interior Ministry News	ES-INTER
Kazakhstan	KZ-Financial Police of Kazakhstan	KZ-FINPOL
Netherlands	NL-Supreme Court of the Netherlands	NL-COURT
Canada	CA-Special Economic Measures against Syria	CA-SYRIA
International	Asian Development Bank	ASIAADB
International	European Bank for Reconstruction and Development	EBRD
Canada	CA- Public Safety Canada	PSCA
Russian Federation	RU-Federal Financial Monitoring Service	ROSFINMON
India	IN- India Courts	IN-CRTS
Mexico	MX-Secretaria de la Defensa Nacional	MX-SDN
Mexico	MX-Secretaria de Marina	MX-SDM

Country	Source Name	Source Abbrev
United States	US-U.S. Department of State - Iran Sanctions Act	US-ISA
Bosnia & Herzegovina	BA-The Prosecutor's Office of B&H	BA-PROSEC
Montenegro	ME–Prosecutor's Office of Montenegro	ME-PROS
Romania	RO-Directorate for Investigation of Organized Crime and Terrorism (DIICOT)	RO-DIICOT
Romania	RO-National Anticorruption Directorate (DNA)	RO-DNA
Bosnia & Herzegovina	BA-The Court of Bosnia and Herzegovina	BA-COURT
Russian Federation	RU-Courts	RU-LEGAL
Russian Federation	RU-Prosecutor's Office	RU-PROKUR
Canada	CA–Surete du Quebec	CA-SDQ
United States	US–Department of State Directorate of Defense Trade Controls	US-DDTC
Bulgaria	BG–Commission for Protection of Competition	BG-CPC
Sierra Leone	SL-Special Court for Sierra Leone	SL-SCSL
Australia	AU-Department of Foreign Affairs and Trade	AU-DFAT
Ukraine	UA-State Financial Monitoring Service	UA-SFMS
Japan	JP-Fukuoka Prefecture Police	JP-FPP
United States	US-U.S. OFAC - Part 561 List	561List
Montenegro	ME- Police Directorate of Montenegro	ME-PDM
Indonesia	ID-Attorney General of Indonesia	ID-AGIN
Netherlands	NL-Ministry of Foreign Affairs	NL-MFA
Romania	RO-Ministry of Justice of Romania	RO-MINJUS
India	IN-National Investigation Agency	IN-NIA
Africa	AC-African Development Bank Group	AC-ADBG
International	UN-Security Council Resolution 1970	UN-SC-1970
International	UN-Security Council Resolution 1533	UN-SC-1533
International	UN-Security Council Resolution 1718	UN-SC-1718
International	UN-Security Council Resolution 2048	UN-SC-2048
International	UN-United Nations Security Council Resolution 751 (1990) and 1907 (2009) – Somalia and Eritrea	UN-SC-751
Albania	AL-Albanian State Police	AL-POLICE
Belarus	BY-General Prosecutor’s Office	BY-GPO
Russian Federation	RU-Ministry of Foreign Affairs	RU-MFA
United Nations	UN - United Nations Security Council Resolution 1988 (2011)	UN-SC-1988
Thailand	TH-Anti-Money Laundering Office	TH-AMLO
Nigeria	NG-National Insurance Commission	NG-NIC

Country	Source Name	Source Abbrev
Colombia	CO-Armada Nacional de Colombia	CO-ARMAPRS
Colombia	CO-Colombian Air force - Press Releases	CO-CA-PR
Rwanda	RW-International Criminal Tribunal for Rwanda)	RW-ICT
Colombia	CO-Procuraduría General de la Nación	CO-PGN
United States	US - Rewards for Justice	US-US-RfJ
Albania	AL-District Court of Tirana	AL-AL-TIRA
United States	US - Iowa Public Employee Retirement System	US-IPERS
United States	US - Minnesota State Board of Investment	US-MSBI
Latvia	LV-Competition Council	LV-CC
Croatia	HR-Croatia's State Prosecutor's Office	HR-CSPO
United States	US-OFAC Foreign Sanctions Evaders List	US-OFACFSE
Canada	CA-OSFI-AntiTerrorism	CA-OSFI-AT
Canada	CA-OSFI-Iran UN List	CA-OSFI-IR
United States	US-Dept of State Terrorist Exclusion List	US-DOS-TEL
Singapore	SG - Monetary Authority of Singapore-186	SG-MAS-186
Israel	IL - Ministry of Finance	IL-MOF
Serbia	RS-Belgrade Higher Court	RS-HCB
Sri Lanka	LK-Financial Intelligence Unit - UNSCR 1373	LK-FIU1373
Sri Lanka	LK-Financial Intelligence Unit - UNSCR 1267	LK-FIU1267
International	UN-United Nations Security Council Resolution 2127 (2013) - Central African Republic	ZI-SC-2127
Canada	CA-OSFI-North Korea UN List	CA-DPRK
Canada	CA-Special Economic Measures against Ukraine	CA-SPMEUA
Canada	CA-Special Economic Measures against Russia	CA-SPMERU