Dear SIC Members, Secretary General & Staff,

The absence of government-wide measures that address the political deadlock and the multifaceted financial/economic crisis continue to impact Lebanon. As such, our responsibilities, duties and efforts continue to be geared on one hand towards softening the impact of the crisis, and on the other hand towards mitigating emerging risks by adopting measures that enhance the effectiveness of Lebanon’s AML/CFT regime.

In 2022, the MENAFATF assessment team mandated to evaluate Lebanon’s AML/CFT regime completed its three-week onsite visit to Lebanon, which is an important milestone in the assessment process that continued despite the many hardships associated with the covid-19 pandemic, the port explosion, recurring lockdowns and strikes. In this respect, your efforts and professionalism made it possible to move forward with this process and prevented Lebanon from renouncing its international commitments towards MENAFATF. For that, I reiterate my appreciation to the team handling and coordinating from our side the evaluation process.

During the year, you carried out your duties with dedication and commitment, handling 469 cases that resulted in funds freezing decisions and in case disseminations to the General
I remain confident that despite the difficult prevailing circumstances, you will cooperate with utmost professionalism with concerned Lebanese authorities towards implementing the action plan resulting from MENAFATF’s adoption in mid-2023 of Lebanon’s MER, which will highlight the country’s compliance with the FATF standards for combating money laundering and terrorist financing.

Best regards,
Riad Toufic Salamé

Banque du Liban, Governor
Special Investigation Commission, Chairman
Dear SIC Managers & Staff,

Over the years, we worked together to elevate Lebanon’s compliance with AML/CFT international standards, and improve the effectiveness of our AML/CFT regime. To this end, we assessed and updated as needed our understanding of the ML/TF risks facing Lebanon, adopted risk mitigating measures, and developed related policies and activities in collaboration with concerned Lebanese authorities. We also improved our capabilities with respect to STR analysis and use of financial intelligence to better support the operational needs of LEAs when handling ML & TF cases. In addition we utilized international cooperation channels as needed to support the cases we handle, and provided in a timely manner quality international cooperation, including to identify, freeze and repatriate illicit funds to concerned countries. Moreover, our efforts resulted in improvements to the risk-based supervision, further raised awareness at banks and reporting entities, and increased the effectiveness of their AM/CFT controls, including for beneficial ownership identification and targeted financial sanctions freeze without delay requirements.

Continuing on this path, we recommended during the year several regulations that were
issued to strengthen our compliance with AML/CFT international standards, and also updated the 2019 NRA. Furthermore, our efforts included the handling of 469 ML and TF cases, of which 123 were from foreign sources and 346 from local sources, in addition to 27 spontaneous disclosures. Other tasks included risk-based AML/CFT compliance examinations that covered 21 banks, 130 money dealers, 6 money remittance companies, 17 financial institutions, 4 brokerage firms and 15 insurance companies, in addition to a number of DNFBPs.

As professionals, we hope that its adoption as a FATF based assessment methodology MER will enable us to cooperate with domestic competent authorities on an action plan that addresses the shortcomings and improves the effectiveness of our AML/CFT regime, and to gain in this respect support from lawmakers and policymakers.

Despite the prevailing local challenges, Lebanon was able to fulfill its international obligations and made it possible for the mutual evaluation process to occur. The almost two-year process included preparatory work and submissions from our end that were followed by an onsite visit by the assessment team, leading up to a mutual evaluation report to be discussed with the assessment team prior to its discussion and adoption by the MENAFATF plenary in mid-2023. As professionals, we hope that its adoption as a FATF based assessment methodology MER will enable us to cooperate with domestic competent authorities on an action plan that addresses the shortcomings and improves the effectiveness of our AML/CFT regime, and to gain in this respect support from lawmakers and policymakers.

I am confident that your dedication and sense of responsibility that places Lebanon’s interest above all will enable us to overcome upcoming challenges.

Best regards,
Abdul Hafiz Mansour

Special Investigation Commission, Secretary General
TABLE OF CONTENTS

Section 1

Special Investigation Commission and its Local / Foreign partners

Chapter 1: Special Investigation Commission Structure
1. Organization Chart 21
2. Members 22
3. General Secretariat 23

Chapter 2: Special Investigation Commission 2022 Activities
1. SIC Units 26
2. Important Milestones – A 10 Year Snapshot 34
3. Staff Training Framework 36
   • Training Events 38
4. International Reach Out Policy 41
   • Technical Assistance & Other Engagements 42
   • Secretary General Engagements 44
5. Selection of Typologies 49

Chapter 3: International & Regional Organizations
1. Egmont Group 56
2. MENAFATF 58

Chapter 4: National Committees
1. The National Committee for Coordinating AML Policies 62
2. The National Committee on Suppressing Terrorism Financing 63

Section 2

Statistical Data
1. Cases Received 66
2. Bank Secrecy Lifted & Information Provided 66
3. Breakdown of Cases by Predicate Offence 67
4. Terrorism or Terrorism Finance Related Cases 68
5. Handling Breakdown 69
6. Breakdown by Source & Type 70
7. Source of Foreign ROAs 71
8. Geographic Distribution of STRs 72
   • Nature of Specified Crimes 73
   • Forgery 74
   • Cybercrime 75
   • Spontaneous Disclosures 75
10. AML/CFT Onsite Compliance Examinations 76
## Section 3

### AML/CFT Laws and Regulations

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Law 44</td>
<td>81</td>
</tr>
<tr>
<td>2</td>
<td>Law 32</td>
<td>85</td>
</tr>
<tr>
<td>3</td>
<td>Law 42</td>
<td>86</td>
</tr>
<tr>
<td>4</td>
<td>Law 53</td>
<td>87</td>
</tr>
<tr>
<td>5</td>
<td>Law 55</td>
<td>87</td>
</tr>
<tr>
<td>6</td>
<td>Law 77</td>
<td>89</td>
</tr>
<tr>
<td>7</td>
<td>Law 214</td>
<td>89</td>
</tr>
<tr>
<td>8</td>
<td>BDL Basic Circular 83</td>
<td>92</td>
</tr>
<tr>
<td>9</td>
<td>BDL Basic Circular 1 Addressed to Collective Investments Schemes</td>
<td>102</td>
</tr>
<tr>
<td>10</td>
<td>BDL Basic Circular 1 Addressed to Financial Intermediation Institutions (Brokerage Firms) and Collective Investments Schemes</td>
<td>102</td>
</tr>
<tr>
<td>11</td>
<td>BDL Basic Circular 2 Addressed to Financial Institutions</td>
<td>107</td>
</tr>
<tr>
<td>12</td>
<td>BDL Basic Circular 2 Addressed to Specialized Lending Entities (Comptoirs)</td>
<td>108</td>
</tr>
<tr>
<td>13</td>
<td>BDL Basic Circular 3 (Section 5)</td>
<td>112</td>
</tr>
<tr>
<td>14</td>
<td>BDL Basic Circular 63</td>
<td>118</td>
</tr>
<tr>
<td>15</td>
<td>BDL Basic Circular 69</td>
<td>118</td>
</tr>
<tr>
<td>16</td>
<td>BDL Basic Circular 81</td>
<td>123</td>
</tr>
<tr>
<td>17</td>
<td>BDL Basic Circular 89</td>
<td>124</td>
</tr>
<tr>
<td>18</td>
<td>BDL Basic Circular 111</td>
<td>125</td>
</tr>
<tr>
<td>19</td>
<td>BDL Basic Circular 126</td>
<td>126</td>
</tr>
<tr>
<td>20</td>
<td>BDL Basic Circular 136</td>
<td>126</td>
</tr>
<tr>
<td>21</td>
<td>BDL Basic Circular 137</td>
<td>127</td>
</tr>
<tr>
<td>22</td>
<td>BDL Basic Circular 138</td>
<td>128</td>
</tr>
<tr>
<td>23</td>
<td>BDL Basic Circular 139</td>
<td>128</td>
</tr>
<tr>
<td>24</td>
<td>BDL Basic Circular 144</td>
<td>131</td>
</tr>
<tr>
<td>25</td>
<td>BDL Basic Circular 147</td>
<td>132</td>
</tr>
<tr>
<td>26</td>
<td>BDL Basic Circular 163</td>
<td>132</td>
</tr>
<tr>
<td>27</td>
<td>Capital Markets Authority Series 2000 &amp; 3000</td>
<td>133</td>
</tr>
<tr>
<td>28</td>
<td>SIC Circular 1</td>
<td>134</td>
</tr>
<tr>
<td>29</td>
<td>SIC Circular 2</td>
<td>134</td>
</tr>
<tr>
<td>30</td>
<td>SIC Circular 4 amended by SIC Circular 13</td>
<td>134</td>
</tr>
<tr>
<td>31</td>
<td>SIC Circular 5 amended by SIC Circular 12</td>
<td>135</td>
</tr>
<tr>
<td>32</td>
<td>SIC Circular 7</td>
<td>137</td>
</tr>
<tr>
<td>33</td>
<td>SIC Circular 8</td>
<td>139</td>
</tr>
<tr>
<td>34</td>
<td>SIC Circular 9</td>
<td>139</td>
</tr>
<tr>
<td>35</td>
<td>SIC Circular 10</td>
<td>139</td>
</tr>
<tr>
<td>36</td>
<td>SIC Circular 11</td>
<td>140</td>
</tr>
<tr>
<td>37</td>
<td>SIC Circular 14</td>
<td>140</td>
</tr>
<tr>
<td>38</td>
<td>SIC Circular 15</td>
<td>141</td>
</tr>
<tr>
<td>39</td>
<td>SIC Circular 16</td>
<td>141</td>
</tr>
<tr>
<td>40</td>
<td>SIC Circular 18</td>
<td>141</td>
</tr>
<tr>
<td>41</td>
<td>SIC Circular 19</td>
<td>142</td>
</tr>
<tr>
<td>42</td>
<td>SIC Circular 20</td>
<td>142</td>
</tr>
<tr>
<td>43</td>
<td>SIC Circular 21</td>
<td>143</td>
</tr>
<tr>
<td>44</td>
<td>SIC Circular 22</td>
<td>144</td>
</tr>
<tr>
<td>45</td>
<td>SIC Circular 23</td>
<td>145</td>
</tr>
<tr>
<td>46</td>
<td>SIC Circular 24</td>
<td>145</td>
</tr>
<tr>
<td>47</td>
<td>SIC Circular 25</td>
<td>146</td>
</tr>
<tr>
<td>48</td>
<td>SIC Circular 26</td>
<td>147</td>
</tr>
<tr>
<td>49</td>
<td>SIC Circular 27</td>
<td>150</td>
</tr>
<tr>
<td>50</td>
<td>SIC Circular 28</td>
<td>151</td>
</tr>
</tbody>
</table>
## Foreword

1. **Introduction** 156
2. **Methodology** 158
3. **ML/TF Threats** 159
   - 3.1 Money Laundering Threats 161
   - 3.2 Terrorist Financing Threats 162
4. **Inherent ML/TF Vulnerabilities** 164
5. **Financial Sector and DNFBPs** 164
   - 5.1 Financial Sector 164
   - 5.2 Designated Non-Financial Businesses & Professions 166
6. **Legal Persons & Arrangements and Non-Profit Organizations** 169
   - 6.1 Legal Persons & Arrangements 169
   - 6.2 Non-Profit Organizations 170
7. **ML/TF Risks** 171
8. **Risk Mitigation Measures - AML/CFT Regime** 172
9. **Looking Forward** 175

---

**ML & TF National Risk Assessment**  
**2022 Update** 176
The enacting of the AML law No. 318 in 2001, which allowed for the establishment of the Special Investigation Commission as the Lebanese FIU, was the cornerstone to launching the serious and structured fight against money laundering and terrorism financing in Lebanon. Back in 2001, the start was with an institution unknown to the local community and more so to the world with a few staff members occupying a modest office. Today, the SIC occupies its separate “high security” offices within the Central Bank compound and over the years has grown significantly in size. The SIC is currently considered among the leading institutions in Lebanon, the region, and is well regarded abroad.

This status did not come easy, as each year along the way was filled with challenges that the SIC family has lived up to. Achievements were numerous ranging from the building of an effective FIU and an AML/CFT regime, the removal of Lebanon from the list of non-cooperative countries & territories, joining regional and international bodies such as the Egmont Group (EG), playing a leading and vital role in the creation of MENAFATF, assuming its first year presidency and its presidency in 2018 as well. The SIC owes much of its achievements to its committed and focused leadership and dedicated staff.

Today, with its many accomplishments, the SIC leadership believes that more still needs to be done. As terrorism, organized crime and ML/TF techniques continue to evolve and change, causing greater threats to world economies, the SIC endeavors to work and participate more in the activities of regional and international bodies to face those growing challenges. The SIC, based on its experience, strongly believes that constant adaptation to rapid changes in the world of crime is a must to keep track of law offenders, and that the best way forward to effectively curb financial flows from organized crime and combat terrorism finance, both predominantly cross border crimes, is through increasing the span and extent of international cooperation. On another hand, continuous training that aims not just at creating more awareness but also at sharpening skills and know-how of its staff and those of other concerned authorities is a must.

Keeping high on its agenda Lebanon’s Mutual Evaluation and the results of the ML/TF National Risk Assessments, several laws and regulations were issued since 2015, including the new AML/CFT Law No. 44. Coordination with other concerned agencies also took place to address risks and points of concern through a comprehensive national strategy that aimed to elevate Lebanon’s AML/CFT regime in line with international standards. Moreover, the SIC is working relentlessly towards enhancing AML/CFT risk based on-site compliance examinations, financial investigations and other SIC core activities with hopes that the coming years will be marked with similar success.
2001
- Enactment of AML Law No. 318
- Creation of the SIC

2002
- Removal of Lebanon’s name from FATF NCCT List
- Creation of the National Committee for Coordinating AML Policies

2003
- SIC joins the Egmont Group of FIUs

2004
- Creation of MENAFATF & first year presidency awarded to Lebanon

2005
- Creation of SEEDS (For electronic exchange of information with reporting entities)

2006
- SIC involved in U.S. MENA Private Sector Dialogue (PSD)

2007
- Lebanon ratifies UN Convention Against Corruption (UNCAC), & Law No. 32 was enacted to expand SIC competence to include corruption

2008
- MENAFATF adopts Lebanon’s ME Report

2009
- New SIC Secretary appointment

2010
- SIC joins Egmont Group’s Special Project Team (SPT) on its charter review

2011
- SIC joins the Egmont Group Task Team on the implementation of the EG strategic plan

2012
- Draft AML / CFT law, cross border transportation of funds law and exchange of tax information law forwarded to Parliament

2013
- SIC led the ML/TF National Risk Assessment (NRA)

2014
- SIC joins the Egmont Group Task Team on the implementation of the EG strategic plan
2015
- Strengthening the AML/CFT regime by enacting several laws including a new AML/CFT Law No. 44
- SIC Secretary General becomes EG MENA Region Representative & Egmont Committee Vice Chair

2016
- Enactment of Law No. 77 amending Article 316 bis. of the Lebanese Penal Code (TF Offence) & Law No. 55 on the exchange of information for tax purposes
- The Higher Council of Customs collaborated with the SIC to issue a mechanism to implement Law No. 42 on Declaring the Cross-Border Transportation of Money

2017
- SIC Secretary General re-elected as EG MENA Region Representative & Egmont Committee Vice Chair
- SIC representing Lebanon assumed the Vice Presidency of MENAFATF
- SIC received the STAR Award of Excellence from the World Bank-UNODC Stolen Asset Recovery Initiative (STAR) for investigating a corruption case that resulted in asset recovery

2018
- Lebanon represented by the SIC assumes the MENAFATF Presidency
- The second ML/TF National Risk Assessment was initiated and is being led by the SIC

2019
- The 2019 ML & TF National Risk Assessment was concluded & SIC Circular 25 was issued
- The two national committees for AML & CFT adopted an action plan containing risk mitigation measures

2020
- Enactment of the Law on the Recovery of Assets Derived from Corruption Offences (Law No. 214/2021)
- The ML/TF National Risk Assessment update was initiated

2021
- Enactment of the Law on the Recovery of Assets Derived from Corruption Offences (Law No. 214/2021)
- As part of the evaluation process, the MENAFATF assessment team concluded its onsite visit to Lebanon

2022
- The ML/TF National Risk Assessment and its Strategic Action Plan were updated in 2022
- The UN 1267/2253 Sanctions Committee made a designation based on Lebanon’s request.
- Enactment of the Anti-corruption law in the public sector and the establishment of the National Anti Corruption Agency (Law No. 175/2020)
SECTION I

Special Investigation Commission and its Local / Foreign partners

Chapter 1: Special Investigation Commission Structure
1. Organization Chart 21
2. Members 22
3. General Secretariat 23

Chapter 2: Special Investigation Commission 2022 Activities
1. SIC Units 26
2. Important Milestones – A 10 Year Snapshot 34
3. Staff Training Framework 36
   ◆ Training Events 38
4. International Reach Out Policy 41
   ◆ Technical Assistance & Other Engagements 42
   ◆ Secretary General Engagements 44
5. Selection of Typologies 49

Chapter 3: International & Regional Organizations
1. Egmont Group 56
2. MENAFATF 58

Chapter 4: National Committees
1. The National Committee for Coordinating AML Policies 62
2. The National Committee on Suppressing Terrorism Financing 63
The Governor of Banque du Liban
Mr. Riad Salamé
Chairman

The President of the Banking Control Commission
Mrs. Mayya Dabbagh
Member

The Judge appointed to the Higher Banking Commission
Dr. Ali Ibrahim
Member

The professional appointed by the Council of Ministers
Mr. Shadi Hanna
Member

Mr. Abdul Hafiz Mansour
Secretary General

Analysis & Investigation Unit
Mr. Hisham Hamzé
Executive Director

Database Administrative Unit
Mrs. May Naggear
Executive Director

Compliance Unit
Mr. Tarek Zahran
Executive Director

IT & Security Unit
Mr. Nasser Lebbos
Executive Director
Members

1 | The Special Investigation Commission is composed of:
   The Governor of Banque du Liban, Mr. Riad Salamé, or the Vice-Governor designated by him.  
   Chairman
   The Judge appointed to the Higher Banking Commission, Dr. Ali Ibrahim, or his alternate judge.  
   Member
   The President of the Banking Control Commission, Mrs. Mayya Dabbagh, or the member of the Commission designated by her.  
   Member
   The professional appointed by the Council of Ministers, Mr. Shadi Hanna, or his alternate Mr. Boutros (Pierre) Kanaan.  
   Member

2 | Article 6 of Law No. 44 of November 24, 2015 establishes “the Special Investigation Commission” or “the Commission” as an independent legal entity with judicial status at Banque du Liban, which shall discharge its functions without being subject to Banque du Liban’s authority.

The mission of the Special Investigation Commission, as per Law No. 44, is to:

- Receive suspicious transaction reports (STRs) and requests of assistance; to investigate operations that are suspected to be money-laundering or terrorism financing offences; to decide on the seriousness of evidence and circumstantial evidence related to the commission of any such offence(s); to take in this regard the adequate decision, particularly the precautionary and temporary freezing of the suspicious accounts and/or transactions, for a maximum period of one year renewable once for six months concerning foreign requests of assistance, and for a maximum period of six months renewable once for three months concerning local STRs and requests of assistance.

- Ensure compliance by the parties referred to in Articles 4 and 5 of this law with the obligations stipulated in this Law and in the regulations issued in relation thereto, except for lawyers, certified accountants and notaries, without prejudice to the provisions of Paragraph 2 of Article 17 of this Law.

- Collect and retain the information received from the parties referred to in Articles 4 and 5 of this law, as well as the information received from Lebanese and foreign official authorities, and all other collected information, and to share such information with the Commission’s counterparts, in its capacity as the competent authority and the official center to undertake such a task.

- Issue regulations on the implementation of the provisions of this Law addressed to the parties referred to in Article 5 of this law, and to issue recommendations to all concerned parties.

- Permanently freeze the concerned accounts and/or transactions, and/or lift the banking secrecy in favor of the competent judicial authorities and the Higher Banking Commission represented by its Chairman on accounts or transactions suspected to be related to money laundering or terrorism financing.

- Keep suspicious accounts as traceable accounts.

- Attach an encumbrance on the records and entries pertaining to movable or immovable assets, indicating that such assets are under investigation by “the Commission”. The encumbrance shall be kept until doubts are erased or until a final decision in this regard is taken.

- Request the Public Prosecutor of the Court of Cassation to take preventive measures concerning the movable and immovable assets that have no records or entries, so as to prevent the use of such assets until a final judicial decision in this regard is taken.

- Require from concerned persons and parties, whether public or private, to take the necessary measures to prevent the use of movable or immovable assets belonging to any names designated or to be designated on the national lists issued by the competent Lebanese authorities or any other lists it circulates concerning terrorism and terrorism financing and any acts related thereto. The concerned persons and parties, whether public or private, must comply without any delay to this requirement.
**General Secretariat**

1 | The Special Investigation Commission General Secretariat is composed of:
- The Secretary General
- The Analysis & Investigation Unit
- The Compliance Unit
- The Database Administrative Unit
- The Information Technology & Security Unit

2 | The tasks include the following:

- Supervise directly the SIC Units.
- Receive all suspicious transaction reports, requests of assistance, and other reports, and process them through the concerned SIC Units, and notify relevant parties of SIC decisions.
- Provide an analytical opinion on SIC Units’ reports on executed tasks.
- Implement when allocating tasks the principle of avoiding conflict of interest.
- Monitor domestic/foreign laws and regulations as well as international standards, and recommend amendments to Lebanese legislations and regulations.
- Foster cooperation between the SIC and its foreign counterparts.
- Engage and follow up on the work of AML/CFT regional and international bodies.
- Engage and follow up on the work of the AML and CFT National Committees.
- Oversee staff related administrative matters, prepare the budget, and oversee expenditures and the audit thereof.
The Analysis and Investigation Unit is the financial investigation and analysis arm of the Special Investigation Commission. The Unit analyzes STRs filed on money laundering, associated predicate offences, terrorism and terrorism financing, and investigates related persons and transactions. This work is supported when needed with additional information requested from reporting entities, law enforcement authorities, government agencies, and counterpart FIUs. The Unit also handles spontaneous disclosures and ROAs received from local and foreign authorities. Decisions taken by the SIC based on this work include disseminating cases to the General Prosecutor, exchanging information with counterpart FIUs, sending spontaneous disclosures as well as freezing accounts/transactions. SIC decisions also include keeping accounts traceable, and placing an encumbrance on records and entries pertaining to movable or immovable assets.
The Unit’s tasks include the following:

- Conduct operational analysis, investigation and audit on STRs received and on the related accounts/transactions, and process ROAs received from local and foreign authorities, in addition to spontaneous disclosures.
- Handle STRs and ROAs received according to priorities, and in accordance with the results of the ML/TF National Risk Assessment.
- Prepare reports on the results of the analysis, investigation and audit, and on the ROAs received, and in this respect:
  - Request additional information when needed from reporting entities, law enforcement authorities, government agencies, in addition to information from foreign FIUs.
  - Use the widest possible range of evidence, financial and administrative information and information available to concerned authorities (including information from open or public sources, as well as relevant information collected and/or maintained by other authorities and, where appropriate commercially held data).
- Provide reporting entities with feedback and seek feedback from the General Prosecutor or from concerned local competent authorities to ensure that they receive accurate information that assists them in performing their duties, and improves their operational expertise and applications.
- Inform the Database Administrative Unit of operational analysis reports prepared, to be entered in the SIC database, and cooperate on strategic analysis work. Inform the Compliance Unit of this work to be considered during supervisory activities.
- Develop a procedural manual for the Unit that sets the details adopted to implement its duties, and use of software tools for analysis.

In 2022, the Unit continued prioritizing its handling of STRs in accordance with the adopted risk classification criteria that include high risk crimes identified in the NRA (low, medium, high). During the year, it handled 469 cases comprised of 207 STRs and 287 ROAs originating from foreign/local sources, in addition to 27 spontaneous disclosures. The Unit’s analysis, audit and cooperation work resulted in disseminating information to the General Prosecutor / law enforcement authorities, and exchanging information with concerned FIUs. The SIC decisions with respect to several cases included requesting from reporting entities to freeze accounts, keep accounts traceable, and refrain from carrying out certain transactions, in addition to attaching an encumbrance on properties.
The Compliance Unit is the supervisory arm of the Special Investigation Commission tasked with ensuring compliance of banks, financial institutions and other reporting entities, including at the financial group level, with prevailing AML/CFT obligations. It conducts onsite and offsite supervision to assess the implementation and effectiveness of compliance programs, CDD measures and internal controls adopted to monitor, detect and report suspicious transactions. Onsite supervision is risk based and is complemented with ongoing offsite work, and a tailored risk based approach for supervision of concerned sectors under Law No. 44/2015 is adopted and updated continuously to ascertain effective and precise supervision, as well as adequate coverage. The Unit also highlights corrective measures that banks, financial institutions and other reporting entities need to implement to enhance their compliance programs and internal controls. Moreover, it recommends updating AML/CFT obligations or introducing new ones in accordance with developments in international standards/best practices, and with the evolving risks, or as a result of supervisory findings.
The Unit’s tasks include the following:

- Ensure periodically and continuously through risk-based onsite and offsite supervision, that banks, financial institutions and other concerned institutions implement, as applicable, the obligations stipulated in Law no. 44/2015, BDL and SIC circulars on AML/CFT.
- Prepare reports and statistics on banks, financial institutions and other concerned institutions’ compliance with AML/CFT obligations, and propose penalties including warnings and monetary fines as necessary.
- Correspond with banks, financial institutions and other concerned institutions when supervisory findings reveal partial or non-compliance with AML/CFT requirements, and request that they take the necessary corrective measures to enhance their compliance programs and internal controls.
- Develop a tailored supervisory risk-based approach for each of the concerned sectors under Law no. 44/2015 and update them continuously to ensure effective and precise supervision as well as adequate coverage.
- Recommend updates to prevailing AML/CFT requirements or new requirements in accordance with developments in international standards/best practices, and with the evolving risks, or as a result of supervisory findings.
- Assist entities subject to supervision in understanding their AML/CFT obligations and ML/TF risks.
- Follow-up on external auditors’ annual reports on AML/CFT procedures at banks and other concerned entities, compare the said reports with the Unit’s reports and verify that banks and other concerned entities implement the observations mentioned in these reports.
- Provide the Analysis & Investigation Unit and the Database Administrative Unit with summarized reports on banks, financial institutions and other concerned institutions’ compliance with AML/CFT requirements.
- Develop a procedural manual for the Unit that sets the details adopted to implement its duties.

During 2022, the Unit worked towards updating the ML/TF NRA that was led by the SIC in cooperation with other AML/CFT stakeholders. The Unit also recommended additional AML/CFT regulations that were issued accordingly via BDL and SIC circulars. Active participation continued in MENAFATF, Egmont Group, and FATF plenaries and working group meetings. The Compliance Unit’s Director was selected for a two-year term for the position of Co-Chair for MENAFATF’s Technical Assistance & Typologies Working Group, and for the Vice-Chair position for Egmont Group’s Membership Support & Compliance Working Group. In addition, members from the Unit coordinated MENAFATF’s mutual evaluation process to assess Lebanon’s AML/CFT regime, and handled preparatory work including the assessment team’s three-week onsite visit to Lebanon. Furthermore, during the year the Unit continued its offsite and onsite risk-based compliance examinations that covered 21 banks, 130 money dealers, 6 money remittance companies, 17 financial institutions, 4 brokerage firms and 15 insurance companies, in addition to a number of DNFBPs to ensure their compliance with the AML/CFT regulations.
The Database Administrative Unit is entrusted with managing the Special Investigation Commission’s database. It logs and maintains all filed STRs and ROAs received from local/foreign sources and through the Egmont Secure Web, as well as spontaneous disclosures, and ROAs sent to foreign authorities including FIUs. Its tasks include retaining existing and gathered information, along with the results of conducted analysis & investigations, and SIC decisions taken in this regard. Reviews, updates and classifications are periodically performed to ensure data accuracy. The Unit also issues statistics that is used in SIC annual reports, in strategic analysis and when identifying ML/TF trends and patterns.
The Unit’s tasks include the following:

• Set up and manage the SIC database by logging / retaining filed STRs, ROAs received from local/foreign sources, spontaneous disclosures, and ROAs sent to foreign authorities, in addition to names of concerned persons, reporting entities and all related information and decisions taken.

• Coordinate with the IT & Security Unit on implemented security controls and access rights to the SIC database, IT programs and to the Egmont Secure Web (ESW).

• Cooperate with the Analysis & Investigation Unit to conduct strategic analysis by using available and accessible information, in order to identify ML/TF trends and patterns.

• Prepare requested studies and propose awareness raising needs and relevant training.

• Coordinate with the IT & Security Unit to periodically update the SIC website.

• Develop a procedural manual for the Unit that sets the details adopted to implement its duties.

During 2022, the Unit continued managing the SIC database including reviewing the accuracy of retained information, and logging in new information related to STRs and ROAs received from local and foreign sources, along with spontaneous disclosures and decisions taken in this regard. This adequate classification of information allows for the identification of links and the extraction of statistics used in the strategic analysis work.

The Unit also focused on training and capacity building programs for staff through the Continuing Professional Education program (CPE) which covered during the year topics on compliance with global sanctions and combatting corruption. In this regards, the SIC collaborated with an international consulting company to provide training for banks and several SIC staff, who were later tested to obtain a certification.
The IT & Security Unit manages, updates and makes available for SIC staff all technical tools and equipment, as well as the servers, internal network, programs and applications needed for their work. It is also tasked with the technical development and security measures of the SIC database, as well as with establishing the network and programs needed for the secure exchange of messages and information with reporting entities and concerned authorities. Among the Unit’s responsibilities is also the safety and security of the premises, data and archived documents, in addition to developing and updating the SIC website and the disaster recovery plan.
The Unit’s tasks include the following:

- Install and activate the main servers, computers, telecommunication devices, security & motoring equipment and all technical devices.
- Update and maintain the SIC database and provide SIC Units with IT programs needed for their work.
- Adopt safety rules and procedures for the premises, offices, and for access rights. Also develop and adopt rules and procedures to ensure security and confidentiality of data, archived documents and programs, and apply access rules based on needs and rights granted.
- Study and implement programs to safely disseminate and exchange information with AML/CFT stakeholders.
- Update the SIC website periodically.
- Develop, implement and update the disaster recovery plan to ensure work continuity.
- Develop a procedural manual for the Unit that sets the details adopted to implement its duties.

During 2022, the IT & Security Unit engaged its staff in specialized training seminars on cyber security and combating cybercrimes that helped sharpen their skills. The Unit also updated certain features of the SIC website making it more user friendly. On the other hand, the search and classification capabilities of the SIC database were developed, and information and security systems were improved after revisions were made to software, computers, laptops, communication devices and to security / monitoring equipment. Furthermore, during the year reviews were made to the disaster recovery plan, the information exchange system with reporting entities and concerned government agencies, and necessary improvements were made as needed.
2013

 país 

 BDL Basic Circular No. 83 amended to strengthen the AML/CFT compliance function at the branch level

 Issuance of SIC Circulars 15, 16 & 18

 Issuance of SIC Circular 17 on the electronic filing of STRs in accordance with the SIC modernization plan

 SIC joins the Egmont Group Task Team on the implementation of the EG strategic plan

 SIC joins a Committee tasked by the Ministry of Justice with preparing a draft Law for the recovery of funds related to corruption and smuggled to Lebanon

 Lebanon’s Fourth Progress Report submitted to MENAFATF

 The review of Lebanon’s implementation of UNCAC was initiated (chapters 3 & 4)

 MOUs signed with Counterpart FIUs since SIC Inception

<table>
<thead>
<tr>
<th>País</th>
<th>FIU</th>
<th>Fecha de firma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bélgica</td>
<td>CTIF-CFI</td>
<td>Sep. 10, 2002</td>
</tr>
<tr>
<td>Croacia</td>
<td>AMLO</td>
<td>Oct. 7, 2002</td>
</tr>
<tr>
<td>Tailandia</td>
<td>AMLO-TH</td>
<td>Feb. 25, 2003</td>
</tr>
<tr>
<td>Mónaco</td>
<td>SCICFIN</td>
<td>May 20, 2003</td>
</tr>
<tr>
<td>Australia</td>
<td>AUSTRAC</td>
<td>Sep. 24, 2003</td>
</tr>
<tr>
<td>Francia</td>
<td>TRACFIN</td>
<td>Jun. 21, 2004</td>
</tr>
<tr>
<td>Países Bajos</td>
<td>MOT-AN</td>
<td>Jun. 23, 2004</td>
</tr>
<tr>
<td>Albania</td>
<td>GDPML</td>
<td>Oct. 4, 2004</td>
</tr>
<tr>
<td>Guatemala</td>
<td>IVE</td>
<td>Sep. 8, 2005</td>
</tr>
<tr>
<td>Moldavia</td>
<td>SPCS</td>
<td>Sep. 9, 2005</td>
</tr>
</tbody>
</table>

2014

 • Institution of BDL Basic Circular No. 83 amended to strengthen the AML/CFT compliance function at the branch level

 • Issuance of SIC Circulars 15, 16 & 18

 • Issuance of SIC Circular 17 on the electronic filing of STRs in accordance with the SIC modernization plan

 • SIC joins the Egmont Group Task Team on the implementation of the EG strategic plan

 • SIC joins a Committee tasked by the Ministry of Justice with preparing a draft Law for the recovery of funds related to corruption and smuggled to Lebanon

 • Lebanon’s Fourth Progress Report submitted to MENAFATF

 • The review of Lebanon’s implementation of UNCAC was initiated (chapters 3 & 4)

 • Enactment of a new AML/CFT Law (Law No. 44)

 • Lebanon accedes to the UN International Convention for the Suppression of the Financing of Terrorism (Law No. 53)

 • Enactment of a law on Dealing the Cross-Border Transportation of Money & a law on the Exchange of Tax Information (Laws No. 42 & 43)

 • The National Committee on Suppressing Terrorism Financing adopts two Targeted Financial Sanctions Mechanisms for UNSCR 1267 & 1373

 • Issuance of BDL Basic Circular No. 136 & SIC Circular 19 on the implementation of UNSCR 1267

 • Issuance of BDL Intermediate Circular No. 393 on AML/CFT requirements for Money Remittance Companies

 • SIC Secretary General becomes EG MENA Region Representative & Egmont Committee Vice Chair

 • Lebanon’s Sixth Progress Report submitted to MENAFATF

 • SIC reaches its 3000 case milestone

 • MOUs signed with Counterpart FIUs since SIC Inception

<table>
<thead>
<tr>
<th>País</th>
<th>FIU</th>
<th>Fecha de firma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bélgica</td>
<td>CTIF-CFI</td>
<td>Sep. 10, 2002</td>
</tr>
<tr>
<td>Croacia</td>
<td>AMLO</td>
<td>Oct. 7, 2002</td>
</tr>
<tr>
<td>Tailandia</td>
<td>AMLO-TH</td>
<td>Feb. 25, 2003</td>
</tr>
<tr>
<td>Mónaco</td>
<td>SCICFIN</td>
<td>May 20, 2003</td>
</tr>
<tr>
<td>Australia</td>
<td>AUSTRAC</td>
<td>Sep. 24, 2003</td>
</tr>
<tr>
<td>Francia</td>
<td>TRACFIN</td>
<td>Jun. 21, 2004</td>
</tr>
<tr>
<td>Países Bajos</td>
<td>MOT-AN</td>
<td>Jun. 23, 2004</td>
</tr>
<tr>
<td>Albania</td>
<td>GDPML</td>
<td>Oct. 4, 2004</td>
</tr>
<tr>
<td>Guatemala</td>
<td>IVE</td>
<td>Sep. 8, 2005</td>
</tr>
<tr>
<td>Moldavia</td>
<td>SPCS</td>
<td>Sep. 9, 2005</td>
</tr>
</tbody>
</table>

2015

 • Enactment of a new AML/CFT Law (Law No. 44)

 • Lebanon accedes to the UN International Convention for the Suppression of the Financing of Terrorism (Law No. 53)

 • Enactment of a law on Dealing the Cross-Border Transportation of Money & a law on the Exchange of Tax Information (Laws No. 42 & 43)

 • The National Committee on Suppressing Terrorism Financing adopts two Targeted Financial Sanctions Mechanisms for UNSCR 1267 & 1373

 • Issuance of BDL Basic Circular No. 136 & SIC Circular 19 on the implementation of UNSCR 1267

 • Issuance of BDL Intermediate Circular No. 393 on AML/CFT requirements for Money Remittance Companies

 • SIC Secretary General becomes EG MENA Region Representative & Egmont Committee Vice Chair

 • Lebanon’s Sixth Progress Report submitted to MENAFATF

 • SIC reaches its 3000 case milestone

 • MOUs signed with Counterpart FIUs since SIC Inception

<table>
<thead>
<tr>
<th>País</th>
<th>FIU</th>
<th>Fecha de firma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bélgica</td>
<td>CTIF-CFI</td>
<td>Sep. 10, 2002</td>
</tr>
<tr>
<td>Croacia</td>
<td>AMLO</td>
<td>Oct. 7, 2002</td>
</tr>
<tr>
<td>Tailandia</td>
<td>AMLO-TH</td>
<td>Feb. 25, 2003</td>
</tr>
<tr>
<td>Mónaco</td>
<td>SCICFIN</td>
<td>May 20, 2003</td>
</tr>
<tr>
<td>Australia</td>
<td>AUSTRAC</td>
<td>Sep. 24, 2003</td>
</tr>
<tr>
<td>Francia</td>
<td>TRACFIN</td>
<td>Jun. 21, 2004</td>
</tr>
<tr>
<td>Países Bajos</td>
<td>MOT-AN</td>
<td>Jun. 23, 2004</td>
</tr>
<tr>
<td>Albania</td>
<td>GDPML</td>
<td>Oct. 4, 2004</td>
</tr>
<tr>
<td>Guatemala</td>
<td>IVE</td>
<td>Sep. 8, 2005</td>
</tr>
<tr>
<td>Moldavia</td>
<td>SPCS</td>
<td>Sep. 9, 2005</td>
</tr>
</tbody>
</table>

2016

 • Enactment of a new AML/CFT Law (Law No. 44)

 • Lebanon accedes to the UN International Convention for the Suppression of the Financing of Terrorism (Law No. 53)

 • Enactment of a law on Dealing the Cross-Border Transportation of Money & a law on the Exchange of Tax Information (Laws No. 42 & 43)

 • The National Committee on Suppressing Terrorism Financing adopts two Targeted Financial Sanctions Mechanisms for UNSCR 1267 & 1373

 • Issuance of BDL Basic Circular No. 136 & SIC Circular 19 on the implementation of UNSCR 1267

 • Issuance of BDL Intermediate Circular No. 393 on AML/CFT requirements for Money Remittance Companies

 • SIC Secretary General becomes EG MENA Region Representative & Egmont Committee Vice Chair

 • Lebanon’s Sixth Progress Report submitted to MENAFATF

 • SIC reaches its 3000 case milestone

 • MOUs signed with Counterpart FIUs since SIC Inception

<table>
<thead>
<tr>
<th>País</th>
<th>FIU</th>
<th>Fecha de firma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bélgica</td>
<td>CTIF-CFI</td>
<td>Sep. 10, 2002</td>
</tr>
<tr>
<td>Croacia</td>
<td>AMLO</td>
<td>Oct. 7, 2002</td>
</tr>
<tr>
<td>Tailandia</td>
<td>AMLO-TH</td>
<td>Feb. 25, 2003</td>
</tr>
<tr>
<td>Mónaco</td>
<td>SCICFIN</td>
<td>May 20, 2003</td>
</tr>
<tr>
<td>Australia</td>
<td>AUSTRAC</td>
<td>Sep. 24, 2003</td>
</tr>
<tr>
<td>Francia</td>
<td>TRACFIN</td>
<td>Jun. 21, 2004</td>
</tr>
<tr>
<td>Países Bajos</td>
<td>MOT-AN</td>
<td>Jun. 23, 2004</td>
</tr>
<tr>
<td>Albania</td>
<td>GDPML</td>
<td>Oct. 4, 2004</td>
</tr>
<tr>
<td>Guatemala</td>
<td>IVE</td>
<td>Sep. 8, 2005</td>
</tr>
<tr>
<td>Moldavia</td>
<td>SPCS</td>
<td>Sep. 9, 2005</td>
</tr>
</tbody>
</table>

2017

 • MOUs signed with Counterpart FIUs since SIC Inception

<table>
<thead>
<tr>
<th>País</th>
<th>FIU</th>
<th>Fecha de firma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bélgica</td>
<td>CTIF-CFI</td>
<td>Sep. 10, 2002</td>
</tr>
<tr>
<td>Croacia</td>
<td>AMLO</td>
<td>Oct. 7, 2002</td>
</tr>
<tr>
<td>Tailandia</td>
<td>AMLO-TH</td>
<td>Feb. 25, 2003</td>
</tr>
<tr>
<td>Mónaco</td>
<td>SCICFIN</td>
<td>May 20, 2003</td>
</tr>
<tr>
<td>Australia</td>
<td>AUSTRAC</td>
<td>Sep. 24, 2003</td>
</tr>
<tr>
<td>Francia</td>
<td>TRACFIN</td>
<td>Jun. 21, 2004</td>
</tr>
<tr>
<td>Países Bajos</td>
<td>MOT-AN</td>
<td>Jun. 23, 2004</td>
</tr>
<tr>
<td>Albania</td>
<td>GDPML</td>
<td>Oct. 4, 2004</td>
</tr>
<tr>
<td>Guatemala</td>
<td>IVE</td>
<td>Sep. 8, 2005</td>
</tr>
<tr>
<td>Moldavia</td>
<td>SPCS</td>
<td>Sep. 9, 2005</td>
</tr>
</tbody>
</table>
• Lebanon represented by the SIC assumes the MENAFATF Presidency, and the 27th & 28th Plenary meetings were held in Beirut
• BDL Basic Circular No. 83 amended to cover the definition and identification of the Beneficial Owner and to add an indicator for certain suspicious real estate transactions
• Issuance of two BDL Basic Circulars for Brokerage Firms and for Collective Investments Schemes on the Beneficial Owner
• Issuance of SIC Circular 24 on the definition and identification of the Beneficial Owner
• The Lebanese Tax Procedures Code amended to include the Beneficial Owner (Law No. 106/2018)
• The second ML/TF National Risk Assessment was initiated and is being led by the SIC
• The SIC, MENAFATF and ACINET jointly organized in Beirut the “Arab Forum for Anti Corruption Agencies and Financial Intelligence Units”, with support from the UN, EG, and OECD
• The SIC, MENAFATF & ISF jointly organized in Beirut the “4th Anti-Cybercrime Forum”
• The Lebanese Association of Certified Public Accountants and the Lebanese Ministry of Justice issued two separate manuals on the implementation of AML/CFT Law no. 44/2015

2018
• The 2019 ML & TF National Risk Assessment was concluded & SIC Circular 25 was issued
• The two national committees for AML & CFT adopted an action plan containing risk mitigation measures
• BDL Basic Circular No. 83 was amended
• Issuance of BDL Basic Circular No. 147 & BDL Intermediate Circular No. 521 to mitigate tax evasion risks
• Issuance of BDL Intermediate Circulars No. 528 & 529 to money dealers and money remittance companies
• The Lebanese Code of Commerce was amended to include among other things Beneficial Owner requirements (Law No. 126/2019)
• The OECD-Global Forum Peer Review Report rated Lebanon Largely Compliant on the Exchange of Information on Request

2019
• Issuance of BDL Basic Circular No. 163 to banks, and BDL Intermediate Circulars No. 625, 630, 631, 632, 633 and 634 to all financial sector institutions
• Issuance of SIC Circular 26
• The ML/TF National Risk Assessment update was initiated

2020
• The UN 1267/2253 Sanctions Committee made a designation based on Lebanon’s request.
• Enactment of the Anti-corruption law in the public sector and the establishment of the National Anti Corruption Agency (Law No. 175/2020)
• Enactment of a Law on “Financial Disclosure, Conflicts of Interest and Illicit Enrichment” (Law No. 189/2020)
• Enactment of a Law legalizing Cannabis cultivation for medical and industrial use (Law No. 178/2020)
• The Commercial Register at the Ministry of Justice adopted a Beneficial Owner Form.

2021
• The Commercial Register at the Ministry of Justice adopted a Beneficial Owner Form.
• The OECD-Global Forum Peer Review Report rated Lebanon Largely Compliant on the Exchange of Information on Request
• The ML/TF National Risk Assessment and its Strategic Action Plan were updated in 2022

2022
• Issuance of BDL Intermediate Circulars No. 605, 602, 606, 603 and 604 to banks and financial institutions, money dealers, money remittance companies, financial intermediation institutions and specialized lending entities
• Issuance of SIC Circular 26
• The ML/TF National Risk Assessment update was initiated

<table>
<thead>
<tr>
<th>Country</th>
<th>FIU</th>
<th>Signing Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 Qatar</td>
<td>QFIU</td>
<td>Apr. 28, 2010</td>
</tr>
<tr>
<td>22 Kingdom of Saudi Arabia</td>
<td>SAFIU</td>
<td>Jun. 30, 2010</td>
</tr>
<tr>
<td>23 Japan</td>
<td>JAFIC</td>
<td>Jul. 10, 2012</td>
</tr>
<tr>
<td>24 Philippines</td>
<td>AMLC</td>
<td>Jul. 10, 2012</td>
</tr>
<tr>
<td>25 Russia</td>
<td>FSFM</td>
<td>Jul. 11, 2012</td>
</tr>
<tr>
<td>26 Algeria</td>
<td>CTRF</td>
<td>Sep. 13, 2012</td>
</tr>
<tr>
<td>28 Sint Maarten</td>
<td>MOT-SM</td>
<td>Feb. 18, 2014</td>
</tr>
<tr>
<td>29 Burkina Faso</td>
<td>CENTIF-BF</td>
<td>Feb. 18, 2014</td>
</tr>
<tr>
<td>30 Greece</td>
<td>Hellenic FIU</td>
<td>Mar. 14, 2014</td>
</tr>
</tbody>
</table>
The SIC believes that intellectual capital is its most valuable asset, therefore investing in the training and development of its staff is a stable policy. This investment is crucial for the day-to-day work and equally important for other engagements that require exceptional know-how to create the necessary awareness, provide technical assistance and participate in the various assignments undertaken by international and regional bodies such as FATF, MENAFATF and the Egmont Group.

Sharpening skills and exposing staff to AML/CFT best practices has become almost a ritual at the SIC, and is considered a high level professional education. On-job training provides learning through experience where acquired knowledge is shared through discussions and brainstorming sessions, while feedback and communication among units and levels perfects the understanding of an efficient AML/CFT regime.

Participation in off-job training events such as seminars and workshops organized in Lebanon jointly by the SIC and other bodies or abroad (US Federal Reserve, Banque de France, Australian Federal Police, etc.) is also intended for this purpose. Moreover, visits to FIUs such as Tracfin, FinCEN and Austrac, to name a few, are intended to grow relationships and to allow the sharing of expertise.

Whether staff attended local, regional or international training events, the in-house Continuous Professional Education (CPE) program is intended to complement SIC training initiatives by exposing staff to the standards and ML/TF trends. Special attention is also given to the training needs of other national agencies that make up for the AML/CFT regime, in addition to reporting entities from the financial sector and DNFBPs.
### LOCAL & INTERNATIONAL TRAINING

<table>
<thead>
<tr>
<th>Date</th>
<th>Organizer</th>
<th>Event / Location</th>
<th>No. of SIC Staff Attending</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Q'22</td>
<td>UNODC</td>
<td>Financial Disruption Workshop - International Money Laundering Networks (Hybrid)</td>
<td>3</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>MENAFATF / FATF</td>
<td>Lebanon Mutual Evaluation Country Training (Virtual)</td>
<td>10</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>Egmont Group - ECOFEL / MENAFATF</td>
<td>Regional Workshop on Information Sharing between FIUs/Supervisory Agencies/LEAs (Virtual)</td>
<td>2</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>FATF</td>
<td>Session on the RBA Guidance to the Real Estate Sector (Virtual)</td>
<td>6</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>Egmont Group/GAFILAT/FLI Ecuador</td>
<td>Webinar on Beneficial Ownership (Virtual)</td>
<td>2</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>Egmont Group - MENA Regional Group</td>
<td>Session on How to Improve the Request for Information among Egmont Group Members (Virtual)</td>
<td>1</td>
</tr>
<tr>
<td>1st Q'22</td>
<td>OECD</td>
<td>Global Anti-Corruption &amp; Integrity Forum (Virtual)</td>
<td>3</td>
</tr>
</tbody>
</table>

| 2nd Q'22 | The EU AML/CFT Global Facility / The French Embassy in Jordan | Regional Workshop on “Forensic Audit in the fight against Money Laundering” (Amman, Jordan) | 1                          |
| 2nd Q'22 | FATF/ MENAFATF | FATF Standards Training Course (Virtual)                                      | 2                          |
| 2nd Q'22 | The EU AML/CFT Global Facility | Regional Conference on “The use of AML /CFT in the investigation of Art and Antiquities Criminality” (Cairo, Egypt) | 1                          |
| 2nd Q'22 | World Bank | Training on “Proceeds of Crimes and Illicit Financial Flows Data Collection Tool” (Virtual) | 1                          |
| 2nd Q'22 | K2 Integrity/SIC | Training on:  
  - Financial Crimes  
  - Enhanced Due Diligence measures  
  - Global Sanctions and Combating Corruption (Virtual) | 5                          |
<table>
<thead>
<tr>
<th>Date</th>
<th>Organizer</th>
<th>Event/Location</th>
<th>No. of SIC Staff Attending</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Q’22</td>
<td>FATF</td>
<td>Webinar on Beneficial Ownership Transparency of Legal Persons (Virtual)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Egmont Group / MENAFATF</td>
<td>Webinar on “Virtual Assets Supervision and Investigation” (Virtual)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>BDL / Basil Fuleihan Institute for Economy and Finance</td>
<td>Training on the Public Procurement Law No. 244/2021 (Beirut, Lebanon)</td>
<td>1</td>
</tr>
<tr>
<td>4th Q’22</td>
<td>MENAFATF / The German Agency for International Cooperation (GIZ)</td>
<td>Training Webinar on Enhancing Transparency on Beneficial Ownership (Virtual)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>OECD International Academy for Tax and Financial Crime Investigation</td>
<td>Managing Financial Investigations (Intermediate) Programme for the MENA Region (Virtual)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Saudi Arabia Financial Investigation Unit (SAFIU)</td>
<td>Comprehensive Training Program on AML/CFT - Risk Assessment and Customer Due Diligence measures and Targeted Sanctions for ML and TF (Riyadh, Kingdom of Saudi Arabia)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>The ACT project team / The Presidency of the Council of Ministers</td>
<td>High-level workshop on Cryptocurrencies (Beirut, Lebanon)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>UNOCT / MENAFATF / Kingdom of Morocco</td>
<td>Workshop on Terrorism Financing Regional Risk Assessment (Hybrid)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>Standards Training Course Train-the-Trainer (Busan, Korea)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>The EU AML/CFT Global Facility / Jordanian National AML &amp; CFT Committee / MENAFATF</td>
<td>Regional Conference on “Dealing with Virtual Assets and AML / CFT - From Risk Assessment to Asset Freezing of Virtual Assets, methodology and best practices in Middle East and North Africa region” (Amman, Jordan)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>The ACT project team / The Presidency of the Council of Ministers</td>
<td>High-level seminar on Counter Terrorism (CT) Coordination Mechanisms (Beirut, Lebanon)</td>
<td>1</td>
</tr>
</tbody>
</table>
The SIC co-sponsored 4 FIUs from the MENA region. To date, 3 of them have joined the Egmont Group.

The SIC has provided training and technical assistance to several FIUs from the MENA region.

To date, several SIC and Lebanese LEA staff participated as assessors in seventeen Mutual Evaluation Missions for several countries.
Globalization and the interconnection of world economies and financial systems, in addition to new technologies that allow for swift movement of funds around the globe, necessitate stronger cooperation to better fight organized crime and the flow of illicit funds. To address the threats at hand, the SIC realized, early on, the importance of providing AML/CFT technical assistance especially to counterparts in the region. This stems from its strong belief that money laundering (and its predicate offences), terrorism financing and proliferation financing are crimes that can be best fought, not only by domestic cooperation, but also by collective efforts of counterpart FIUs and other foreign competent agencies.

Reach out efforts over the years in the form of technical assistance and other engagements were carried out by the SIC on its own or in partnership with regional and international bodies such as MENAFATF, FATF, UNODC, World Bank, IMF and the Egmont Group. SIC’s expertise were channeled to several FIUs to satisfy their needs for technical assistance and training. Tailored programs were designed to accommodate these needs, notably in compliance, policy drafting, information analysis, IT & security, and supervision of reporting entities. Technical assistance programs also comprised providing regional FIUs and bank supervisors with AML/CFT training. Moreover, seconding SIC staff on missions including on mutual evaluation missions with international bodies and standing out as guest speakers in different regional and international events on topics such as AML/CFT compliance, FATF international standards, FIU operations and ML/TF trends while providing sanitized cases derived from the SIC rich experience compliment such efforts. This is all done on the back of the SIC commitment to providing technical assistance and enhancing regional cooperation.

The SIC presence in plenary meetings (MENAFATF, EGMONT & FATF) and active involvement in working groups and projects as well as its previous involvement in the FATF Middle East & Africa Regional Review Group (RRG) to review the progress reports of jurisdictions brought within the ICRG process also paid off. Such efforts resulted in bringing several FIUs from MENAFATF member countries to full Egmont Group membership and in raising compliance levels to international standards.

The SIC has grown accustomed to quality work with international and regional bodies. Be it in engagements such as joint Egmont/FATF typologies workshops, and in projects such as: the FATF Global Threat Assessment (GTA), the Experts Group work on amendments to the FATF recommendations and in EG’s charter review project as well as the EG ISIL project. Going forward, and in spite the fact that such contributions require lots of resources, their rewarding outcome leads the SIC to continue on this path.
## Technical Assistance & Other Engagements

<table>
<thead>
<tr>
<th>Date</th>
<th>Organizer</th>
<th>Event/Location</th>
<th>No. of SIC Staff Involved</th>
<th>Type of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Q’22</td>
<td>Special Inquiry, Technical Assistance (SIC)</td>
<td>ML/TF National Risk Assessment Private Sector Consultation (Beirut, Lebanon)</td>
<td>1</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>Special Inquiry, Technical Assistance (SIC)</td>
<td>Awareness raising sessions on the “2022 ML/TF National Risk Assessment Update results &amp; mitigating measures” (Beirut, Lebanon)</td>
<td>1</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups meetings (Hybrid)</td>
<td>4</td>
<td>Participants</td>
</tr>
<tr>
<td>2nd Q’22</td>
<td>MENAFATF</td>
<td>The 34th MENAFATF Plenary &amp; Working Groups Meetings (Virtual)</td>
<td>9</td>
<td>Delegation</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>6</td>
<td>Participants</td>
</tr>
<tr>
<td>3rd Q’22</td>
<td>Special Inquiry, Technical Assistance (SIC)</td>
<td>Egmont Plenary and Working Groups Meetings (Riga, Latvia)</td>
<td>1</td>
<td>Delegation</td>
</tr>
<tr>
<td></td>
<td>BDL</td>
<td>Internship Program: Lebanon’s experience in fighting ML/TF (Beirut, Lebanon)</td>
<td>1</td>
<td>Speaker</td>
</tr>
<tr>
<td>4th Q’22</td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>3</td>
<td>Participants</td>
</tr>
<tr>
<td></td>
<td>MENAFATF</td>
<td>MEWG exceptional meeting for reviewing Procedures for the 2nd round of Mutual Evaluations and Follow-up Process (Virtual)</td>
<td>5</td>
<td>Delegation</td>
</tr>
<tr>
<td></td>
<td>MENAFATF</td>
<td>The 35th MENAFATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>3</td>
<td>Delegation</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>Financial Disruption Workshop - International Money Laundering Networks (Virtual)</td>
<td>1</td>
<td>Speaker</td>
</tr>
</tbody>
</table>
## Secretary General Engagements

<table>
<thead>
<tr>
<th>Date</th>
<th>Organizers</th>
<th>Event/Location</th>
<th>Type of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Q'22</td>
<td>Egmont Group</td>
<td>Egmont Working Groups Meetings (Virtual)</td>
<td>Head of Delegation</td>
</tr>
<tr>
<td></td>
<td>MENAFATF / FATF</td>
<td>Lebanon Mutual Evaluation Country Training (Virtual)</td>
<td>Opening Speech</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>The EU AML/CFT Global Facility/The Siracusa International Institute for Criminal Justice and Human Rights</td>
<td>Regional Conference on Strengthening Judicial Cooperation in the MENA Region: Judges and Prosecutors at the Forefront of the Fight against Money Laundering and Terrorism Financing (Manama, Bahrain)</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>Egmont Group - MENA Regional Group</td>
<td>Session on How to Improve the Request for Information among Egmont Group Members (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>OECD</td>
<td>Global Anti-Corruption &amp; Integrity Forum (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td>2nd Q'22</td>
<td>MENAFATF</td>
<td>The 34th MENAFATF Plenary &amp; Working Groups Meetings (Virtual)</td>
<td>Head of Delegation</td>
</tr>
<tr>
<td></td>
<td>K2 Integrity / SIC</td>
<td>Session on Combating Corruption (Beirut, Lebanon)</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>Participant</td>
</tr>
<tr>
<td>3rd Q'22</td>
<td>Egmont Group</td>
<td>Egmont Plenary and Working Groups Meetings (Riga, Latvia)</td>
<td>Head of Delegation</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>The first resumed 13th session of the Implementation Review Group of the UNCAC (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td>Date</td>
<td>Organizers</td>
<td>Event/Location</td>
<td>Type of Involvement</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>4th Q’22</td>
<td>American University of Beirut</td>
<td>A ‘Fireside Chat’ on combating Financial Crimes and Money Laundering in the midst of the crisis in Lebanon (Beirut, Lebanon)</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>FATF</td>
<td>FATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>MENAFATF</td>
<td>MEWG exceptional meeting for reviewing Procedures for the 2nd round of Mutual Evaluations and Follow-up Process (Virtual)</td>
<td>Head of Delegation</td>
</tr>
<tr>
<td></td>
<td>MENAFATF</td>
<td>The 35th MENAFATF Plenary &amp; Working Groups Meetings (Hybrid)</td>
<td>Head of Delegation</td>
</tr>
<tr>
<td></td>
<td>UNOCT / MENAFATF / Kingdom of Morocco</td>
<td>Workshop on Terrorism Financing Regional Risk Assessment (Hybrid)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>The second resumed 13th session of the Implementation Review Group of the UNCAC (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>The 16th meeting of the Open-ended Intergovernmental Working Group on Asset Recovery (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>The 11th Open-ended Intergovernmental Expert Meeting to enhance International Cooperation under the UNCAC (Virtual)</td>
<td>Participant</td>
</tr>
<tr>
<td></td>
<td>UNODC</td>
<td>Financial Disruption Workshop - International Money Laundering Networks (Virtual)</td>
<td>Speaker</td>
</tr>
<tr>
<td></td>
<td>Al Iktissad Wal-Aamal Group/Union of Arab Chambers / Lebanese Economic Organisations</td>
<td>Arab Economic Forum (Beirut, Lebanon)</td>
<td>Participant</td>
</tr>
</tbody>
</table>
2022 Training, Technical Assistance & Other Engagements

Prior Years

N.B. Some countries visited in 2022 were also visited in prior years
During the Macao 2017 Egmont Group Plenary meeting, the World Bank-UNODC Stolen Asset Recovery Initiative presented, for the first time, a STAR Award of Excellence to the SIC and to another FIU. Both were recognized for investigating, freezing, and also for the successful repatriation of corruption related funds.
Selection of Typologies

**TERRORISM FINANCING**

**Report (ROA):** The SIC received a request of assistance through the General Prosecutor from the ISF - Information Division to identify accounts and transactions in a TF case involving several detainees accused of facilitating the travel of terrorist fighters to join ISIS.

**Analysis and Investigation:** The SIC initiated its investigation by circulating the names of the detained suspects to all banks, financial institutions and money remittance companies operating in Lebanon, as well as to the real estate register and the vehicle register. Bank accounts with minimal balances pertaining to one of the suspects were identified. Furthermore, outgoing/incoming transfers relating to four of the suspects were identified at two money remittance companies, in addition to a vehicle.

**Subsequent Measures:** The SIC decided to freeze the identified bank accounts, requested from all money transfer companies not to perform any transaction for the suspects, placed an encumbrance on the identified vehicle, and forwarded the findings to the General Prosecutor for further investigation.

**CORRUPTION**

**Report (STR):** The enhanced due diligence measures implemented towards high-risk customers and the robust transaction monitoring in place to fight corruption associated with public sector dealings, alerted a bank to file with the SIC a suspicious transaction report on a customer’s account that had received transfers from an international organization executing projects in Lebanon. The account activity review revealed that the funds were withdrawn in cash thus making it difficult to confirm their use, and supporting documents that justify disbursements were not provided.

**Analysis and Investigation:** The SIC initiated its work by obtaining all related documents, bank statements and available EDD information. The SIC also obtained a copy of the contract signed between the customer and the international organization, which included project details and valuation, in addition to financial statements and invoices issued to the international organization. The analysis of the bank account revealed that it was credited with incoming transfers worth a few million dollars, of which more than 50% were withdrawn in cash, with amounts transferred to the customer’s personal account.

**Subsequent Measures:** The SIC decided to lift banking secrecy off the identified bank account and forwarded the findings to the General Prosecutor.
CORRUPTION

Report (STR): The compliance officer at a local bank filed a suspicious transaction report with the SIC after coming across negative press articles and media reports concerning a non-profit organization that had an agreement with a public administration to conduct laboratory tests.

Analysis and Investigation: The SIC obtained from the bank all related documents and statements. The review of the contract signed between the non-profit organization and the public administration, revealed that it contains clauses for the distribution of proceeds generated from the laboratory tests with a mandatory clause for using part of the proceeds to finance health care projects. The analysis of the bank account revealed that it was credited with transfers that were withdrawn in cash, making it difficult to verify that the proceeds intended for the health care projects were allocated accordingly.

Subsequent Measures: The SIC decided to lift banking secrecy of the non-profit organization’s bank account and forwarded the findings to the General Prosecutor.

CORRUPTION

Report (ROA): The SIC received a request of assistance through the General Prosecutor from the ISF - Information Division concerning ongoing investigations with government employees accused of embezzling public funds, corruption and generating illicit proceeds.

Analysis and Investigation: The SIC initiated its work by circulating the names of the suspects to all banks, financial institutions and money remittance companies operating in Lebanon. Bank accounts were identified for the suspects at several banks, and minimal transactions were executed through two money remittance companies. The analysis of the bank accounts revealed cash deposits below the ten thousand dollars threshold, with totals exceeding in some accounts the suspects’ salaries that were consequently withdrawn in cash. Furthermore, information obtained by the SIC from the real estate register and the vehicle register revealed ownerships.

Subsequent Measures: The SIC froze the balances of identified accounts, requested from all money remittance companies not to perform any transaction for the suspects, and placed an encumbrance on the identified properties and vehicles. All findings were forwarded to the General Prosecutor for further investigation.
**DRUG TRAFFICKING**

**Report (ROA):** The SIC received a request of assistance through the General Prosecutor from the ISF - Combating Financial Crimes & ML Office concerning investigations with individuals accused of drugs related crimes.

**Analysis and Investigation:** A search of the SIC database revealed that several of the accused individuals were subject to previous investigations that resulted in freezing their accounts, and forwarding the findings to the General Prosecutor. The SIC circulated the names of the remaining individuals to all banks, financial institutions and money remittance companies operating in Lebanon in search of bank accounts and financial transactions. The SIC also requested information from several domestic agencies including the real estate register and the vehicle register. The analysis of the identified accounts revealed minimal transactions, and some suspects had incoming/outgoing transfers executed at three money remittance companies, and ownership of real estate.

**Subsequent Measures:** The SIC froze the balances of identified accounts, requested from all money remittance companies not to perform any transaction for the suspects, and placed an encumbrance on the identified properties. All findings were forwarded to the General Prosecutor for further investigation.

---

**SMUGGLING**

**Report (STR):** A bank filed with the SIC a suspicious transaction report on a customer after suspecting that imported subsidized goods intended for sale in the local market were smuggled and sold abroad.

**Analysis and Investigation:** The SIC initiated its investigation by obtaining all bank records, including KYC forms and identification documents pertaining to the customer, related individuals and companies. During its analysis work, the SIC received information from the ISF - Combating Financial Crimes & ML Office revealing investigations with the same customer for smuggling subsidized goods and embezzling public funds, and that his company was ordered to shut down. The SIC expanded its analysis by circulating the name of the customer, related individuals and companies to all bank, financial institutions and money remittance companies operating in Lebanon, as well as to the real estate register and the vehicle register. Additional bank accounts identified for the customer, and for related individuals and companies were analyzed.

**Subsequent Measures:** The SIC decided to freeze the balances of the identified bank accounts, requested from all money remittance companies not to perform any transaction for the suspect, placed an encumbrance on the identified properties and forwarded the findings to the General Prosecutor.
COUNTERFEITING OF PRODUCTS

Report (ROA): The SIC received a request of assistance through the General Prosecutor from the ISF - Combating Financial Crimes & ML Office concerning a suspect being investigated for importing counterfeited and expired goods, falsifying their validity date and generating illicit returns.

Analysis and Investigation: The SIC circulated the name of the suspect to all banks, financial institutions and money remittance companies in order to identify related transactions and bank accounts. Accounts for the suspect were identified at two banks along with transactions performed at three money remittance companies. The SIC obtained all available CDD information, including KYC forms, related bank records and transactions executed at the money remittance companies, and carried out the needed analysis which revealed recurrent cash deposits below the ten thousand dollars threshold.

Subsequent Measures: The SIC froze the balances of the identified accounts, requested from all money remittance companies not to perform any transaction for the suspect and forwarded the findings to the General Prosecutor for further investigation.
International & Regional Organizations
• The Egmont Group of Financial Intelligence Units (EG) was formed in 1995 and derived its name from the “Egmont-Arenberg Palace” in Brussels – Belgium where the first meeting was held.

• The EG is a non-political international forum of operational Financial Intelligence Units (FIUs).

• The EG goal is to provide a forum for FIUs to improve cooperation in the fight against money laundering and terrorism financing.

• The EG member FIUs must meet the FATF definition of an FIU and have full operational status.

• The EG grown from 13 FIUs in 1995 to 166 FIUs by year-end 2022.

• The EG comprises 14 FIUs from the MENA region.

• The EG operating structure is comprised of: the Heads of FIUs (HoFIUs), the Chair of the EG, the Egmont Committee (EC), the Working and Regional Groups, and the Secretariat.

• The EG governing body is the HoFIUs and their decisions are taken by consensus.

• The Egmont Committee serves as a consultative and coordination body for the HoFIUs.

• There are four Working Groups within the EG, each has a Chair and Vice Chairs:
  - Information Exchange on ML/TF WG
  - Membership, Support & Compliance WG
  - Policy & Procedures WG
  - Technical Assistance & Training WG

• There are eight Regional Groups within the EG:
  - Asia & Pacific (28 FIUs)
  - Americas (39 FIUs)
  - Europe I (29 FIUs)
  - Europe II (24 FIUs)
  - East & Southern Africa (14 FIUs)
  - Middle East & Northern Africa (14 FIUs)
  - West & Central Africa (11 FIUs)
  - Eurasia (7 FIUs)

• The Egmont Secure Web (ESW) is the electronic communication system that allows encrypted sharing of e-mails, financial intelligence and other information among EG member FIUs.

• The Egmont Group Secretariat (EGS) is located in Ottawa-Canada and provides strategic, administrative and other support to the EG activities.

• The EG has its own charter as well as principles for information exchange that were last updated in July 2013 in the South Africa EG plenary.
• The SIC joined the EG in 2003, and was among the first from the MENA region.
• The SIC is active in the work of EG Working Groups.
• The SIC co-sponsored a number of MENA FIUs to obtain EG membership, and has also provided technical assistance to FIUs.
• The SIC participated in the Charter Review Project and in the Task Team that worked on the implementation of the EG Strategic Plan for 2014 – 2017.
• In January 2015, the SIC Secretary General was elected as the MENA Regional Representative. The main roles and functions of the Regional Representatives include with respect to their regions the following:
  • Representing their regions in the EC, and communicating FIUs developments, views and interests to the EC.
  • Developing a regional action plan in coordination with FIUs and ensuring its effective implementation.
  • Facilitating & coordinating training and technical assistance for FIUs as needed.
  • Assisting in identifying, where applicable, possible sponsors for candidate FIUs.
  • Engaging, as appropriate, in all aspects of the Support & Compliance Process.
• In June 2015, the SIC Secretary General was appointed as Vice Chair of the Egmont Committee. The main roles and functions of the EC Vice Chairs include:
  • Supporting and advising the EG Chair on matters affecting the EG.
  • Representing the EG in ceremonial duties as needed.
  • Acting as a Chair in the absence of the EG Chair.
• In 2016, the SIC joined the team working on the “Egmont Centre of FIU Excellence and Leadership (ECOFEL)” project.
• In July 2017, and during the Macao Egmont Group Plenary meeting:
  • The SIC Secretary General was re-elected as the EG MENA Regional Representative for a second consecutive term of two-years. The SIC Secretary General was also re-appointed as Vice Chair of the Egmont Committee.
  • The World Bank-UNODC Stolen Asset Recovery Initiative presented, for the first time, a STAR Award of Excellence to the SIC and to another FIU. Both were recognized for investigating, freezing, and also for the successful repatriation of corruption related funds.
• In 2018, the SIC organized along with other partners, and with the support of the Egmont Group, the “Arab Forum for Anti-Corruption Agencies and Financial Intelligence Units” that was held in Beirut.
• In 2019 & 2020, the SIC co-led a project on the revision of certain elements of the EG Support & Compliance Process.
• During year 2022, the SIC Compliance Unit Director assumed the position of MSCWG-Vice Chair.
About MENAFATF

- MENAFATF is a FATF Style Regional Body (FSRB) established in 2004 at an inaugural meeting held in Bahrain. It is independent from any other international body or organization, and is voluntary and co-operative in nature.

- MENAFATF member countries are committed to a Memorandum of Understanding that aims to achieve the following main objectives:
  - Adopt & implement FATF 40 recommendations
  - Cooperate among each other to raise compliance with FATF standards within the MENA region and cooperate with other international & regional organizations to improve compliance
  - Work jointly to identify issues of regional nature related to ML & TF, and to share relevant experiences & develop solutions for dealing with them

- MENAFATF member countries also commit to participate in mutual evaluation programs which the Plenary adopts, and to participate in other MENAFATF activities.

- MENAFATF sets its own work, regulations and procedures and cooperates with other international bodies, notably the FATF, to reach its objectives.

- MENAFATF decisions are taken in the Plenary meeting either unanimously or by consensus.

- Membership has grown from 14 countries in 2004 to 21 countries by year-end 2020.

- There are two Working Groups (WGs) within MENAFATF:
  - Technical Assistance and Typologies Working Group (TATWG)
  - Mutual Evaluation Working Group (MEWG)

- Observer countries are:
  - Republic of France
  - United States of America
  - United Kingdom of Great Britain & Northern Ireland
  - Kingdom of Spain
  - Australia
  - Federal Republic of Germany
  - The Russian Federation

- Observer institutions/organizations are:
  - International Monetary Fund
  - World Bank
  - Co-operation Council for the Arab States of Gulf
  - Financial Action Task Force
  - Egmont Group of FIUs
  - Asia/Pacific Group on Money Laundering
  - World Customs Organization
  - Arab Monetary Fund
  - Eurasian Group on combating money laundering and financing of terrorism
  - United Nations
  - European Commission

- MENAFATF Secretariat is headquartered in the Kingdom of Bahrain.

- MENAFATF is an Associate Member of FATF, a status shared with eight other FSRBs.
Lebanon is a founding member of MENAFATF, it played an important role in its creation, and assumed its first year Presidency in 2005.

The SIC represents Lebanon in MENAFATF.

The SIC is actively involved in MENAFATF Working Groups activities & projects.

The SIC participates in the MENAFATF delegation to FATF Plenary and WG meetings.

In 2009, MENAFATF carried an assessment of Lebanon’s AML/CFT regime and adopted Lebanon’s Mutual Evaluation Report (MER). Nine follow-up progress reports were submitted by the SIC pursuant to the said MER.

Assessors from Lebanon participated in mutual evaluation missions of several MENA countries.

In 2017, Lebanon represented by the SIC, assumed the Vice Presidency of MENAFATF.

In 2018, Lebanon represented by the SIC, assumed the MENAFATF Presidency.

In 2018, the SIC organized in collaboration with MENAFATF and other organizations:
- The “Arab Forum for Anti Corruption Agencies and Financial Intelligence Units” that was held in Beirut.
- The “Fourth Anti-Cybercrime Forum”

In 2019, the SIC assumed a leading role in the oversight of the implementation of the joint MENAFATF / FATF action plan.

In 2020, the SIC was involved through MENAFATF in the works of the FATF ad-hoc group on strategic review (AGSR).

As part of the evaluation process, the MENAFATF assessment team concluded its onsite visit to Lebanon.

During year 2022, the SIC Compliance Unit Director assumed the position of TATWG - Co-Chair.

\[\text{Note: Russia is also a member of MONEYVAL while China & India are also members of APG}\]
The National Committee for Coordinating AML Policies

As is the case for all inter-agency committees, the National Committee for Coordinating AML Policies plays an important role in addressing challenges and fostering coordination and cooperation among Lebanese agencies involved in the fight against money laundering. The Committee is engaged in Lebanon’s ML/TF risk assessments and serves as a forum to exchange views and suggestions informed by the risks identified, leading up to the adoption and constant review of a national AML strategy and policies that aim to enhance Lebanon’s AML regime. Moreover, it serves as a platform for follow up to ensure that the said strategy and policies are being implemented.

In addition, keeping track of evolving AML international standards and recommending how such standards should be tailored and integrated into laws, regulations or best practices, remain at the core of the Committee’s work and a top priority in its periodic meetings.

MILESTONES

• Suggested by the Governor of Banque du Liban in September 2002.
• Established by the Lebanese Council of Ministers in October 2002.
• Comprised of Banque du Liban’s Vice Governor as Chair, with members including the SIC Secretary General, representatives from the General Prosecutor, Banking Control Commission, Customs Directorate and the Internal Security Forces.
• Assigned with tasks including improving coordination among concerned national authorities.
• Chaired by Banque du Liban’s Vice Governor Dr. Marwan Nsouli (2002 – 2008).
• Suggested expansion to include additional authorities as members made by the Governor of Banque du Liban in August, 2007.
• Expanded by the Lebanese Council of Ministers in September 2007 to include representatives from the Ministry of Justice, Ministry of Finance, Ministry of Interior & Municipalities, Ministry of Foreign Affairs, Ministry of Economy & Trade and Beirut Stock Exchange.
• Chaired by Banque du Liban’s Vice Governor Dr. Muhammad Baasiri (2009 – April 2019).
• Chaired by the Governor of Banque du Liban (April 2019 – present).
The **National Committee** on Suppressing **Terrorism Financing**

With the threat of “terrorism finance” on the rise and with the negative impact that such a crime has on countries, their financial sectors, and societies at large, the Lebanese Council of Ministers established in 2007 the National Committee on Suppressing Terrorism Financing. This was done to ensure that concerned national agencies are doing their best to fight and keep away this phenomenon.

Bringing together professionals on the matter to share expertise, knowledge and keep track of evolving international standards is of utmost concern to the Committee. The Committee is engaged in Lebanon’s ML/TF National Risk Assessments, and since its establishment, its periodic meetings focus on recommending to the Council of Ministers actions and policies that aim to address identified TF risks and to keep the country’s CFT efforts at par with international standards, including with respect to non-profit organizations.

### MILESTONES

- **Suggested by the Governor of Banque du Liban in August 2007.**
- **Established by the Lebanese Council of Ministers in September 2007.**
- **Headed by the Ministry of Interior & Municipalities and includes members representing the Ministry of Justice, Ministry of Finance, Ministry of Foreign Affairs, General Prosecutor Office, Special Investigation Commission and Banque du Liban.**
- **Chaired by the representative of the Ministry of Interior & Municipalities, the Director General of the Lebanese Internal Security Forces, Gen. Ashraf Rifi, (2007 – 2013).**
- **Chaired by the representative of the Ministry of Interior & Municipalities, the Director General of the Lebanese Internal Security Forces, Gen. Ibrahim Basbous, (2013 – 2017).**
- **Adopted in December 2015 two Targeted Financial Sanctions Mechanisms for UNSCRs 1267 & 1373 in accordance with FATF Recommendation No. 6.**
- **Chaired by the representative of the Ministry of Interior & Municipalities, the Director General of the Lebanese Internal Security Forces, Major General Imad Osman since March 2017.**
SECTION II

Statistical Data

1. Cases Received

2. Bank Secrecy Lifted & Information Provided

3. Breakdown of Cases by Predicate Offence

4. Terrorism or Terrorism Finance Related Cases

5. Handling Breakdown

6. Breakdown by Source & Type

7. Source of Foreign ROAs

8. Geographic Distribution of STRs

   - Nature of Specified Crimes
   - Forgery
   - Cybercrime
   - Spontaneous Disclosures

10. AML/CFT Onsite Compliance Examinations

66  66  67  68  69  70  71  72  73  74  75  76
### Cases Received

**469 CASES RECEIVED**
From Local & Foreign Sources

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% of Received Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>346</td>
<td>73.8%</td>
</tr>
<tr>
<td>Foreign</td>
<td>123</td>
<td>26.2%</td>
</tr>
</tbody>
</table>

### STATUS OF RECEIVED CASES

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% Passed on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>294</td>
<td>62.7%</td>
</tr>
<tr>
<td>Foreign</td>
<td>139</td>
<td>29.6%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% of Investigated Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>174</td>
<td>89.9%</td>
</tr>
<tr>
<td>Foreign</td>
<td>120</td>
<td>89.2%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% of Investigated Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>137</td>
<td>99.2%</td>
</tr>
<tr>
<td>Foreign</td>
<td>2</td>
<td>99.0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>35</td>
<td>17.0%</td>
</tr>
<tr>
<td>Foreign</td>
<td>1</td>
<td>9.1%</td>
</tr>
</tbody>
</table>

Note: The 38 pending cases mentioned in year 2021 annual report were resolved as follows:
28 Passed on, and 10 not passed on.

### Bank Secrecy Lifted & Information Provided

**230 CASES** in which Information was provided (Including covered by Bank Secrecy)

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% Information Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>121</td>
<td>73.8%</td>
</tr>
<tr>
<td>Foreign</td>
<td>109</td>
<td>26.2%</td>
</tr>
</tbody>
</table>

**64 CASES** in which Bank Secrecy was lifted

<table>
<thead>
<tr>
<th>Type</th>
<th>Number</th>
<th>% Bank Secrecy Lifted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>53</td>
<td>10.1%</td>
</tr>
<tr>
<td>Foreign</td>
<td>11</td>
<td>0.8%</td>
</tr>
</tbody>
</table>

### Received Cases vs. Investigated Cases vs. Passed on vs. Pending Cases

<table>
<thead>
<tr>
<th>Received Cases</th>
<th>Investigated Cases</th>
<th>Passed on*</th>
<th>Information Provided</th>
<th>Bank Secrecy Lifted</th>
<th>Pending Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Number</td>
<td>% of Cases</td>
<td>Number</td>
<td>Number</td>
<td>Number</td>
</tr>
<tr>
<td>Local</td>
<td>346</td>
<td>89.9%</td>
<td>121</td>
<td>38.9%</td>
<td>35</td>
</tr>
<tr>
<td>Foreign</td>
<td>123</td>
<td>99.2%</td>
<td>109</td>
<td>89.3%</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>% of Cases</th>
<th>Number</th>
<th>% of Cases</th>
<th>Number</th>
<th>% of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>53</td>
<td>17.0%</td>
<td>1</td>
<td>9.0%</td>
<td>1</td>
</tr>
<tr>
<td>Foreign</td>
<td>1</td>
<td>10.1%</td>
<td>11</td>
<td>0.8%</td>
<td>11</td>
</tr>
</tbody>
</table>

Total

<table>
<thead>
<tr>
<th>Number</th>
<th>% of Cases</th>
<th>Number</th>
<th>% of Cases</th>
<th>Number</th>
<th>% of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>469</td>
<td>92.3%</td>
<td>433</td>
<td>53.1%</td>
<td>64</td>
<td>14.8%</td>
</tr>
</tbody>
</table>

*Cases forwarded to GP and/or requesting authorities
## Breakdown of Cases by Predicate Offence*

<table>
<thead>
<tr>
<th>Offence</th>
<th>Local Cases</th>
<th>Foreign Cases</th>
<th>Total Cases</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgery</td>
<td>41</td>
<td>2</td>
<td>43</td>
<td>10.2%</td>
</tr>
<tr>
<td>Fraud</td>
<td>32</td>
<td>2</td>
<td>34</td>
<td>8.1%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>36</td>
<td>0</td>
<td>36</td>
<td>8.6%</td>
</tr>
<tr>
<td>Corruption</td>
<td>22</td>
<td>16</td>
<td>38</td>
<td>9.0%</td>
</tr>
<tr>
<td>Trade of Narcotics</td>
<td>49</td>
<td>4</td>
<td>53</td>
<td>12.6%</td>
</tr>
<tr>
<td>Embezzlement of Private Funds</td>
<td>16</td>
<td>4</td>
<td>20</td>
<td>4.8%</td>
</tr>
<tr>
<td>Terrorism or TF</td>
<td>22</td>
<td>8</td>
<td>30</td>
<td>7.1%</td>
</tr>
<tr>
<td>Tax Evasion</td>
<td>3</td>
<td>62</td>
<td>65</td>
<td>15.5%</td>
</tr>
<tr>
<td>Smuggling</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0.7%</td>
</tr>
<tr>
<td>Insider Trading</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0.7%</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Illegal Arms Trade</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0.7%</td>
</tr>
<tr>
<td>Embezzlement of Private Funds</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>Counterfeiting of goods</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Not Specified</td>
<td>68</td>
<td>20</td>
<td>88</td>
<td>21.0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>297</strong></td>
<td><strong>123</strong></td>
<td><strong>420</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

*Excluding 4 Customs Cross Border Cash Cases and 45 Banking Control Commission Administrative Assistance Cases.
## Terrorism or Terrorism Finance Related Cases

### Received

<table>
<thead>
<tr>
<th>Source</th>
<th>No. of Cases</th>
<th>No. of Suspects</th>
<th>% of Received</th>
<th>No. of Cases</th>
<th>% of Received</th>
<th>No. of Cases</th>
<th>% of Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money Remittance Companies</td>
<td>13</td>
<td>17</td>
<td>100.0%</td>
<td>13</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>Police</td>
<td>5</td>
<td>48</td>
<td>100.0%</td>
<td>5</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>Banks</td>
<td>2</td>
<td>2</td>
<td>100.0%</td>
<td>2</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>Ministries</td>
<td>2</td>
<td>11</td>
<td>100.0%</td>
<td>2</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Total Local</strong></td>
<td><strong>22</strong></td>
<td><strong>78</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>22</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>0</strong></td>
<td><strong>0.0%</strong></td>
</tr>
<tr>
<td>Interpol</td>
<td>1</td>
<td>13</td>
<td>100.0%</td>
<td>1</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>UN Security Council</td>
<td>3</td>
<td>4</td>
<td>100.0%</td>
<td>3</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>FIUs</td>
<td>4</td>
<td>11</td>
<td>100.0%</td>
<td>4</td>
<td>100.0%</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Total Foreign</strong></td>
<td><strong>8</strong></td>
<td><strong>28</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>8</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>0</strong></td>
<td><strong>0.0%</strong></td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td><strong>30</strong></td>
<td><strong>106</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>30</strong></td>
<td><strong>100.0%</strong></td>
<td><strong>0</strong></td>
<td><strong>0.0%</strong></td>
</tr>
</tbody>
</table>

### Breakdown by Source

- **Local**: 73%
- **Interpol**: 14%
- **UN Security Council**: 10%
- **FIUs**: 3%

### No. of Suspects Involved

- **Local**: 78
- **Interpol**: 13
- **FIUs**: 11
- **UN Security Council**: 4
Handling Breakdown

<table>
<thead>
<tr>
<th></th>
<th>1st Q’20</th>
<th>2nd Q’20</th>
<th>3rd Q’20</th>
<th>4th Q’20</th>
<th>Annual Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No.</td>
<td>% of Q1 Total</td>
<td>No.</td>
<td>% of Q2 Total</td>
<td>No.</td>
</tr>
<tr>
<td>STR</td>
<td>47</td>
<td>48.0%</td>
<td>58</td>
<td>39.7%</td>
<td>48</td>
</tr>
<tr>
<td>ROA</td>
<td>51</td>
<td>52.0%</td>
<td>88</td>
<td>60.3%</td>
<td>73</td>
</tr>
<tr>
<td>CBR</td>
<td>0</td>
<td>0.0%</td>
<td>0</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0.0%</td>
<td>0</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>98</strong></td>
<td><strong>100%</strong></td>
<td><strong>146</strong></td>
<td><strong>100%</strong></td>
<td><strong>121</strong></td>
</tr>
</tbody>
</table>

Note: The above does not include 27 Spontaneous Disclosures received / Processed.
## Statistical Data

### Breakdown by Source & Type

<table>
<thead>
<tr>
<th>Source &amp; Type</th>
<th>Number</th>
<th>% of Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Suspicious Transaction Reports</strong></td>
<td>207</td>
<td>41.6%</td>
</tr>
<tr>
<td><strong>Customs (Cross Border Cash)</strong></td>
<td>4</td>
<td>0.8%</td>
</tr>
<tr>
<td>Police</td>
<td>110</td>
<td>22.1%</td>
</tr>
<tr>
<td>Ministries</td>
<td>2</td>
<td>0.4%</td>
</tr>
<tr>
<td>Banking Control Commission (Administrative Assistance)</td>
<td>45</td>
<td>9.0%</td>
</tr>
<tr>
<td><strong>Total Local Requests of Assistance</strong></td>
<td>157</td>
<td>31.5%</td>
</tr>
<tr>
<td>FIUs</td>
<td>52</td>
<td>10.4%</td>
</tr>
<tr>
<td>Foreign Ministries / Embassies</td>
<td>61</td>
<td>12.2%</td>
</tr>
<tr>
<td>Foreign Judicial Authorities</td>
<td>10</td>
<td>2.0%</td>
</tr>
<tr>
<td>UN Security Council</td>
<td>3</td>
<td>0.6%</td>
</tr>
<tr>
<td>Foreign Supervisory Authorities</td>
<td>2</td>
<td>0.4%</td>
</tr>
<tr>
<td>Interpol</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Foreign Law Enforcement Authorities</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td><strong>Total Foreign Requests of Assistance</strong></td>
<td>130</td>
<td>26.1%</td>
</tr>
<tr>
<td>FIUs</td>
<td>52</td>
<td>10.4%</td>
</tr>
<tr>
<td>Foreign Ministries / Embassies</td>
<td>61</td>
<td>12.2%</td>
</tr>
<tr>
<td>Foreign Judicial Authorities</td>
<td>10</td>
<td>2.0%</td>
</tr>
<tr>
<td>UN Security Council</td>
<td>3</td>
<td>0.6%</td>
</tr>
<tr>
<td>Foreign Supervisory Authorities</td>
<td>2</td>
<td>0.4%</td>
</tr>
<tr>
<td>Interpol</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Foreign Law Enforcement Authorities</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td><strong>Other (Local/Foreign Source)</strong></td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>498</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Note:** The above does not include 27 Spontaneous Disclosures received/processed.
## Source of Foreign ROAs

<table>
<thead>
<tr>
<th>Region</th>
<th>No. of ROAs</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Europe</strong></td>
<td>86</td>
<td>66.2%</td>
</tr>
<tr>
<td>Denmark</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>France</td>
<td>63</td>
<td>48.5%</td>
</tr>
<tr>
<td>Germany</td>
<td>4</td>
<td>3.1%</td>
</tr>
<tr>
<td>Greece</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td>Ireland</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Latvia</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Lithuania</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Macedonia</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Malta</td>
<td>3</td>
<td>2.3%</td>
</tr>
<tr>
<td>Montenegro</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td>Spain</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Switzerland</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td><strong>Africa</strong></td>
<td>9</td>
<td>6.9%</td>
</tr>
<tr>
<td>Algeria</td>
<td>4</td>
<td>3.1%</td>
</tr>
<tr>
<td>Cape Verde Islands</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Nigeria</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td>Tunis</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td><strong>Middle East &amp; Gulf</strong></td>
<td>24</td>
<td>18.5%</td>
</tr>
<tr>
<td>Bahrain</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Iraq</td>
<td>13</td>
<td>10.0%</td>
</tr>
<tr>
<td>Jordan</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Kuwait</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Oman</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Qatar</td>
<td>3</td>
<td>2.3%</td>
</tr>
<tr>
<td>Syria</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td>UAE</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td><strong>North America</strong></td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>United States</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td><strong>Asia</strong></td>
<td>6</td>
<td>4.6%</td>
</tr>
<tr>
<td>Georgia</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Japan</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>2</td>
<td>1.5%</td>
</tr>
<tr>
<td>Russia</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Turkey</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>United Nations</td>
<td>3</td>
<td>2.3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>130</td>
<td>100%</td>
</tr>
</tbody>
</table>
Geographic Distribution of STRs

<table>
<thead>
<tr>
<th>Region</th>
<th>No. of STRs</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beirut</td>
<td>109</td>
<td>52.7%</td>
</tr>
<tr>
<td>Mount Lebanon</td>
<td>40</td>
<td>19.3%</td>
</tr>
<tr>
<td>South Lebanon</td>
<td>13</td>
<td>6.3%</td>
</tr>
<tr>
<td>North Lebanon &amp; Akkar</td>
<td>12</td>
<td>5.8%</td>
</tr>
<tr>
<td>Bekaa</td>
<td>12</td>
<td>5.8%</td>
</tr>
<tr>
<td>Keserwan/ Jbeil</td>
<td>10</td>
<td>4.8%</td>
</tr>
<tr>
<td>Nabatieh</td>
<td>6</td>
<td>2.9%</td>
</tr>
<tr>
<td>Baalbeck/Hermel</td>
<td>5</td>
<td>2.4%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>207</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

No. of STRs % of Total

Beirut 109 52.7%
Mount Lebanon 40 19.3%
South Lebanon 13 6.3%
North Lebanon & Akkar 12 5.8%
Bekaa 12 5.8%
Keserwan/ Jbeil 10 4.8%
Nabatieh 6 2.9%
Baalbeck/Hermel 5 2.4%
Total 207 100%
NATURE OF SPECIFIED CRIMES

Annual Report 2022

Strategic Analysis (2018 – 2022)

- Cybercrime
- Forgery
- Terrorism or TF
- Embezzlement of Private Funds
- Trade of Narcotics
- Corruption
- Fraud
- Tax Evasion
- Smuggling
- Other

Graph showing the percentage of specified crimes from 2018 to 2022.
FORGERY

- Checks: 65%
- Identification Documents: 16%
- Other: 15%
- Transfers: 3%
- Loan Instruments: 1%
- Banknotes: 0%

2018 2019 2020 2021 2022

- Checks
- Identification Documents
- Other
- Transfers
- Banknotes
- Loan Instruments
Note: The number of spontaneous disclosures exchanged with FIUs in the region in 2018 is primarily related to the efforts to counter the financing of ISIL and affiliates.
### AML/CFT Onsite Compliance Examinations

<table>
<thead>
<tr>
<th>Financial Sector Reporting Entities Coverage</th>
<th>Q1 Coverage</th>
<th>Q2 Coverage</th>
<th>Q3 Coverage</th>
<th>Q4 Coverage</th>
<th>Annual Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type</td>
<td>No. % of Q1 Total</td>
<td>No. % of Q2 Total</td>
<td>No. % of Q3 Total</td>
<td>No. % of Q4 Total</td>
</tr>
<tr>
<td>Banks</td>
<td>61</td>
<td>6 30%</td>
<td>7 12%</td>
<td>3 6%</td>
<td>5 8%</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>40</td>
<td>0 0%</td>
<td>0 0%</td>
<td>9 17%</td>
<td>8 13%</td>
</tr>
<tr>
<td>Insurance Companies</td>
<td>49</td>
<td>0 0%</td>
<td>15 25%</td>
<td>0 0%</td>
<td>0 0%</td>
</tr>
<tr>
<td>Money Dealers</td>
<td>298</td>
<td>14 70%</td>
<td>35 58%</td>
<td>35 69%</td>
<td>46 74%</td>
</tr>
<tr>
<td>Brokerage Firms</td>
<td>16</td>
<td>0 0%</td>
<td>0 0%</td>
<td>4 8%</td>
<td>0 0%</td>
</tr>
<tr>
<td>Money Remittance Companies</td>
<td>13</td>
<td>0 0%</td>
<td>3 5%</td>
<td>0 0%</td>
<td>3 5%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>20</td>
<td>100%</td>
<td>60 100%</td>
<td>51 100%</td>
<td>62 100%</td>
</tr>
</tbody>
</table>

- Covered (21)
- Not covered (40)
- Covered (130)
- Not covered (168)
- Covered (17)
- Not covered (23)
- Covered (15)
- Not covered (34)
- Covered (4)
- Not covered (12)

---

**Graph:**
- Banks
- Financial Institutions
- Insurance Companies
- Money Dealers
- Money Remittance Companies
- Brokerage Firms
In 2022, the risk-based onsite compliance examinations covered 21 banks, 130 money dealers, 6 money remittance companies, 17 financial institutions, 4 brokerage firms and 15 insurance companies, in addition to a number of DNFBPs.
Laws & Regulations

- Learn
- Understand
- Comply
SECTION III

AML/CFT Laws & Regulations

1. Law 44 81
2. Law 32 85
3. Law 42 86
4. Law 53 87
5. Law 55 87
6. Law 77 89
7. Law 214 89
8. BDL Basic Circular 83 92
9. BDL Basic Circular 1 Addressed to Collective Investments Schemes 102
10. BDL Basic Circular 1 Addressed to Financial Intermediation Institutions (Brokerage Firms) and Collective Investments Schemes 102
11. BDL Basic Circular 2 Addressed to Financial Institutions 107
12. BDL Basic Circular 2 Addressed to Specialized Lending Entities (Comptoirs) 108
13. BDL Basic Circular 3 (Section 5) 112
14. BDL Basic Circular 63 118
15. BDL Basic Circular 69 118
16. BDL Basic Circular 81 123
17. BDL Basic Circular 89 124
18. BDL Basic Circular 111 125
19. BDL Basic Circular 126 126
20. BDL Basic Circular 136 126
21. BDL Basic Circular 137 127
22. BDL Basic Circular 138 128
23. BDL Basic Circular 139 128
24. BDL Basic Circular 144 131
25. BDL Basic Circular 147 132
26. BDL Basic Circular 163 132
27. Capital Markets Authority Series 2000 & 3000 133
28. SIC Circular 1 134
29. SIC Circular 2 134
30. SIC Circular 4 amended by SIC Circular 13 134
31. SIC Circular 5 amended by SIC Circular 12 135
32. SIC Circular 7 137
33. SIC Circular 8 139
34. SIC Circular 9 139
35. SIC Circular 10 139
36. SIC Circular 11 140
37. SIC Circular 14 140
38. SIC Circular 15 141
39. SIC Circular 16 141
40. SIC Circular 18 141
41. SIC Circular 19 142
42. SIC Circular 20 142
43. SIC Circular 21 143
44. SIC Circular 22 144
45. SIC Circular 23 145
46. SIC Circular 24 145
47. SIC Circular 25 146
48. SIC Circular 26 147
49. SIC Circular 27 150
50. SIC Circular 28 151
Extortion

AML/CFT Law No. 44 – Predicate Offences
The draft law required by Decree No. 8200 of May 24, 2012 (amending Law No. 318 of April 20, 2001, on Fighting Money Laundering) is adopted, as amended by the subcommittee of the joint parliamentary committees and the Parliament.

**Article 1**
For the purpose of this Law, illicit funds include assets, tangible and intangible, movable and immovable, including any legal documents or instruments evidencing title to, or interest in, such assets, resulting from the commission of, or the punishable attempted commission of, or the participation in any of the following offences, whether in Lebanon or abroad:
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 terrorist 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. Incitement to debauchery and offence against ethics and public decency by way of organized gangs.
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.
20. Murder.
21. Tax evasion, in accordance with the Lebanese laws.

**Article 2**
Money laundering is any act committed with the purpose of:
1. Concealing the real source of illicit funds, or giving, by any means, a false justification regarding the said source, while being aware of the illicit nature of these funds.
2. Transferring or transporting funds, or substituting or investing the latter in purchasing movable or immovable assets or in carrying out financial transactions for the purpose of concealing or disguising the such funds’ illicit source, or assisting a person involved in the commission of any of the offences mentioned in Article 1 to avoid prosecution, while being aware of the illicit nature of these funds.

Money laundering is a separate offence that does not necessitate a charge with the underlying predicate offence. Charging the offender with an underlying predicate offence shall not preclude the pursuing of any legal proceedings against the latter for a money laundering offence, in case of variation in the elements of the offences.

**Article 3**
Whoever undertakes or attempts to undertake or incites or facilitates or intervenes or participates in:
1. Money-laundering operations, shall be punishable by imprisonment for a period of three to seven years, and by a fine not exceeding twice the amount laundered.
2. Terrorism financing operations or any related activities, shall incur the penalties stipulated in Article 316 bis and Articles 212 to 222 of the Penal Code.

**Article 4**
Banks, financial institutions, leasing companies, institutions that issue and promote credit or charge cards, institutions that perform money transfers electronically, exchange institutions, financial intermediation institutions, collective investments schemes, and any other institution requiring a license or supervised by Banque du Liban, must comply with the obligations specified below and with the regulations issued by Banque du Liban for the purpose of implementing the provisions of this Law:
1. To implement Customer Due Diligence measures on permanent customers (whether natural persons or legal persons or unique legal arrangements), in order to check their identity on the basis of reliable documents or information or data.
2. To implement Customer Due Diligence measures on transient customers to verify their identity, if the amount of a single operation or series of operations exceeds the threshold designated by Banque du Liban.

3. To determine the identity of the economic right owner and take the steps needed to verify this identity, on the basis of reliable documents or information or data.

4. To retain copies of related documents of all operations, and to retain information or data or copies of the customers’ identification documents, for at least five years after performing the operations or ending the business relationship, whichever longer.

5. To continuously monitor and review the business relationship.

6. To apply the measures specified in Paragraphs 1 to 5 above to permanent and transient customers, whenever there are doubts regarding the accuracy or adequacy of declared customer identification data, or whenever there is a suspicion of money laundering or terrorism financing, regardless of any thresholds or exemptions that limits the implementation of these measures.

7. To take into account the indicators that flag the likelihood of a money laundering or terrorism financing operation, as well as the due diligence principles to detect suspicious operations.

Article 5
Institutions not subjected to the Banking Secrecy Law of September 3, 1956, particularly insurance companies, casinos, real estate dealers and agents, and merchants of valuables (jewelry, precious stones, gold, works of art, antiques), must keep records of operations that exceed the threshold designated by the “Special Investigation Commission” (hereinafter referred to “the Commission”) that was established pursuant to Article 6 of this Law. Such institutions must also comply with the obligations specified in Article 4 above and with the regulations and recommendations issued by “the Commission” for the purpose of implementing the provisions of this Law. Certified accountants and notaries must implement these obligations, when preparing or carrying out on behalf of their customers any of the following activities:
- Buying and selling of real estate.
- Management of customers’ movable and immovable assets, in particular transactions consisting of money accumulation and joint investment.
- Management of bank accounts and securities accounts.
- Organization of contributions for the establishment or management of companies.
- Establishment or management of legal persons or unique legal arrangements, and buying and selling of single person enterprise or companies.

The same obligations shall apply to lawyers when they carry out any of the above-mentioned activities. The implementation rules of these obligations shall be specified pursuant to a mechanism to be set by the Beirut Bar Association and the Tripoli Bar Association, taking into account the particularities and rules of the Legal Profession.

Article 6
An independent, legal entity with judicial status shall be established at Banque du Liban, referred to as “the Special Investigation Commission” or “the Commission”, which shall discharge its functions without being subject to Banque du Liban’s authority.

1. The “Special Investigation Commission” shall consist of:
   - The Governor of Banque du Liban or, in case of impediment, one of the Vice-Governors he designates. Chairman
   - The judge appointed to the Higher Banking Commission or, in case of impediment, an alternate judge appointed by the Higher Judicial Council for a period equal to the term of the initially appointed judge. Member
   - The Chairman of the Banking Control Commission or, in case of impediment, a member of the latter designated by its Chairman. Member
   - A principal member and an alternate member appointed by the Council of Ministers upon proposal of the Governor of Banque du Liban, provided each of them has an experience of at least 15 years in financial or banking law. Member

2. The mission of the “Special Investigation Commission” is:
   - To receive suspicious transaction reports (STRs) and requests of assistance; to investigate operations that are suspected to be money-laundering or terrorism financing offences; to decide on the seriousness of evidence and circumstantial evidence related to the commission of any such offence(s); to take in this regard the adequate decision, particularly the precautionary and temporary freezing of the suspicious accounts and/or transactions, for a maximum period of one year renewable once for six months concerning foreign requests of assistance, and for a maximum period of six months renewable once for three months concerning local STRs and requests of assistance.
   - To ensure compliance by the parties referred to in Articles 4 and 5 above with the obligations stipulated in this Law and in the regulations issued in relation thereto, except for lawyers, certified accountants and notaries, without prejudice to the provisions of Paragraph 2 of Article 17 of this Law.
• To collect and retain the information received from the parties referred to in Articles 4 and 5 above, as well as the information received from Lebanese and foreign official authorities, and all other collected information, and to share such information with the Commission’s counterparts, in its capacity as the competent authority and the official center to undertake such a task.

• To issue regulations on the implementation of the provisions of this Law addressed to the parties referred to in Article 5 above, and to issue recommendations to all concerned parties.

3. After conducting the necessary audit and analysis, “the Commission” is the solely certified to decide:

• To permanently freeze the concerned accounts and/or transactions, and/or to lift the banking secrecy in favor of the competent judicial authorities and the Higher Banking Commission represented by its Chairman on accounts or transactions suspected to be related to money laundering or terrorism financing.

• To keep suspicious accounts as traceable accounts. “The Commission” may withdraw any of its decisions, in whole or in part, in case it obtains any new relevant information.

4. “The Commission” is entitled to:

a) Attach an encumbrance on the records and entries pertaining to movable or immovable assets, indicating that such assets are under investigation by “the Commission”. The encumbrance shall be kept until doubts are erased or until a final decision in this regard is taken,

b) Request the Public Prosecutor of the Court of Cassation to take preventive measures concerning the movable and immovable assets that have no records or entries, so as to prevent the use of such assets until a final judicial decision in this regard is taken, when there is a suspicion that these assets are related to money laundering or terrorism financing, and/or during the precautionary, temporary freezing of suspicious accounts and/or transactions, as specified in Paragraph 2 of this Article, and/or during the permanent freezing of these accounts and/or transactions, as specified in Paragraph 3 of this Article.

5. “The Commission” requires from concerned persons and parties, whether public or private, to take the necessary measures to prevent the use of movable or immovable assets belonging to any names designated or to be designated on the national lists issued by the competent Lebanese authorities or any other lists it circulates concerning terrorism and terrorism financing and any acts related thereto.

The concerned persons and parties, whether public or private, must comply without any delay to this requirement.

6. “The Commission” shall meet, upon its Chairman’s call, at least twice a month and when needed. The legal quorum requires the presence of three members at least.

7. “The Commission” shall take its decisions at a majority of the attending members. In case of a tie, the Chairman shall have a casting vote.

8. “The Commission” shall appoint a full-time Secretary General, who shall be responsible for the tasks assigned to him by “the Commission”, for implementing its decisions and for directly supervising its regular and contractual staff and the persons delegated by “the Commission” for a specific mission. The provisions of the Banking Secrecy Law of September 3, 1956 shall not be opposed to any of them.

9. The members of “the Commission”, its regular and contractual staff, as well as the persons delegated by “the Commission” for a specific mission, shall be bound by the obligation of confidentiality.

10. “The Commission” shall set its operating rules, as well as the internal rules governing its regular and contractual staff, who are subject to private law.

11. The expenses of “the Commission” and its ancillary bodies shall be borne by Banque du Liban as part of the budget prepared by “the Commission”, provided the budget is approved by the Central Council of Banque du Liban.

Article 7
The parties referred to in Articles 4 and 5 of this Law, including certified accountants and notaries, when preparing or carrying out on behalf of their customers any of the activities mentioned in Article 5 above must promptly report to the Chairman of “the Commission” the details of operations undertaken or attempted to be undertaken that are suspected to be related to money laundering or terrorism financing.

The same obligations shall apply to lawyers, according to a mechanism to be set by the Beirut Bar Association and the Tripoli Bar Association, taking into account the particularities and rules of the Legal Profession. The supervisors of the Banking Control Commission must, through the Chairman of the latter, report to the Chairman of “the Commission” any operations they suspect to be related to money laundering or terrorism financing and which they are aware of while performing their duties.

The auditors of the parties referred to in Article 4 above must promptly report to the Chairman of “the Commission” the details of the operations they suspect to be concealing money-laundering or terrorism financing and which they are aware of in the course of performing their work.
Article 8

1. “The Commission” shall convene after receiving information from the parties referred to in Article 7 above, or after receiving information from Lebanese or foreign official authorities.

2. After the assessment and analysis of the information relating to the case under examination, “the Commission” shall either decide to take notice, or conduct the required investigation, particularly by auditing the accounts or operations, or investigating the suspicious assets. “The Commission” shall conduct its investigations through a delegated person chosen amongst its members or its concerned officers, or through its Secretary General or an appointed auditor. All these persons shall perform their duties subject to confidentiality obligations, and without being opposed to the provisions of the Banking Secrecy Law of September 3, 1956.

3. Upon the completion of its audit and analysis, “the Commission” shall take its decisions in accordance with the provisions of Paragraphs 2, 3, and 4 of Article 6 of this Law.

4. If “the Commission” decides to lift the banking secrecy off the concerned accounts and/or to freeze them permanently and/or to request the maintain of the prohibition to dispose of the assets, it shall send a certified true copy of its decision to the Public Prosecutor of the Court of Cassation, the Higher Banking Commission through its Chairman, the concerned party, and the concerned local or foreign bodies, either directly or by the same means/body through which the information was received.

5. In case the Public Prosecutor of the Court of Cassation decides to drop the case of money laundering and discontinue the proceedings, the frozen accounts and all other assets shall be deemed free. The decision to drop the case shall be notified to “the Commission”, and the latter shall not be entitled to maintain the lifting of the banking secrecy, the freezing and the prohibition to dispose of the assets, and shall immediately notify the concerned banks and any other concerned parties thereof. However, if “the Commission” finds, before implementing the decision, any new evidence or circumstantial evidence that justifies the maintain of the freezing, or the prohibition to dispose of the assets, and of the lifting of the banking secrecy, then it must send a justified report, along with the documents containing such evidence or circumstantial evidence to the Public Prosecutor of the Court of Cassation who may decide, where applicable, to widen the investigation in light of the new information.

6. In case the Instruction Judge or the Chamber of Accusation issues a final decision dismissing any legal prosecution, as well as in the case of a final judgement or decision that ceases the legal proceedings or states the innocence of the holders of frozen accounts or assets not to be disposed of, these accounts and assets shall be deemed free, and a copy of the judgement or decision shall be notified to “the Commission” through the Public Prosecutor of the Court of Cassation. “The Commission” shall in turn notify the ruling or the decision to the concerned banks and other concerned parties. “The Commission” shall not be empowered to lift again the banking secrecy off the accounts or to reinstate the freezing decision and to prevent again the use of the accounts and assets, covered by the decision dismissing the legal prosecution, except through the mechanism stipulated in Article 127 of the Code of Criminal Procedures.

Article 9

The Chairman of “the Commission” or any person delegated by the Chairman may directly communicate with any Lebanese or foreign authority (judicial, administrative, financial, or security) in order to request information or take cognizance of the details of previously conducted investigations that are linked or related to ongoing investigations by “the Commission”. The concerned Lebanese authorities must promptly respond to this information request, and shall not be subject to any confidentiality obligation.

Article 10

The Chairman of “the Commission” or any person delegated by the Chairman may directly request from the parties referred to in Articles 4 and 5 above to provide “the Commission” with all the documents and information needed to perform its duties. Such parties must respond to this request within a reasonable period of time.

Article 11

Reporting entities, as well as their Board members, officers and employees, are prohibited from disclosing or insinuating to anyone that a suspicious transaction report or other relevant information is submitted or intended to be submitted to “the Commission”, or that “the Commission” is inquiring about customers or auditing their operations or accounts.

Article 12

Within the scope of their work, the Chairman, members, staff and delegates of “the Commission”, shall enjoy immunity. Thus, they may not be prosecuted or sued, neither collectively nor individually, for any civil or criminal liability related to the performance of their duties, including offences specified by the Banking Secrecy Law of September 3, 1956, except in case such secrecy is breached. The parties referred to in Articles 4 and 5 above and their staff, as well as the supervisors of the Banking Control Commission and auditors, shall also enjoy the same immunity in performing their duties under the provisions of this Law or according to the decisions of “the Commission”, particularly when they report in good faith to “the Commission” the details of operations they suspect to be related to money laundering or terrorism financing.
Article 13
Any party that violates the provisions of Articles 4, 5, 7, 10, and 11 of this Law shall be punishable by imprisonment for a period of two months to one year and by a fine not exceeding one hundred million Lebanese pounds, or by either penalties. “The Commission” may address a warning to the parties who are in violation of the provisions of the regulations issued for the purpose of implementing this Law, and may request from these parties periodic reports about the measures taken to rectify their situation. “The Commission” may as well, in case of violation, refer the parties mentioned in Article 4 to the Higher Banking Commission, and correspond with the supervisory or oversight authorities concerning the parties mentioned in Article 5. The Higher Banking Commission may impose on the parties that were referred to it a fine for non-compliance with the regulations issued for the purpose of implementing this Law, provided this fine does not exceed two hundred times the official minimum wage. Fines shall be collected to the benefit of Banque du Liban. The foregoing shall not preclude the enforcement of the administrative penalties stipulated in Article 208 of the Code of Money and Credit on the parties referred to in Article 4, nor shall it preclude the enforcement of the sanctions stipulated in all other laws and regulations on the parties referred to in Article 5.

Article 14
The movable or immovable assets that are proved, by a final Court ruling, to be related to, or derived from, a money-laundering or terrorism financing offence, shall be confiscated to the benefit of the State, unless the owners of the said assets prove in a Court of Law their legal rights thereupon. The confiscated assets may be shared with other countries, whenever the confiscation results directly from coordinated investigations or cooperation between the concerned Lebanese authorities and the concerned foreign body(ies).

Article 15
The reservations specified in Paragraphs 2, 3 and 4 of Article 1 of Law No. 426 of May 15, 1995, on authorizing the ratification of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, are repealed, as well as the provisions of Article 132 of Law No. 673 of March 16, 1998, on Narcotic Drugs and Psychotropic Substances.

Article 16
Upon the enactment of this Law, all provisions that are contrary to, or are in contradiction with the provisions of this Law, especially those specified in the Banking Secrecy Law of September 3, 1956, and those of Law No. 673 of March 16, 1998, on Narcotic Drugs and Psychotropic Substances, shall cease to be applicable.

Article 17 (Final Provisions)
The auditors of banks, financial institutions and other companies and institutions specified in Article 4 of this Law must verify the compliance by all these companies and institutions with the provisions of this Law and with the implementation regulations issued in relation thereto, and must also notify the Chairman of “the Commission” of any violation thereof.
The Ministry of Justice, the Beirut Bar Association, the Tripoli Bar Association, and the Certified Accountants Association, shall be responsible for verifying the compliance by notaries, lawyers, and certified accountants, as far as each is concerned, with the measures stipulated in this Law and in the implementation regulations issued in relation thereto.

Article 18
This Law shall enter into force upon its publication in the Official Gazette.

Beirut, November 24, 2015
Promulgated by the Council of Ministers
The President of the Council of Ministers
Signed: Tammam Salam

Law 32
Expanding the SIC Competence to Include Corruption

Unique Article
The Special Investigation Commission established pursuant to Law 318 of April 20, 2001 on Fighting Money Laundering, has the exclusive right to freeze and lift banking secrecy on bank accounts, in accordance with the anti-corruption agreements and laws in force, particularly the United Nations Convention against Corruption, provided the procedures specified in Law 318 are adopted. This law shall enter into force upon publication in the Official Gazette.

Baabda, October 16, 2008
Signed: Michel Sleiman
Promulgated by the President of the Republic
The President of the Council of Ministers
Signed: Fouad Siniora
Article 1
For the purpose of implementing the provisions of this Law, the following expressions shall mean:

1. **Currency / Negotiable Instruments:**
   - Banknotes and coins in circulation, whether in Lebanese pound or any other currency.
   - Commercial papers, securities, means of payment and other types of negotiable movable assets, in case they are not made out or endorsed to the benefit, or to the order of a designated payee (drawing bonds, promissory notes, checks, payment orders, bearer shares, prepaid cards, etc.).

2. **Declaration:** to provide detailed information on the owner of the Currency/Negotiable Instruments being transported, the person transporting them, the recipient party, their value, type, origin and intended use, the routes and modes of transportation.

3. **Disclosure:** to provide detailed information, at the request of the Customs authorities, on the owner of the Currency/Negotiable Instruments being transported, the person transporting them, the recipient party, their value, type, origin and intended use, the routes and modes of transportation.

4. **False declaration/false disclosure:** to provide false or incomplete information on the value of Currency / Negotiable Instruments transported across borders or other information which is asked for in the declaration / disclosure requested by the authorities; or failing to make a declaration / disclosure as imposed / required.

Article 2
All persons transporting physically, in or out of the border, Currency / Negotiable Instruments on them, in their accompanying luggage, or by any other means, by containerized cargo or any other means of shipping, or through the post, must submit a written declaration thereon to the Customs authorities, whenever the value of the Currency / Negotiable Instruments exceeds the amount of USD 15,000 or its equivalent in other currencies, by filling in a form that includes the complete relevant information requested.

As an exemption to the preceding paragraph, a disclosure thereof to the Customs authorities may be sufficient without the need for the declaration, when the Currency / Negotiable Instruments are being physically transported outside Lebanon and their value exceeds the amount of USD 15,000 or its equivalent in other currencies, according to the implementation rules mentioned in Article 6 below to be issued in relation to this Law.

Article 3
Customs authorities are empowered to search natural persons, inspect their luggage and the transportation modes referred to in Article 2 above, in order to check the accuracy of the information declared or disclosed.

In case a false declaration/disclosure is detected or suspected, or in case of non-declaration/non-disclosure, or in case of suspecting the transportation of illicit Currency/Negotiable Instruments, within the meaning of Article 1 of amended Law No. 318/2001, the Customs authorities are empowered to request additional information about the transported Currency/Negotiable Instruments, to seize them and prepare relevant seizure records, after notifying the Public Prosecution of the Court of Cassation. The latter shall, within a maximum period of two days, take the appropriate decision in light of the available data, as to whether maintain the seizure or free the said Currency/Negotiable Instruments, and accordingly notify its decision to the “Special Investigation Commission” established pursuant to amended Law No. 318 of April 20, 2001 on Fighting Money Laundering and Terrorism Financing.

Customs authorities shall promptly notify the “Special Investigation Commission” of the above-mentioned seizure records.

Article 4
Customs authorities shall establish an electronic database that has the necessary safety and confidentiality specifications. All the declarations, disclosures, records, files and official documents shall be archived in the database in a way that clearly distinguishes between the declarations and disclosures referred to in Article 2 of this Law and those mentioned in Article 3 thereof.

The Special Investigation Commission shall be empowered to directly access the declarations, disclosures, records, files and official documents mentioned in Article 3 of this Law.

Article 5
Customs authorities shall impose on any person making a false declaration/disclosure or failing to make a declaration/disclosure, a fine not exceeding ten million Lebanese pounds, not precluding any criminal prosecution as specified in the provisions of above-mentioned Law No. 318.

Article 6
The Customs Higher Council shall issue, within three months from the enactment date of this Law, and in collaboration with the “Special Investigation Commission”, a decision pursuant to which it shall set the implementation rules of the provisions of this Law, notably the preparation of the declaration form mentioned in Article 2 thereof.
Article 7
The detailed implementation of the provisions of this Law shall be set, where applicable, through Decrees taken by the Council of Ministers, upon a proposal made by the Minister of Finance on the basis of the preparation work done by the Customs Higher Council in collaboration with the “Special Investigation Commission” specified in Law No. 318/2001.

Article 8
This Law shall enter into force upon its publication in the Official Gazette.

Beirut, November 24, 2015
Promulgated by the Council of Ministers
The President of the Council of Ministers
Signed: Tammam Salam

Law 53
Authorizing the Lebanese Government to accede to the International Convention for the Suppression of the Financing of Terrorism signed in New York on December 9, 1999

Single Article
1. The Lebanese Government is authorized to accede to the International Convention for the Suppression of the Financing of Terrorism that was signed in New York on December 9, 1999 and came into force on April 10, 2002, however with certain reservations regarding the definition of terrorism as specified in Article 2, Paragraph 1, Sub-paragraph (b) of this Convention, and adopting the definition of terrorism as specified in Articles 1 and 2 of the Arab Convention for the Fighting of Terrorism, signed in Cairo on April 22, 1998, which the Lebanese Government was authorized to accede to pursuant to Law No. 57 of March 31, 1999.

2. This Law shall enter into force upon its publication in the Official Gazette.

Beirut, November 24, 2015
Promulgated by the Council of Ministers
The President of the Council of Ministers
Signed: Tammam Salam

Law 55
Exchange of Information for Tax Purposes

Unique Article
FIRST:
The purpose of this Law is to:

- Implement and execute the provisions of any duly signed and ratified convention relating to the exchange of information for tax purposes.
- Commit, under any such convention, the exchange of requested information.

SECOND:
1. Unless otherwise stated in this law, the following terms shall mean:
   a) Convention: any international treaty, convention or agreement stipulating the exchange of information for tax purposes, including the automatic exchange of information between Lebanon and any other foreign State;
   b) Automatic exchange of information: providing, periodically and without prior request, previously specified information, about residents of a foreign State that have concluded a Convention with Lebanon;
   c) Competent Authority: the Minister of Finance or a representative mandated by such Minister.
   d) The Competent Authority Agreement: any bilateral or multilateral convention concluded between the Competent Authority and any foreign State, with the purpose to clarify or explain the provisions of a specific Convention or to facilitate the automatic exchange of information under any Convention;
   e) Information: any data or record, in whatever form, that contains specific facts;
   f) Request: a request submitted to the Competent Authority in order to obtain information pursuant to a specific Convention;
   g) Requesting State: the State that submits a request to obtain information;
   h) Person: any individual, entity or other body established pursuant to the laws in force.

2. In case of divergence between the provisions of this Law or of any Convention with those of another law, the provisions of this Law and this Convention shall prevail.

THIRD:
In compliance with the provisions relating to the exchange of information under any Convention, the Competent Authority shall use the powers stipulated in Articles 23, 44, 48, and 103 of the Tax Procedures Code to collect Information, even where the tax administration does not need such information for internal tax purposes.
FOURTH:
1. The Competent Authority shall assist the Requesting State pursuant to the terms of the Convention. Where the Competent Authority finds, following the receipt of a Request, that the latter complies with the provisions of the Convention concluded with the concerned State, the Competent Authority shall then proceed with responding to the Request pursuant to the provisions of both the said Convention and this Law.
2. The Competent Authority may ask the Requesting State for additional information, where it deems this necessary in order to process the Request.
3. If the Competent Authority decides that the request is not in compliance with the provisions of the Convention concluded with the Requesting State, the Competent Authority shall then reject the Request and notify the Requesting State of such decision.

FIFTH:
1. Where the requested Information is not covered by the Law on Banking Secrecy of September 3, 1956 or by Article 151 of the Code of Money and Credit, such Information shall be directly provided by the Competent Authority to the foreign Requesting State.
2. Where the requested Information is covered by the Law on Banking Secrecy of September 3, 1956 or by Article 151 of the Code of Money and Credit, and where the Competent Authority finds that the Request complies with the provisions of the Convention concluded with the Requesting State, the Special Investigation Commission (SIC) established pursuant to Law No. 44 of November 24, 2015 on Fighting Money Laundering and Terrorism Financing shall request the Information and provide them directly to the Competent Authority.
3. The Information specified in Paragraph (2) shall not be provided to the Requesting State unless the person whose information is being requested is notified thereof. The latter shall have the right to object the decision of the Competent Authority before the State Council, within 15 days of such notification pursuant to the notification provisions stipulated in the Tax Procedures Code. The State Council shall issue, within maximum three months from the submission date of the aforesaid objection, a final and irrevocable decision regarding the merits of the legal conditions requiring the exchange of Information.

At the expiry of such deadline, or if the State Council decides to provide the requested Information, the Competent Authority shall forward the requested Information to the Requesting State.
4. Notwithstanding the foregoing, if the Requests are of urgent nature or if notifying the person whose Information is being requested may compromise the investigation carried out by the Requesting State, the requested Information shall be provided to the Requesting State without giving prior notification to such person, in accordance with standards and procedures agreed upon between the two States to preserve the rights of all parties.

SIXTH:
1. Banque du Liban and the SIC may ask financial institutions, during a specified time and according to a specific method in accordance with the provisions of this Law, to provide the requested Information in order for the Competent Authority to proceed with the automatic exchange of information, pursuant to any Convention or to the Competent Authority Agreement. The Information shall be forwarded to the Competent Authority to enable it to perform its functions under the Convention.
2. The Minister of Finance or Banque du Liban may, each based on its prerogatives and pursuant to decisions issued thereafter, determine:
   a) The institutions required to provide Information;
   b) The Information to be exchanged and the method of exchange, including by electronic means.
   c) The accuracy and comprehensiveness of the Information to be provided.
3. The Council of Ministers shall, where necessary, issue decrees to take the measures needed to implement the provisions of this Law where this is not specified in Paragraph (2) above.
4. In case of breach or non-compliance with the provisions of this Article, a fine ranging between one hundred million and two hundred million Lebanese pounds shall be imposed, without prejudice to the right of the concerned regulatory authority to impose administrative sanctions and financial penalties in accordance to its own laws.

SEVENTH:
This Law shall apply to all Double Taxation Avoidance agreements currently in force.

EIGHTH:
The Government is authorized to ratify the “Multilateral Convention on Mutual Assistance in Tax Matters-MAC, (which is attached hereto and may be amended from time to time), as well as the attached “Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information – MCAA). The Minister of Finance is mandated to sign the above Convention and Agreement.

NINTH:
1. The provisions of this Law shall come into force, notwithstanding any confidentiality obligation or other restrictions on the disclose of information imposed by any other law.
2. Any Information exchanged pursuant to Paragraphs Fourth and Sixth with the Competent Authority, under any convention or under this Law, shall be dealt with as being confidential, pursuant to the provisions of Article 25 of the Tax Procedures Code.

TENTH:
The provisions of Law No. 43 of November 24, 2015 (Exchange of Tax Information) shall be repealed.

ELEVENTH:
This Law shall come into force upon its publication in the Official Gazette and shall be expeditedly promulgated pursuant to Article 56 of Paragraph one of the Constitution.

Beirut, October 27, 2016
Promulgated by the Council of Ministers
The President of the Council of Ministers
Signed: Tammam Salam

Law 77
Amending Article 316 bis of the Lebanese Penal Code

Single Article
Article 316 bis of the Lebanese Penal Code relating to Terrorism Financing shall be amended to read as follows, based on the Arab Convention on the Suppression of Terrorism signed in Cairo on April 22, 1998 and ratified by Law No. 57 of March 31, 1999:

The new Article 316 bis
Whoever undertakes or attempts to undertake or directs or participates, intentionally and by any means, directly or indirectly, in financing totally or partially, or contributes to the financing of terrorism or terrorist acts, or the financing of an individual terrorist or terrorist organizations or any related acts, including offering or providing or collecting movable or immovable funds, from legitimate or illegitimate sources, in Lebanon or abroad, whether the funds were used or not used, and whether the terrorist act took place or not in Lebanon or abroad.

The terrorism financing offence includes the travel, attempt to travel, recruitment, planning, preparation, organizing, facilitation, participation, providing or receiving training, and any other related act with the intention of committing terrorist acts, without being linked to a specific terrorist act.

The perpetrators of the abovementioned acts shall be punished by temporary hard labor for a period of at least 3 years but not exceeding 7 years, and by a fine equaling at least the value of the paid amount but not exceeding its triple. This does not preclude the implementation of the penalties stipulated in articles 212 to 222 inclusively of the Penal Code.

This Law shall enter into force upon its publication in the Official Gazette.

Beirut, October 27, 2016
Promulgated by the Council of Ministers
The President of the Council of Ministers
Signed: Tammam Salam

Law 214
Law on the Recovery of Assets Derived from Corruption Offences

Chapter I: Scope of the Law and Definitions

Article 1
This Law shall govern all operations related to the recovery of any type of assets derived from corruption offences, whether located inside or outside the Lebanese territory, and whether they remain in the ownership or possession of the offender or are transferred into the ownership or possession of a third party.

Article 2
The provisions of this Law shall apply in accordance with the United Nations Convention against Corruption (UNCAC) adopted by United Nations General Assembly Resolution No. 58/4 that Lebanon joined by virtue of Law No. 33/2008, particularly Article 51 of that Convention, in line with Law No. 64/2015 on Fighting Money Laundering and Terrorist Financing, Law No. 175/2020 on Combating Corruption in the Public Sector and Establishing the National Anti-Corruption Commission, and Law No. 189/2020 amending Law No. 154/1999 on Illicit Enrichment.

Article 3
For the purposes of this Law, the following terms and expressions shall have the meanings set out below:

1. Offences: Corruption offences specified in Law No. 175/2020 on Combating Corruption in the Public Sector and Establishing the National Anti-Corruption Commission, as well as the laundering of funds, including those derived from corruption offences and the offences specified in Law No. 318/2001 on Fighting Money Laundering and Terrorist Financing and its amendments, particularly Law No. 44/2015. Money laundering encompasses the acquisition, possession or use of assets, knowing, at the time of receipt, that they are the proceeds of crime.

2. Funds: Assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable,
3. **Recovery**: The overall process of tracing, freezing, seizing, confiscating, and recovering assets and their substitutes, which would enable the State to identify and recover assets, whether located in Lebanon or abroad, and whether deriving directly or indirectly from offences, in addition to the rights associated to these assets and the income and profits derived or generated therefrom, as the case may be.

4. **Asset Tracing**: To examine information and documents; to retrieve, organize and analyze data evidencing the movement of assets derived from criminal offences, including to resort to international cooperation, where applicable, in order to determine the nature and type of these assets, assess their value, follow their trail and the method of their ownership transfer between concerned legal and/or natural persons, as the case may be, whether inside and/or outside Lebanon, from the moment they generate from any such crimes through to their last location.

5. **Repatriation**: The last step in the recovery process of criminally derived assets located outside the jurisdiction of the Lebanese State; which means that the foreign country to which the assets were smuggled will return them to Lebanon, either by court order, or under a bilateral or multilateral agreement, or any other legally available means.

**Chapter II: Asset Recovery Division**

**Article 4**

A “Division for the Recovery of Assets Derived from Corruption Offences” (hereunder “the Division”) shall be established at the National Anti-Corruption Commission mentioned in Law No. 175/2020, and shall undertake the tasks below:

1. To coordinate with all judicial, supervisory and security authorities, and with the Special Investigation Commission mentioned in Law No. 44/2015, with regard to prosecutions, reports, and allegations related to corruption offences, in terms of recovering corruption-derived assets, in all matters that do not conflict with the competencies granted to the above-mentioned authorities by applicable laws.

2. To develop strategies and plans regarding the overall asset recovery process at all administrative and judicial stages, and any other related issue submitted to that Division in particular.

3. To follow up the asset recovery process with the relevant administrative and judicial authorities, to the extent permitted by their laws and regulations, with the Division’s right to obtain information on the files concerning the recovery of corruption-derived assets, and to provide the requested information, a task to be carried out by the Division until the management of these assets by the Fund established pursuant to this Law.

4. To propose negotiation strategies and mechanisms, in particular to the Committee of Cases at the Ministry of Justice and to the National Anti-Corruption Commission, with respect to settlements, reconciliations, and agreements that would expedite and activate asset recovery efforts, with no need to initiate legal proceedings; and to propose therefore the relevant procedures.

5. To identify the obstacles facing the recovery of assets and to recommend to the concerned authorities the necessary legislative and regulatory texts as well as the remedial legal and administrative measures.

6. To seek the assistance, where applicable, of any person deemed appropriate, whether natural or legal, Lebanese or foreigner, having the necessary qualifications and experience, based on documented Curriculum Vitae.

**Article 5**

The Division is formed of:

- The Chairman of the National Anti-Corruption Commission as Head of the Division, and
- Two members of that Commission to be selected under the rules of procedure referred to in Law No. 175/2020.

**Article 6**

The Division may invite to its meetings, representatives of the Court of Accounts, the Central Inspection, and the security entities, and any representative of other concerned parties whose attendance is deemed useful.

**Article 7**

The deliberations of the Division are confidential; each member of the Division and of the Division’s Secretariat, as well as any person whose assistance and/or attendance to meetings is requested, shall be bound by professional secrecy with respect to the information and documents that come to their notice when discharging their duties in accordance with this Law.

Any person that violates the provisions of this Article shall be liable to imprisonment for a period of two months to two years, and to a fine varying between ten to twentyfold the minimum wage, without prejudice to the implementation of disciplinary sanctions and procedures provided for by applicable laws.

**Article 8**

The Division may request from the Administration, as per the definition specified in Law No. 28/2017 on the Right to Access Information, the needed information and documents held by the latter. The Administration shall provide such information...
and documents within a time limit of 15 days from the date of
the request, to be extended only once, for another 15 days at
most, if need be. Professional secrecy shall not be opposed
to the Division and the persons entrusted with that secrecy
shall not be held liable for satisfying the Division’s requests.

Article 9
The Division shall hold a public meeting, no later than every
two months, with the plaintiffs, corruption whistleblowers,
and representatives of anti-crime organizations, in order to
provide them, to the largest extent, with information on the
files the Division is working on, and to consult with them on
ways to enhance their cooperation for the implementation of
this Law, except for unwilling whistleblowers.

Article 10
The Division shall prepare yearly in the month of January,
a detailed annual report on its activities, pursuant to the
provisions of Law No. 28/2017 on the Right to Access
Information. This report shall be published on the website of
the National Anti-Corruption Commission.

Chapter III: The National Fund

Article 11
By virtue of this Law, a “National Fund for the management
and investment of assets in recovery or recovered” (hereunder
The National Fund) shall be established, as a legal entity
with financial and administrative independence, and shall be
connected to the National Anti-Corruption Commission with
respect to the Fund’s budget allocated to the management
of criminally derived assets.

Article 12
Asset management, depending on the asset recovery stage,
includes the right to invest assets in recovery, i.e. at the stage
of freezing or seizure, or to dispose of assets derived from the
criminal offences specified in this Law and all other criminal
offences, and the related proceeds, recovered through a
final Court order, by way of regulations and a mechanism
specifically developed for this purpose, until these assets are
disbursed:
• First: to contribute in covering the Fund’s expenses and
  those of the Division and the National Anti-Corruption
  Commission, and to reward, pay compensation, and
  protect whistleblowers; and
• Second: to offer the remainder of the assets, in the form of
donations, to State projects aimed at combating poverty
and achieving sustainable development.

Article 13
The National Fund shall have all the powers to enter into
contracts and take all kinds of necessary measures with
any party, whether in the public or private sector, inside or
outside Lebanon, in order for the Fund to efficiently carry
out the functions entrusted to it by this Law. The National
Fund may receive donations or aid from internal or external
parties, provided the donors’ identity is published and
disclosed, while avoiding any conflict of interest or impact
on its functioning.

Article 14
With regard to corporate equities or shares in recovery or
recovered, the National Fund shall exercise the powers of
holding companies pursuant to the provisions of Legislative
Decree No. 45/1983 and its amendments.

Article 15
All operations undertaken by the National Fund in relation
to the management, investment and transfer of ownership
of assets in recovery and recovered, as well as the rights
associated with these assets and all income and profits
derived or generated therefrom, shall be exempted from all
fees and taxes due.

Article 16
The National Fund shall submit its annual report to
Parliament, and its activities shall subsequently be subject to
the control of the Court of Accounts. The Minister of Finance
shall commission, based on the advice of the National Anti-
Corruption Commission, and as per the provisions of Article
73 of Law No. 326/2001, an internationally recognized
independent external auditor to control the National Fund’s
accounts.

Article 17
The National Fund and its governance, including the
conditions for Board membership, the designation and
appointment of Board members, their remunerations,
management, financial rules, scope of investments,
prohibitions, accountability and transparency, shall be
regulated in accordance with the Santiago Principles
governing sovereign wealth funds, by virtue of a decree
based on a decision taken by the Council of Ministers,
upon the proposal of the Ministers of Finance and Justice,
and following the advice of the National Anti-Corruption
Commission upon its establishment, within a period of six
months at most from the date of publication of this Law.

Chapter IV: International Mutual Legal Assistance

Article 18
The Ministry of Justice shall establish detailed regulations
and procedures allowing to send, receive, and execute
international mutual legal assistance requests as promptly
as possible, within the widest possible scope, after
prioritizing mutual legal assistance requests, and taking into
account the principle of reciprocity and dual criminality in
all matters relating to investigations into corruption offences
and criminal offences specified in Law No. 318/2001 on
Fighting Money Laundering and Terrorist Financing and its amendments, particularly Law No. 44/2015, in consistency with international agreements concluded by Lebanon.

Chapter V: Final Provisions

Article 19
The detailed implementation of this Law shall be determined, where applicable, through decrees issued by the Council of Ministers upon the proposal of the Ministers of Finance and Justice, following the advice of the National Anti-Corruption Commission upon its establishment.

Article 20
This Law shall enter into force upon its publication in the Official Gazette.

Baabda, April 8, 2021
Signed: Michel Aoun
Promulgated by the President of the Republic
The President of the Council of Ministers
Signed: Hassan Diab

SECTION II - RELATIONS WITH CUSTOMERS AND DUE DILIGENCE MEASURES

Article 3
The following expressions shall mean:

- Customer: any natural or legal person, whether a company or a partnership of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (mutual funds, cooperatives, welfare centers, charities, clubs, etc.).

- Beneficial Owner: any natural person who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the Customer and/or the natural person on whose behalf a transaction is carried out.

Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

2. As far as each is concerned, banks must refrain from keeping anonymous accounts or accounts in fictitious names, must adopt clear measures for account opening, must apply due diligence measures which include verifying the identity of their permanent and occasional customers, whether resident or non-resident, determining the nature of their business, their tax residency, and obtaining the relevant tax written self-certification form, understanding the ownership structure and/or control over the legal person, understanding and identifying the purpose and nature of the business relationship and/or the account
opening, obtaining data on that purpose when needed, identifying the beneficial owner and the source of funds, and conducting ongoing monitoring of operations, particularly in the following cases:

- Prior to, or when dealing with a customer or opening any kind of account, including fiduciary accounts and numbered accounts.
- Lending operations.
- The conclusion of contracts for leasing bank safes.
- Electronic funds transfers.
- Cashier’s operations totaling or exceeding USD 10,000 or its equivalent in any other currency.

Cashier’s operations include cash payments made by the customer at the bank’s counters (deposit of funds, exchange of currencies, purchase of precious metals, purchase of financial instruments in cash, cash subscription to vouchers at the counter, purchase of checks in cash, including traveler’s checks, etc.).

2 bis. Upon the identification of the Beneficial Owner, the same Due Diligence measures applicable to Customers shall apply, including those issued by the Special Investigation Commission.

3. The employee in charge of executing the operation must conduct due diligence measures, which include verifying the customer’s identity, regardless of the amount involved, if he/she notices a single operation or several linked operations that are being carried out for amounts below the designated threshold in Paragraph (2) of this Article but whose aggregate value totals or exceeds USD 10,000 or its equivalent, or if he/she suspects a customer to attempt a money laundering or terrorist financing operation.

4. In order to verify the identity of the customer and the beneficial owner, the employee in charge of executing the operation must request from the customer or the person acting on behalf of the latter, the following official documents or data:

a) In case the customer is a natural person: a passport, an identity card, an extract from the Civil Status Register, or a residence permit.

b) For a legal person, whether a company or an institution or a legal arrangement, duly certified copies of the bylaws, the registration certificate, the ownership structure, the list showing the distribution of equities or shares (directly or indirectly) and the nature of associated voting rights, the list of authorized signatories, in addition to a copy of the identity of the legal representative, the managers, and the natural persons who own, directly or indirectly, a controlling interest in the company’s management, and also the statement submitted by the beneficial owner to the Ministry of Finance and to the Commercial Register.

c) In case the operation is carried out through a proxy or a person acting on behalf of the customer: the original power of attorney or a certified copy thereof, or any document proving that this person is authorized to act as such, in addition to the identity documents of the customer and the proxy or the person acting on the customer’s behalf, and these documents must be verified. The due diligence measures specified in Paragraph (2) of Article 3 above must also be applied to the non-professional proxy.

d) In case the operation is carried out by correspondence: an official authentication of the customer’s signature on the same document or on a separate certificate. If the customer resides abroad, his/her signature authentication or identity verification may take place through a correspondent bank or affiliated bank, or through a branch or representative office of the concerned bank, or through another bank whose authorized signatures can be verified, provided that bank is subject to a sound 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 sound control and implements sufficient and effective AML/CFT procedures. The bank shall be liable for the accuracy of statements or information when it relies on a third party to identify customers and verify their identity.

5. The bank must maintain all the records obtained through CDD measures toward the customer and the beneficial owner, in particular the full name, occupation, and residential address, the address of the registered office for the legal entity, or, if different, the principal place of business, and the financial situation, as well as the account files for at least five years after the account is closed or the business relationship is ended, and all the records of operations, including business correspondence and the results of any analysis undertaken, for at least five years after the date of the operation. Such records must be sufficient to permit reconstruction of individual operations, so as to provide, if necessary, evidence for legal action and prosecution of criminal activity.

6. When the due diligence measures specified in Paragraph (2) of Article 3 above cannot be satisfactorily applied to customers and beneficial owners, then no account should be opened or relationship started or operation performed, or the existing business relationship should be terminated; and notifying the SIC that was established pursuant to Law 318 of 20 April 2001 (replaced by AML/CFT Law 44 of 24 November 2015) should be considered.

7. When opening numbered deposit accounts for their customers, in accordance with Article 3 of the Banking Secrecy Law of 3 September 1956, banks must exclusively utilize numbers and/or letters to identify these accounts, and refrain from utilizing pseudonyms; they must also conduct all relevant due diligence measures.
Article 4
In case the bank suspects that the customer is not the beneficial owner or if the customer states that the beneficial owner is a third party, the bank must request from the customer a written statement that identifies the beneficial owner, particularly the latter’s full name, residential address, occupation and financial status. The bank must keep a copy of this statement and of the beneficial owner’s identity throughout the period indicated in Paragraph 5 of Article 3 above.

Doubts about the beneficial owner’s identity arise in instances that include, but are not limited to, the following:

a) When a power of attorney is given to a non-professional person (e.g. other than a lawyer or a fully authorized representative or a financial intermediary) and no relationship between the customer and the proxy justifies that power of attorney.

b) When the business relationship is conducted through numbered accounts or through front institutions/companies.

c) When the customer’s financial status is known to the employee executing the operation and the amount of the intended operation is inconsistent with the said financial status.

d) When any other indicator draws the attention of the bank during the course of its business.

Article 5
The bank must promptly notify the Governor of Banque du Liban in his capacity as Chairman of the Special Investigation Commission, whenever it suspects or believes, based on reasonable or objective grounds, that the executed or attempted banking operation is related to money laundering or associated predicate offences, or to terrorist financing, terrorist acts, or terrorist organizations, regardless of the amount involved, particularly when:

- It has irrefutable suspicions about the veracity of the customer’s written statement regarding the beneficial owner’s identity, or that false or inaccurate information was given about that identity.
- It realizes that it was misled in the course of verifying the customer or beneficial owner’s identity, and has persistent suspicions about the information provided by the customer.
- Transfers or checks are returned, directly or upon the request of concerned parties, particularly correspondent banks, due to forgery or to suspicions that they involve suspicious operations.
- It has reasonable grounds to believe that conducting due diligence measures will alert the customer to the bank’s suspicions about the existence of a money laundering or terrorism financing operation. In this case, the bank is allowed not to pursue this process.

Article 5 bis
Banks must promptly notify the Special Investigation Commission of any procedures and measures they might take in accordance with applicable AML/CFT laws and regulations, in order to freeze or close any account held by a customer, or to refrain from dealing with that customer or from opening an account in the latter’s name. Banks are also required to justify any such procedures and measures.

Article 6
Banks must conduct due diligence measures towards all existing customers, including the owners of accounts opened before the issuance of Law 318 of 20 April 2001, on the basis of materiality and risk, and must also conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken, whether there are any changes in the customer’s situation, especially if there are doubts about the veracity or adequacy of previously obtained data, or in case there are subsequent changes in the identity of the customer or beneficial owner. Therefore, each bank is required to prepare action plans with precise dates to fulfill these obligations.

SECTION III - CONTROLLING CERTAIN OPERATIONS AND CUSTOMERS

Article 7
1. The bank must conduct enhanced due diligence measures, including to enquire from the customer about the source and destination of funds, the object of the operation, and the identities of both the beneficiary and the beneficial owner, when the operation is characterized by the following:

a) The operation is carried out in exceptionally complicated circumstances. In this respect, the bank must assess the said circumstances, not only in relation to the nature and type of the operation, but also in relation to its apparent purpose.

b) The operation seems to have no economic rationale or legitimate purpose, especially when there is a discrepancy between the operation and the customer's occupation, or even between the operation and the customer's habits and personality.

c) When one of the operation’s counterparties is a national or a resident of countries that do not apply or insufficiently apply the FATF Recommendations. This shall be verified through a periodic review of the FATF website, particularly after every FATF plenary meeting.

2. The bank is required:
FIRST: when accepting a cheque drawn on it by an exchange institution, or when executing a banking operation
requested by an exchange institution on behalf of one of its customers, whether directly or indirectly, and if the value of the cheque or the operation is above USD 10,000 or its equivalent, to take the following measures:

   a) Ensure that it receives the notification specified in Paragraph 1, Article 9 of the Implementation Rules of the Law Regulating the Money Exchange Profession, attached to Basic Decision No. 7933 of 27 September 2001, which includes information about the cheque-related operation or the banking operation, particularly whether or not the cheque-related operation or the banking operation was executed against an amount received in cash by the exchange institution, in addition to information about the source and destination of funds, and the identity of both the beneficiary and the beneficial owner.

   b) Keep this notification for a five-year period.

   c) Request and obtain this notification directly from the concerned exchange institution, in case it has not yet received it when the check is submitted or when the banking operation is requested.

SECOND:
when requested to execute a transfer resulting from an exchange operation or a cross-border transportation of cash and/or precious metals to a third person in Lebanon, regardless of the transferred amount:

   a) Ensure that it receives the notification specified in Paragraph 2, Article 9 of the Implementation Rules of the Law Regulating the Money Exchange Profession.

   b) Keep this notification for a five-year period.

3. The bank must promptly inform Banque du Liban when an exchange institution fails to send any of the notifications specified in Paragraph (2) above.

4. The bank is prohibited from:
   • Opening any account for any exchange institution, before obtaining the approval of the Compliance Unit specified in Article 10 below.
   • Opening accounts for exchange institutions or executing transfers upon the latter’s request for purposes other than those specified in the Implementation Rules of the Law Regulating the Money Exchange Profession issued by Banque du Liban.
   • Accepting or executing an exchange operation in favour of any exchange institution, unless the latter is one of the customers of the concerned bank.

5. When issuing a chequebook in favour of an exchange institution, the bank must insert in all the cheques the expression “payable to the first beneficiary only”.

Article 8
Banks must, as far as each is concerned:

   a) Consider the following indicators in particular, and for indicative purposes only, as evidence of operations involving money laundering or terrorism financing:

1. The exchange of big quantities of small-denomination bills for large-denomination bills of the same currency or of any other currency.

2. Large or recurrent foreign exchange operations (cambio), by using cash funds.

3. Certain movements in the customer’s account, such as large or recurrent deposits unjustified by the customer’s apparent activities.

4. An account operated for the main purpose of transferring abroad, or receiving from abroad, sizeable amounts of money, while such operations are unjustified by the customer’s activities.

5. Large or recurrent operations related to a customer’s offshore activities, and which appear to be inconsistent with the volume of the customer’s activities.

6. The replacement of large cash amounts by electronic transfer requests or by bank cheques.

7. A change in the pattern of deposit operations made by a customer exempted from filling the cash transaction slip (CTS).

8. Large cash operations performed by a customer in the form of deposits and withdrawals, with insufficient personal identification.

9. The fact of cashing or receiving cheques to the bearer issued abroad, or drawn to the order of a person but previously endorsed by persons other than the depositor, or cheques of different amounts that might be unrelated to commercial operations or are alleged to be resulting from gambling.

10. Cash deposits and/or bank transfers followed by direct and numerous withdrawals.

11. The existence of several accounts that are held by a single customer and are unjustified by the nature of the latter’s activities, or the undertaking of numerous cash transfers between and through these accounts.

12. The occurrence of cash deposits and/or bank transfers, while the customer’s activities do not generate such a volume of funds.

13. The fact of depositing bank/traveler’s cheques in the account of a company/institution whose activities do not justify such deposits.

14. Cash operations and/or bank transfers which appear unusual, considering the location of the branch.

15. E-banking operations which appear unusual.

16. Transfers between the accounts of an exchange institution and other accounts, in particular those held by any of the institution’s owners, partners, shareholders, directors or authorized signatories or any of the family members of these persons (spouse, ascendants, descendants), especially if these transfers are followed by withdrawals.
17. A cash deposit resulting from the sale of a real estate, followed by the withdrawal of the deposited amount or its transfer to the buyer or to any person designated by the buyer, under the pretext of cancelling the sale transaction.

b) To monitor, through the units and sections mentioned in Article 11 of these Regulations, the accounts opened and operations carried out, by utilizing specialized software programs for the control of accounts and operations that correspond to any of the above-mentioned indicators, based on customer profiling, and also to retrieve (daily, weekly, monthly, annual) reports on such accounts and operations.

c) Take sufficient measures to prevent the misuse of technological developments for money laundering or terrorism financing purposes.

Article 9
Banks must take appropriate steps to identify, assess and understand their ML/FT risks, and must apply, based on risk understanding, the measures below:

FIRST:
Adopt a risk-based approach to classify customers and operations according to the following risk levels: low risk, medium risk and high risk. The following risks shall be taken into account, for indicative purposes only:

1. Customer risk:
   a) Customers whose occupation relies mainly on cash (money exchange, gold and precious stones dealers, restaurants and night-clubs, real estate companies, car dealers, specialized lending entities known as “Comptoirs” (governed by the provisions of Articles 183 and 184 of the Code of Money and Credit), non-banking institutions performing electronic transfers of cash...).
   b) Politically Exposed Persons (PEPs) according to the FATF definition.
   c) Offshore companies.
   d) Companies established in countries known to be tax havens.
   e) The non face-to-face customers of the bank.
   f) Customers dealing only through intermediaries.
   g) Customers dealing through fiduciary contracts or trusts.
   h) Companies whose capital is totally or partly constituted of bearer shares.
   i) Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
   j) Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.

2. Country risk:
   a) The strictness of AML/CFT laws, and the efficiency of the regulatory and judiciary authorities in charge of their implementation.
   b) The existence of banking secrecy.
   c) The situation of the country in terms of corruption and organized crime.

3. Service risk:
   a) Private Banking.
   b) Payable-through accounts, which are accounts opened by banks or financial institutions at other banks and put at their customers’ disposal to be used directly or through subaccounts.
   c) Electronic Banking.

SECOND:
To put in place risk-based control measures and procedures, and at least to adopt for customers and beneficial owners, for PEPs1 as per FATF definition and their family members and close associates, and for operations classified as “high risk” according to risk scoring, the enhanced measures and procedures below for the purpose of risk management and mitigation:

1. To increase and prioritize control, and to conduct enhanced ongoing monitoring of the business relationship.
2. To obtain more detailed information on customers and beneficial owners (Increased KYC Levels), in particular to determine the source of their wealth.
3. To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers, and for executing operations, in a way that is commensurate to the specified level of risk.
4. To review periodically the relationship with customers.
5. To make continuous peer comparisons.
6. To set up an adequate system so as to determine whether the customer or beneficial owner is a PEP.

1) Politically Exposed Persons (PEPs) are foreign or domestic individuals who are or have been entrusted with prominent public functions by a foreign country or domestically, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, as well as members of senior management, i.e. directors, deputy directors and members of the Board or equivalent functions in any international organization. This definition of PEPs is not intended to cover middle ranking or more junior individuals in the aforementioned categories.
THIRD:
Take into consideration the duration and the soundness of the business relationship with the customer.

FOURTH:
Use specialized software for performing controls in line with the adopted scoring.

FIFTH:
To have the Senior Management adopt a special policy as well as controls and measures that are based on the requirements specified in this Article, in order to classify and mitigate risks.

SIXTH:
To document and keep the risk assessment findings, to update the assessment when necessary, and to provide it to the supervisory authorities when needed.

Article 9 bis

FIRST:
With respect to the Customer that is a legal person, the Beneficial Owners shall be identified and reasonable measures taken to identify them in the following manner:

1. Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.

2. In case of doubt as to whether the natural person(s) identified pursuant to Subparagraph 1 above is (are) the Beneficial Owner(s), or when no natural person holds 20% or more of the Customer’s capital, the natural person who exercises control over the legal person through other means (e.g. holding a majority of voting rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities…).

3. When no natural person is identified pursuant to Subparagraphs (1) and (2) above, reasonable measures shall be taken in order to identify and verify the identity of the persons holding senior management positions.

SECOND:
With respect to Customers that are legal arrangements, the Beneficial Owners shall be identified and reasonable measures taken to identify them, in the following manner:

1. With regard to trusts, each of the persons below shall be identified:
   • The Settlor
   • The Trustee
   • The Protector
   • The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.

   • Any other natural person exercising an effective control over the trust through direct or indirect ownership or through other means.

   The definitions stated in the glossary attached to the FATF 40 Recommendations shall be adopted to identify the persons mentioned in this Subparagraph 1.

2. With respect to other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Paragraph Second, Subparagraph 1, shall be identified.

SECTION IV - COMMITTEES AND ADMINISTRATIVE UNITS IN CHARGE OF THE CONTROL OF OPERATIONS FOR FIGHTING MONEY LAUNDERING AND TERRORIST FINANCING, AND THEIR TASKS

Article 10

Each bank operating in Lebanon is required to:

1. Establish an AML/CFT Board Committee composed of three Board members at least, according to the following conditions:
   • To appoint a Chairman to this Board Committee chosen among its members, provided he/she is independent and has the necessary expertise.
   • To determine the remunerations of the Chairman and members of this Board Committee.

   Except for the Chairman, any member of the AML/CFT Board Committee may, simultaneously, serve as member of the Audit Committee or the Risk Committee or the Remuneration Committee (Cross membership).

   The Chairman of the AML/CFT Board Committee may not delegate his/her powers to any other person.

2. Establish, within the central management of the bank, an AML/CFT Compliance Unit (hereafter the Compliance Unit). The Head of this Unit must have sufficient experience in fighting money laundering and hold specialized certificates such as the CAMS-Certified Anti-Money Laundering Specialist or any other certificate; the staff must be appropriately skilled; and the Unit provided with the adequate resources to perform its mission.

3. Appoint, in each of its branches, an AML/CFT Branch Officer in charge of controlling the operations, who is not the director of the branch. This Officer must hold a high position, have professional and academic expertise, and be entrusted with independent functions, without performing any marketing activity and receiving any kind of incentives against this activity (bonuses, remunerations, grants…).

   The AML/CFT Branch Officer’s performance shall be directly evaluated by the Head of the Compliance Unit.
who will communicate the results of the evaluation to the Human Resources Department and to the AML/CFT Board Committee.

4. Establish, within the Compliance Unit, two Divisions at least. The first Division shall oversee the Head Office and the branches in Beirut, while the second Division shall oversee all other branches in Lebanon. Each Division shall ascertain that operations control standards are implemented by the Head Office and the relevant branches, to ensure their compliance with AML/CFT regulations.

In case a bank is unable to establish the above-mentioned Divisions, it may submit to the Governor of Banque du Liban, by 31 March 2015, alternative proposals based on justified grounds to be considered by the Central Council for proper decision.

**Article 11**

The committees and administrative units established at banks are respectively required, as all other concerned officers at the bank, to comply with the procedures aiming at controlling, fighting and preventing money laundering and terrorism financing operations. These procedures shall include, for indicative purposes only, what follows:

1. Regarding the AML/CFT Board Committee mentioned in Paragraph 1 of Article 10 above:
   a) To support the Board of Directors in its functions and supervisory role with respect to fighting money laundering and terrorism financing and understanding the related risks, and to assist it in taking the proper decisions in this regard.
   b) To review, from a risk-based approach, 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, exemptions from filling Cash Transaction Slips (CTS) and the link between these operations and economic activities, and to also take the relevant decisions.

2. Regarding the Compliance Unit:
   a) To put in place and adopt guidelines for the implementation of the provisions of both the AML/CFT Law and these Regulations, and to submit these guidelines to the Committee mentioned in Paragraph 1 of Article 10 above.
   b) To prepare a customer identification form (KYC: Know Your Customer) that includes basic information to be provided about customers, in particular the information specified in Article 3 of these Regulations for indicative purposes only, and to submit this form to the Board Committee mentioned in Paragraph 1 of Article 10 above.
   c) To verify the proper implementation and effectiveness of AML/CFT procedures and regulations.
   d) To review periodically these procedures and regulations and to develop them in line with the latest adopted methods.
   e) To prepare a staff training program on controlling financial and banking operations in order to fight money laundering and terrorism financing.
   f) To monitor, when theoperation totals or exceeds USD 10,000 or its equivalent, the adequacy of exemption procedures whereby some well-known customers are exempted from filling the cash transaction slip (CTS), and also to determine the exemption ceiling and to modify it according to developments in the customer’s economic situation.
   g) To ascertain that concerned employees are complying with the procedure guide on the implementation of AML/CFT legal and regulatory texts, and that the KYC Forms are filled, and to prepare reports to this effect.
   h) To review periodically the effectiveness of AML/CFT procedures and regulations, to improve them and submit any proposed amendments thereto to the Board Committee referred to in Paragraph 1 of Article 10 above, for proper decision.
   i) To review the daily/weekly reports received from the concerned departments and branches about cash operations and transfers.
   j) To monitor all the customer’s accounts and operations on a consolidated basis, in and off balance sheet, at the Head Office and at all branches in Lebanon and abroad, so as to ensure their consistency with the information provided in the KYC Form and with any other information held by the bank.
   k) To investigate unusual operations, in particular those mentioned in Paragraph 1 of Article 7 and Paragraph (a) of Article 8, provided the reasons behind these operations and their purpose are verified, and the findings are documented, retained for a five-year period and submitted to the SIC upon request; and also to prepare a periodical (at least, monthly) report to this effect and submit it to the Board Committee mentioned in Paragraph 1 of Article 10 above.
   l) To approve the opening of accounts for exchange institutions.
   m) To control the accounts of the exchange institution on a consolidated basis.
   n) To prepare the agenda of the AML/CFT Board Committee.
   o) To notify directly the Chairman of the Board/Director General whenever the Compliance Unit is in possession of evidence or doubts that the banking operation involves money laundering or terrorism financing.
3. Regarding Internal Audit:
   a) To audit cash operations, transfers, and account movements.
   b) To ascertain that the branches and specialized sections are complying with the procedure guide on the implementation of AML/CFT legal and regulatory texts, and that the KYC Forms are properly filled.
   c) To report discrepancies to the appointed external auditor, through a periodical report.
   d) To inform the Compliance Unit through reports concerning the stipulations of Paragraphs a, b and c above, and any risky or unusual operations.

4. Regarding the AML/CFT Branch Officer:
   a) To ascertain that the employees of the branch are complying with the procedure guide on the implementation of AML/CFT applicable laws and regulations, and that the KYC Form is properly filled.
   b) To 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).
   c) To report to the Compliance Unit, through the AML/CFT Branch Officer, any suspicious cash deposit that may involve money laundering or terrorism financing operations, if the relevant supporting documents cannot be obtained.

5. Regarding the Head of the Transfers Section:
   a) To verify transfers received by customers’ accounts, particularly electronic transfers that do not include the name of the originator (ordering customer) or of the beneficiary (beneficiary customer), and that exceed a specified amount and do not follow a specific pattern relative to the nature and size of the customer’s activities; to verify also the accounts through which recurrent or unusual transfers are made, including the validity of their source of funds.
   b) To report to the Compliance Unit, through the AML/CFT Branch Officer, any suspicious transfer that may involve money laundering or terrorism financing operations.
   c) To keep for a five-year period at least, a record with information on the object of the operation, the source of funds, and the beneficial owner, in case of cash deposits totaling or exceeding each USD 10,000 or its equivalent, or in case of multiple cash deposits involving lower amounts but whose aggregate amount totals or exceeds USD 10,000 or its equivalent.

6. Regarding Cashiers:
   a) To require from customers, except those exempted, to fill and sign a cash transaction slip (CTS), which must include in addition to the amount involved, information on the object of the operation, the source of funds, and the beneficial owner, in case of cash deposits totaling or exceeding each USD 10,000 or its equivalent, or in case of multiple cash deposits involving lower amounts but whose aggregate amount totals or exceeds USD 10,000 or its equivalent.
   b) To prepare special tables for the operations that exceed the ceiling specified for customers exempted from filling the cash transaction slip, and to take the technical measures needed to safeguard these tables, in order to make them available, upon request, to the Internal Audit Unit, the External Auditors, or the SIC.
   c) To report to the Compliance Unit, through the AML/CFT Branch Officer, any suspicious cash deposit that may involve money laundering or terrorism financing operations, if the relevant supporting documents cannot be obtained.

7. Regarding the Head of the Cheque Section:
   a) To give caution and attention to cheques endorsed to a third party, to bank cheques that are not directly deposited by the first beneficiary, to traveler’s cheques, to cheques issued by institutions located in foreign countries, and to cheques that do not specify the account holder’s identity.
   b) To report to the Compliance Unit, through the AML/CFT Branch Officer, any suspicious cheques.
   c) To make sure that cheques are not credited to customers’ accounts before they are effectively collected from the issuing banks.

8. Regarding the Branch Director:
   a) –
   b) To review account opening operations, to approve the exemption of certain customers from filling the cash transaction slips (CTS), and to determine the ceilings of exemption, based on criteria that justify these exemptions and ceilings, provided the names of exempted customers and the ceilings of exemption are submitted to the Compliance Unit for consideration.
c) To coordinate with the Credit Director regarding debit accounts, and with the Branches Director regarding credit accounts.

d) To make personally, or to request from the Branch Accounts Officer to make periodical visits to customers, so as to be informed of their business and assess their accounts’ movements, then prepare the relevant report with a copy to be sent to the Compliance Unit in case that report indicates the occurrence of unusual operations.

9. Regarding each of the Divisions established within the Compliance Unit, as mentioned in Paragraph 4 of Article 10 of this Decision:

a) To ascertain that operations control standards are implemented at the Head Office and the branches under its supervision, to ensure their compliance with AML/CFT regulations.

b) To prepare a monthly report on the compliance at the Head Office and branches with AML/CFT requirements, and to keep this report with the Senior Management.

SECTION V— FINAL PROVISIONS

Article 12

FIRST:
Each bank is required:

1. To establish a computerized central archive for information collected about money laundering and terrorism financing operations that includes, at least, the names circulated by the Special Investigation Commission (SIC), and those of holders of suspicious accounts reported by the bank itself. The bank must also notify the SIC of any account opened subsequently by any of these persons, whether directly, indirectly, or by proxy, as long as the SIC has not taken a decision stating that there are not, at the present time, reasonable grounds for the doubts arisen relative to any of these persons.

2. To train the employees on a continuous basis, and involve the persons in charge of the training program as well as the concerned employees in relevant seminars, workshops and lectures, in a way to keep them abreast of the latest AML/CFT methods.

3. To not close any suspicious account before referring to the SIC.

4. To maintain a special registry with the names of the persons that open or activate accounts by proxy; such registry must determine the customer/representative relationship.

5. To impose, for employees’ recruitment, the highest standards of honesty, integrity and efficiency.

6. To request their staff, subject to liability, to maintain absolute confidentiality and to not tip-off or permit to tip-off customers or any other party that the bank has notified or will notify the SIC in case of proven or suspicious ML/TF operations, or that the SIC is investigating or inquiring about their operations or accounts, until the SIC decides to lift banking secrecy on the said accounts and to notify the concerned parties.

7. When resorting to intermediaries (brokers and introducers) or to any third party, to ensure that they are regulated and supervised and meets the FATF due diligence and record-keeping requirements, and to ensure its ability to promptly and without delay obtain from them any information to identify the customer and the beneficial owner and to understand the nature of the business, as well as copies of the customer’s identification data and the CDD related documents. Provided that the ultimate responsibility for due diligence measures remains with the bank that deals with the third party, whether that third party is located inside or outside Lebanon, taking into account the risk mitigation measures, particularly associated with countries that do not or insufficiently apply the FATF Recommendations.

The bank is also required, when relying on a third party that is part of the same financial group, to act as follows:

- To verify that the third party applies the requirements of the group in terms of due diligence toward customers and PEPs and record-keeping, and complies with internal controls, and that the group is subject to supervision in this respect.

- To mitigate any high risks associated with countries, in particular those which do not or insufficiently apply the FATF Recommendations, by way of the AML/CFT guidelines and internal regulations adopted at the group level.

8. To maintain and update a special register with the names of the Beneficial Owners that were identified relative to each “Customer/natural person” and only when the Customer is not the Beneficial Owner himself, and relative to each “Customer/legal person”.

9. To identify and assess ML/TF risks that might arise due to the development of new products and new business practices, including new mechanisms for service delivery, and due to the use of new or developing technologies for both new and pre-existing products. To assess those risks prior to the launch or use of the new products, business practices, or technologies, and take appropriate measures to manage and mitigate those risks.

10. To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) in relation to the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorist financing; and once the designation decision is issued, to immediately freeze without delay the funds, accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly…) by these names; and to provide the SIC, within 48 hours at most, with evidence
on this action, and with the information available in this respect. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

11. To notify the SIC in case of similarity between the name of a customer and any designated name and details included in the national list mentioned in Subparagraph 10 of Paragraph First above.

12. To apply FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freeze without delay the funds and/or accounts, and/or operations, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; to provide the SIC, within 48 hours at most, with evidence on this action and with the information available in this respect; and in case of similarity to notify the SIC and assess the associated risks. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

13. To conduct enhanced due diligence measures that are commensurate to the level of risk, on business relationships and operations performed with natural and legal persons (including financial institutions) from countries against which the FATF calls for such action, provided that the FATF website is periodically reviewed for that purpose, especially after each FATF plenary meeting.

14. To ensure that customer due diligence information and transaction records are swiftly provided to the SIC upon request, within three business days at most.

SECOND:
Each bank must ensure that their branches and majority-owned subsidiaries operating abroad adopt the AML/CFT measures in force in Lebanon when the minimum requirements of the host country are less strict compared to Lebanon, to the extent permitted by the laws and regulations of the host country. If the host country does not permit the proper implementation of AML/CFT measures that are consistent with those applied in Lebanon, then the financial group should apply appropriate additional measures to manage ML/TF risks, and inform the SIC thereof.

THIRD:
Each Lebanese bank must conduct due diligence measures towards the customers of any of its overseas branches, whenever executing an operation or opening an account in Lebanon for any of these customers, even if these overseas branches are already conducting due diligence measures.

FOURTH:
Banks must apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by the bank itself. Examples of these measures include the following:

- To obtain the approval of the Senior Management for entering into, or continuing a business relationship with customers.
- To increase and prioritize control.
- To not establish branches or subsidiaries or representation offices for the bank in these countries.
- To not rely on third parties located in these countries.
- To terminate any correspondent relationship with institutions located in these countries.

FIFTH:
Financial groups must implement programs against money laundering and terrorist financing across the group including at all branches and majority-owned subsidiaries of that group. These programs should include the following measures:

- The appointment of a Compliance officer at the group management level.
- Policies and procedures for sharing information on customer due diligence and ML/TF risk management.
- The provision of customer, account, and operation information from branches and majority-owned subsidiaries to the compliance officer at the group level when necessary for AML/CFT purposes including information, analytical reports, and reports on activities that appear unusual. Similarly, branches and subsidiaries should receive such information from the Compliance officer at the group-level, as relevant and appropriate to risk management, analysis of information, reports, and unusual operations.
- Putting in place adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent informing or tipping-off the customer.

Article 13
The external auditor of the bank is required to:

1. Review the internal audit procedures to ascertain compliance by the bank with the provisions of the law and of these Regulations. In this respect, the external auditor shall prepare an annual report to be submitted to the Board of Directors of the bank, the Governor of Banque du Liban, and the Banking Control Commission. The report shall include, along the audit results and the external auditor’s propositions for operations control enhancement, detailed information about the verification process of the bank’s fulfillment of, at least, the obligations stated below and which include but are not limited to:

a) Complying with the provisions of Articles 3, 4, 5, 6, 10, 11, and 12 of these Regulations.

b) Filling the KYC Forms.

c) Adopting a policy and written procedures relative to the acceptance of, and the opening of new accounts for customers.

d) Enquiring about the source and final destination of
received funds, and about the reasons behind cash operations, as specified in the Law on Fighting Money Laundering and in these Regulations; setting ceilings for cash deposits and withdrawals, and for incoming cross-border transfers that require vigilance; and adopting deposit forms that show the source of deposited funds when a deposit or the total amount of several deposits exceeds the specified ceiling.

e) Preparing periodical reports (at least, quarterly) on the movement of cash deposits and withdrawals, and on incoming transfers to customers’ accounts; reviewing these reports by Management Officers and by the Internal Audit Unit.

f) Inserting, in the adopted internal audit procedures, specific measures for reviewing compliance with the said procedures.

2. Report immediately to the Governor of Banque du Liban, in his capacity as SIC Chairman, any violation of the provisions of these Regulations.

Article 14

The provisions of these Regulations shall apply to financial institutions, leasing companies, and companies issuing and promoting charge and credit cards that operate in Lebanon.

Beirut, May 18, 2001
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No. 1

Addressed to Collective Investments Schemes

Article 1

Collective Investments Schemes are required to comply, in the conduct of their business, with the provisions of the AML/CFT Law and with the relevant regulations and directives issued by Banque du Liban and/or the Special Investigation Commission, including the definition and identification of the Beneficial Owner.

Article 2

This Decision shall come into force upon its issuance.

Article 3

This Decision shall be published in the Official Gazette.

Beirut, June 26, 2018
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No. 1

Addressed to Financial Intermediation Institutions (Brokerage Firms) and Collective Investment Schemes

(These regulations were amended by BDL Intermediate Circular No. 631 dated 19/07/2022 and BDL Intermediate Circular No. 625 dated 27/05/2022)

Article 1

The following expressions shall mean:

- "Customer": Any natural or legal person, whether a company or an institution of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (mutual funds, cooperatives, welfare centers, charities, clubs, etc.).
- "Beneficial Owner": Any natural person who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the customer and/or the natural person on whose behalf operations are carried out. Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

Article 2

Financial intermediation institutions are required, as far as each is concerned, to refrain from keeping anonymous accounts or accounts in fictitious names, to adopt clear measures for account opening, and to apply to customers and beneficial owners, regardless of the value of the operation, due diligence measures which include verifying the identity of their permanent and occasional customers, whether resident or non-resident, determining the nature of their business, understanding the ownership structure and/or control over the legal person, understanding and identifying the purpose and nature of the business relationship and/or the account opening, obtaining data on that purpose when needed, identifying the beneficial owner and the source of funds, and conducting ongoing monitoring of operations, particularly in the following cases:

- Before or when starting the business relationship or opening accounts of all kinds.
- Electronic funds transfers.
- When carrying out a single operation or several linked operations, whose total is equal to, or above 10,000 USD or its equivalent.
- Whenever a customer is suspected to attempt a money laundering or terrorist financing operation.

Article 3

When identifying the “Beneficial Owner”:
**FIRST:**
With respect to the customer that is a legal person, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:

1. Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.
2. In case of doubt as to whether the natural person(s) identified pursuant to Paragraph “First”, Subparagraph 1 above is (are) the beneficial owner(s), or when no natural person holds 20% or more of the customer’s capital, it is required to identify the natural persons who exercise control over the legal person through other means (e.g. holding a majority of voting rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities...).
3. When no natural person is identified pursuant to Paragraph “First”, Subparagraphs (1) and (2) above, reasonable measures shall be taken in order to identify and verify the identity of the persons holding senior management positions.

**SECOND:**
With respect to customers that are legal arrangements, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:

1. For trusts, each of the persons below shall be identified:
   - The Settlor
   - The Trustee
   - The Protector
   - The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.
   - Any other natural person who exercises an effective control over the trust through direct or indirect ownership or through other means.

The definitions included in the glossary of the FATF 40 Recommendations shall be adopted to identify the persons mentioned in this Subparagraph 1.

2. For other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Paragraph Second, Subparagraph 1 above, must be identified.

**THIRD:**
Upon the identification of the beneficial owner, it is required to conduct the same due diligence measures applicable to customers, including those issued by the Special Investigation Commission (SIC).

**Article 4**
In order to verify the identity of the customer and the beneficial owner, the employee in charge of executing the operation must request from the customer or from the person acting on behalf of the latter, the following official documents or data:

a) For a natural person: a passport, ID card, extract of Civil Status, or residence permit.

b) For a legal person, whether a company or an institution or a legal arrangement, a duly certified copy of the bylaws, the registration certificate, the ownership structure, the list showing the distribution of equities or shares (directly or indirectly), the list of authorized signatories, in addition to a copy of identity for the legal representative, the managers, and the natural persons who own, directly or indirectly, a controlling interest in the company’s management, and also the statement submitted by the beneficial owner to the Ministry of Finance and to the Commercial Register.

c) In case the operation is carried out through a proxy or a person acting on behalf of the customer: the original power of attorney or a certified copy thereof, or a document proving that this person is authorized to act as such, in addition to the identity documents of the customer, the proxy, and the person acting on the customer’s behalf, and these documents must be verified. The due diligence measures must also be applied to the non-professional proxy.

**Article 5**
The financial intermediation institution must maintain all the records obtained through CDD measures toward the customer and the beneficial owner, in particular the full name, occupation, and residential address, the address of the registered office for the legal person, or, if different, the principal place of business, and the financial situation, as well as the account files for at least five years after the account is closed or the business relationship is ended, and all records on operations, including business correspondence and the results of any analysis undertaken, for at least five years after the date of the operation. Such records must be sufficient to permit reconstruction of individual operations, so as to provide, if necessary, evidence for legal action and prosecution of criminal activity.

**Article 6**
Whenever due diligence measures required towards customers and beneficial owners, as mentioned in Article 2 above, cannot be satisfactorily conducted, then no account should be opened or relationship started or operation performed, or the existing business relationship should be terminated; and notifying the SIC should be considered.

**Article 7**
Financial intermediation institution must conduct continuous due diligence measures on all their customers, in order to modify or add to the adopted KYC Form, any information resulting from any changes in the customer’s situation, especially if there are doubts about the veracity or adequacy of previously obtained data, or in case there are subsequent changes in the identity of the customer or beneficial owner. Therefore, each institution is required to prepare an action plan with precise dates to fulfill these obligations.
Article 8
Financial intermediation institutions are required:
1. In case they suspect that the customer is not the beneficial owner or if the customer states that the beneficial owner is a third party, to request from the customer a written statement that identifies the beneficial owner (true beneficiary), particularly the latter’s full name, residential address, occupation and financial situation, and to keep a copy of this statement and of the beneficial owner’s identity throughout the period mentioned in Article 5 above. Doubts about the beneficial owner’s identity arise in instances that include, but are not limited to, the following:
   a) When a power of attorney is given to a non-professional person (e.g. other than a lawyer or a fully authorized representative or a financial intermediary) and no relationship between the customer and the proxy justifies that power of attorney.
   b) When the business relationship is conducted through front institutions/companies.
   c) When the customer’s financial situation is known to the employee executing the operation, and the amount of the intended operation is inconsistent with that financial situation.
   d) When any other indicator draws the attention of the company in the course of its business.
2. To promptly notify the Governor of Banque du Liban in his capacity as Chairman of the Special Investigation Commission, whenever they suspect or believe, based on reasonable or objective grounds that the executed or attempted operation is related to money laundering or associated predicate offences, or to terrorist financing, terrorist acts, or terrorist organizations, regardless of the amount involved. Additionally, if money laundering or terrorist financing is suspected, and if they reasonably believe that performing the CDD measures will tip off the customer, it is then permitted not to pursue the CDD process and the SIC should be notified without delay.

Article 9
Financial intermediation institutions are required:
1. To take appropriate steps to identify, assess and understand their ML/TF risks, and to apply, based on risk understanding, a risk-based approach to classify customers and operations according to the level of risk (low, medium, and high risk).
   For indicative purposes only, customer risk, country risk, and service risk are taken into account when classifying the risk of customers and operations:
   a) Customer risk:
      • Customers whose occupation relies mainly on cash: money exchange, restaurants and night-clubs, car dealers, non-banking institutions performing electronic transfers of cash
      • Politically Exposed Persons (PEPs).
      • Offshore companies.
      • Companies located in countries known to be tax havens.
      • Non face-to-face customers.
      • Customers dealing through intermediaries only.
      • Customers dealing through fiduciary contracts or trusts.
      • Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
      • Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.
   b) Country risk:
      • The stringency of AML/CFT laws, and the efficiency of supervisory and judiciary authorities in charge of their implementation.
      • The existence of banking secrecy.
      • The situation of the country in terms of corruption and organized crime.
   c) Service risk:
      • Private Banking.
      • Management of collective investment schemes.
      • Dealing or trading in financial instruments
2. To put in place risk-based control measures and procedures, and to adopt, at least for customers and beneficial owners, for PEPs as per FATF definition and their family members and close associates, and for operations classified as “high risk” according to risk scoring, the enhanced measures and procedures below for the purpose of risk management and mitigation:
   a) To increase and prioritize control, and to conduct enhanced ongoing monitoring of the business relationship.
   b) To obtain more detailed information on customers and beneficial owners (Increased KYC Levels), in particular to determine the source of their wealth.

1) Politically Exposed Persons (PEPs) are foreign or domestic individuals who are or have been entrusted with prominent public functions by a foreign country or domestically, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, as well as members of senior management, i.e. directors, deputy directors and members of the Board or equivalent functions in any international organization. This definition of PEPs is not intended to cover middle ranking or more junior individuals in the aforementioned categories.
1. Preparing an AML/CFT procedural manual that includes provisions stipulated in this circular, with due consideration of the structure and departments of the financial intermediation institution, and updating the manual when needed. Also, preparing the KYC form as mentioned in Article 7 above and submitting the manual and the KYC form to Senior Management for approval and adoption.

2. Conducting scrutiny of operations undertaken throughout the course of the relationship with customers to ensure that the operations performed are consistent with the institution’s knowledge of the customers, their business and risk profile, including, where necessary, the source of funds.

3. Ensuring that documents, data or information collected under the CDD process are kept up-to-date and are appropriate, by reviewing the existing records, particularly for high-risk categories of customers, as well as preparing relevant periodic reports and submitting them to the Senior Management.

4. Applying due diligence measures to existing customers on the basis of materiality and risk, and also conducting due diligence on such existing business relationships in a timely manner, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.

5. Verifying the proper implementation and efficiency of AML/CFT procedures and monitoring accounts (through adequate software programs when needed that display money laundering and terrorism financing indicators), in order to ensure there are no suspicious ML/TF transactions; and preparing relevant periodic reports and submitting them to the Senior Management.

6. Conducting enhanced due diligence measures that are commensurate to the level of risk, on business relationships and operations performed with natural and legal persons (including financial institutions) from countries against which the FATF calls for such action, provided that the FATF website is periodically reviewed for that purpose, especially after each FATF plenary meeting.

7. _

**Article 10**

Financial intermediation institutions are required to put in place and adopt an efficient internal control system that includes the appointment of a Compliance Officer at the management level, who has sufficient AML/CFT expertise, and whose mission consists of:

1. Preparing an AML/CFT procedural manual that includes provisions stipulated in this circular, with due consideration of the structure and departments of the financial intermediation institution, and updating the manual when needed. Also, preparing the KYC form as mentioned in Article 7 above and submitting the manual and the KYC form to Senior Management for approval and adoption.

2. Conducting scrutiny of operations undertaken throughout the course of the relationship with customers to ensure that the operations performed are consistent with the institution’s knowledge of the customers, their business and risk profile, including, where necessary, the source of funds.

3. Ensuring that documents, data or information collected under the CDD process are kept up-to-date and are appropriate, by reviewing the existing records, particularly for high-risk categories of customers, as well as preparing relevant periodic reports and submitting them to the Senior Management.

4. Applying due diligence measures to existing customers on the basis of materiality and risk, and also conducting due diligence on such existing business relationships in a timely manner, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.

**Article 11**

Financial intermediation institutions must not enter into, or continue a correspondent relationship with a shell bank. When establishing a relationship with a correspondent bank abroad and other similar relationships, the institution must verify that the bank really exists, based on gathered documentary evidence, that it does not deal with shell banks, has a good reputation, is subject to a sound control, including whether it has been subject to a money laundering or terrorist financing investigation or supervisory action, and applies efficient and effective AML/CFT measures.

In addition to the foregoing, the institution must implement the measures below:

1. To obtain the approval of the Senior Management before establishing correspondent banking relationships.

2. To verify the nature of the business of the foreign respondent bank.

3. To understand the respective responsibilities of the institution and the foreign respondent bank.

4. With respect to payable-through accounts opened by foreign correspondent banks, to take adequate steps to be satisfied that these banks have conducted the due diligence measures toward customers having direct access to accounts of the correspondent bank, and verify that this bank is able to provide relevant CDD information upon request.

**Article 12**

Financial intermediation institutions are required to set and keep up-to-date centralized data repository for the information collected on money laundering and terrorist financing operations, which includes, at least, the names circulated by the SIC, those of suspicious accounts reported to the SIC by the concerned institution.
Article 13
Financial intermediation institutions are requested, as far as each is concerned, the following:

1. To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) in relation to the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorist financing; and once the designation decision is issued, to immediately freeze without delay the funds, accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly...) by these names; and to provide the SIC, within 48 hours at most, with evidence on this action, and with the information available in this respect. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

2. To notify the SIC in case of similarity between the name of a customer and any designated name and details included in the national list mentioned in Subparagraph 1 of this article.

Article 14
Financial intermediation institutions are required:

1. To maintain a special registry with the names of the persons that open or activate accounts by proxy; such registry must determine the customer/representative relationship.

2. To impose, when hiring employees, high standards for honesty, integrity, and skills.

3. To provide ongoing training to employees, and to involve the concerned officers and employees in seminars, workshops, and lectures, in a way to keep them abreast of the latest AML/CFT methods.

4. To request its staff, subject to liability, not to inform customers when the SIC investigates or scrutinizes their operations, unless the SIC issues a decision to notify the concerned parties.

5. To ensure that their branches and majority-owned subsidiaries operating abroad apply the AML/CFT measures in force in Lebanon when the minimum requirements of the host country are less strict compared to Lebanon, to the extent permitted by the laws and regulations of the host country. If the host country does not permit the proper implementation of AML/CFT measures that are consistent with those applied in Lebanon, then the financial group should apply appropriate additional measures to manage ML/TF risks, and inform the SIC thereof.

6. To verify, when relying on a third party, that the latter is regulated and supervised, and meets the FATF due diligence and record-keeping requirements; to ensure also that the information needed to identify the customer and the beneficial owner and to understand the nature of the business, as well as copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party immediately and without delay. In all cases, the ultimate responsibility for CDD measures remains with the party relying on the third party, whether the third party is located inside or outside Lebanon, taking into consideration, upon such reliance, risk mitigation measures, in particular for risks associated with countries that do not or insufficiently apply the FATF Recommendations.

7. To identify and assess the ML/TF risks that might arise in relation to the development of new products and new business practices, including new service delivery mechanisms, and in relation to the use of new or developing technologies for both new and pre-existing products. A risk assessment should also take place prior to the launch or use of these products or business practices or technologies, and appropriate measures taken to manage and mitigate those risks.

8. To apply FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freeze without delay the funds and/or accounts, and/or operations, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; to provide the SIC, within 48 hours at most, with evidence on this action and with the information available in this respect; and in case of similarity to notify the SIC and assess the associated risks. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

9. Financial intermediation institutions must apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by the institution itself. Examples of these measures include the following:
   • To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers.
   • To increase and prioritize control.
   • To not establish branches or subsidiaries or representative offices for the institution in these countries.
   • To not rely on third parties located in these countries.
   • To terminate any correspondent relationship with institutions located in these countries.

10. To ensure that customer due diligence information and transaction records are swiftly provided to the SIC upon request, within three business days at most.

11. Financial groups must implement programs against money laundering and terrorist financing across the
group including at all branches and majority-owned subsidiaries of that group. These programs should include the following measures:

• The appointment of a Compliance officer at the group management level.
• Policies and procedures for sharing information on customer due diligence and ML/TF risk management.
• The provision of customer, account, and operation information from branches and majority-owned subsidiaries to the compliance officer at the group level when necessary for AML/CFT purposes including information, analytical reports, and reports on activities that appear unusual. Similarly, branches and subsidiaries should receive such information from the Compliance officer at the group-level, as relevant and appropriate to risk management, analysis of information, reports, and unusual operations.
• Putting in place adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent informing or tipping off the customer.

Article 15
Financial intermediation institutions are required to consider for indicative purposes only that the indicators listed below, if not justified, point out to the possible existence of ML/TF offences:

• Instantly withdrawing funds from accounts after being deposited for a short period of time.
• Transferring funds to banks or financial institutions that differ from those originally received from, including those present in various countries.
• A customer engaging in the purchase of highly priced securities, and consequently selling them for a great loss.
• A customer’s financial transactions reflect a pattern of continuous losses.
• Activating a dormant account after a while, with no clear justification.
• No economic justification for the customer’s transactions.
• A customer’s willingness to invest in a product, while lacking basic understanding of its features and performance.
• Investing in long-term products, followed shortly by a request to liquidate accounts, irrespective of fees and penalties.
• Sudden change in a customer’s account movement that is inconsistent with the usual activity.
• A customer opening multiple accounts for several companies with control over them.

Article 15 bis
The provisions of this Basic Decision shall apply to investment schemes operating in Lebanon.

Article 16
This Decision shall come into force upon its issuance.

Article 17
This decision shall be published in the Official Gazette.

Beirut, June 26, 2018
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No.2
Addressed to Financial Institutions
(Provisions of Article 7 Bis were added as per BDL Intermediate Circular No.274 dated August 22, 2011)

Article 7 bis
All financial institutions are prohibited from:

1. Undertaking money exchange operations, except when such operations are complementary or linked to those they perform, within the limits of their objects, on behalf of their customers.
2. Undertaking cross-border transportation of cash, metal coins and bullion.
3. Receiving funds from their customers, unless through checks or transfers, including funds received for the purpose of creating or covering all margins. They are, however, entitled to receive from a single customer cash amounts whose monthly total does not exceed the equivalent of USD 10,000 for reimbursing the advances granted by these institutions (including factoring operations), or for performing, in a secondary manner, various services that do not include financial intermediation (property management, phone bills’ domiciliation…).
4. Executing, at their customers’ request and in favour of third parties in Lebanon or abroad, foreign or domestic incoming transfers in excess of USD 1,500.

Beirut, October 22, 1998
The Governor of the Banque du Liban
Riad Toufic Salamé
BDL Basic Circular No. 2

Addressed to Specialized Lending Entities
(Known as “Comptoirs”)

(The provisions of Article 12 bis were amended by BDL Intermediate Circular No. 634 dated 19/07/2022 and BDL Intermediate Circular No. 625 dated 27/05/2022)

Article 12
Specialized Lending Entities shall comply with applicable laws, and with the regulations issued by Banque du Liban and the Banking Control Commission, not contradicting with the measures stipulated in this Circular, particularly those:

- Related to fighting money laundering and terrorism financing, including with respect to the definition and identification of the Beneficial Owner.

Article 12 Bis

FIRST:
The following expressions shall mean:

- "Customer": Any natural or legal person, whether a company or an institution of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (Mutual funds, cooperatives, welfare centers, charities, clubs, etc.).

- "Beneficial Owner": Any natural person who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the customer and/or the natural person on whose behalf operations are carried out. Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

SECOND:
Specialized lending entities are required, as far as each is concerned, to refrain from keeping anonymous accounts or accounts in fictitious names, to adopt clear measures for account opening, to apply due diligence measures on customers and beneficial owners regardless of the value of the operation which include verifying the identity of their permanent and occasional customers, whether resident or non-resident, determining the nature of their business, understanding the ownership structure and/or control over the legal person, understanding and identifying the purpose and nature of the business relationship and/or the account opening, obtaining data on that purpose when needed, identifying the beneficial owner and the source of funds, and conducting ongoing monitoring of operations, particularly in the following cases:

- Before or when starting the business relationship or opening accounts of all kinds.

- When carrying out a single operation or several linked operations, whose total is equal to, or above USD 10,000 or its equivalent and that on the same account or on several accounts held by the same person.

- Whenever a customer is suspected to attempt a money laundering or terrorist financing operation.

THIRD:
When identifying the “Beneficial Owner”:

1. With respect to the customer that is a legal person, the “beneficial owner” shall be identified and reasonable measures taken to identify them in the following manner:

   a) Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.

   b) In case of doubt as to whether the natural person(s) identified pursuant to paragraph (1), subparagraph (a) above is (are) the beneficial owner(s), or when no natural person holds 20% or more of the customer’s capital, it is required to identify the natural persons who exercise control over the legal person through other means (e.g. holding a majority of voting rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities…).

   c) When no natural person is identified pursuant to paragraph (1), subparagraphs (a) and (b) above, reasonable measures shall be taken in order to identify and verify the identity of the persons holding senior management positions.

2. With respect to customers that are legal arrangements, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:

   a) For trusts, each of the persons below shall be identified:

      - The Settlor
      - The Trustee
      - The Protector
      - The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.

      - Any other natural person who exercises an effective control over the trust through direct or indirect ownership or through other means.

      The definitions included in the glossary of the FATF 40 Recommendations shall be adopted to identify the persons mentioned in this Subparagraph (a).

   b) For other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Paragraph (2), subparagraph (a) above, must be identified.
3. Upon the identification of the beneficial owner, it is required to conduct the same due diligence measures applicable to customers, including those issued by the Special Investigation Commission (SIC).

FOURTH:
In order to verify the identity of the customer and the beneficial owner, the employee in charge of executing the operation must request from the customer or the person acting on behalf of the latter, the following official documents or data:

1. For a natural person: a passport, ID card, extract of Civil Status, or residence permit.
2. For a legal person, whether a company or an institution considered, account should be opened or relationship should be started (2) of this article cannot be satisfactorily conducted, then no customers and beneficial owners, as mentioned in paragraph of the operation performed, or the existing business relationship should be terminated; and notifying the SIC should be notified without delay.
3. In case the operation is carried out through a proxy or a person acting on behalf of the customer: the original power of attorney or a certified copy thereof, or a document proving that this person is authorized to act as such, in addition to the identity documents of the customer, the proxy, and the person acting on the customer’s behalf, and these documents must be verified. The due diligence measures must also be applied to the nonprofessional proxy.

FIFTH:
Specialized Lending Entities must maintain all the records obtained through CDD measures toward the customer and the beneficial owner, in particular the full name, occupation, and residential address, the address of the registered office for the legal entity, or, if different, the principal place of business, and the financial situation, as well as the account files for at least five years after the account is closed or the business relationship is ended, and all the records of operations, including business correspondence and the results of any analysis undertaken, for at least five years after the date of the operation. Such records must be sufficient to permit reconstruction of individual operations, so as to provide, if necessary, evidence for legal action and prosecution of criminal activity.

SIXTH:
Whenever due diligence measures required towards customers and beneficial owners, as mentioned in paragraph (2) of this article cannot be satisfactorily conducted, then no account should be opened or relationship should be started or operation performed, or the existing business relationship should be terminated; and notifying the SIC should be considered.

SEVENTH:
Specialized Lending Entities are required to conduct continuous due diligence measures on all their customers, in order to modify or add to the adopted KYC Form, any information resulting from any changes in the customer’s situation, especially if there are doubts about the veracity or adequacy of previously obtained data, or in case there are subsequent changes in the identity of the customer or the beneficial owner. Therefore, each specialized lending entity is required to prepare an action plan with precise dates to fulfill these obligations.

EIGHTH:
Specialized Lending Entities are required:

1. In case they suspect that the customer is not the beneficial owner or if the customer states that the beneficial owner is a third party, to request from the customer a written statement that identifies the beneficial owner, particularly the latter’s full name, residential address, occupation and financial situation, and to keep a copy of this statement and of the beneficial owner’s identity throughout the period mentioned in Paragraph (5) of this Article. Doubts about the beneficial owner’s identity arise in instances that include, but are not limited to, the following:
   a) When a power of attorney is given to a non-professional person (e.g., other than a lawyer or a fully authorized representative or a financial intermediary) and no relationship between the customer and the proxy justifies that power of attorney.
   b) When the business relationship is conducted through front institutions/companies.
   c) When the customer’s financial situation is known to the employee executing the operation, and the amount of the intended operation is inconsistent with that financial situation.
   d) When any other indicator draws the attention of the company in the course of its business.

2. To promptly notify the Governor of Banque du Liban in his capacity as Chairman of the Special Investigation Commission, whenever they suspect or believe, based on reasonable or objective grounds that the executed or attempted operation is related to money laundering or associated predicate offences, or to terrorist financing, terrorist acts, or terrorist organizations, regardless of the amount involved. Additionally, if money laundering or terrorist financing is suspected, and if they reasonably believe that performing the CDD measures will tip off the customer, it is then permitted not to pursue the CDD process and the SIC should be notified without delay.

NINTH:
Specialized Lending Entities are required:

1. To take appropriate steps to identify, assess and understand its ML/TF risks, and to apply, based on risk understanding, a risk-based approach to classify
customers and operations according to the level of risk (low, medium, and high risk).

For indicative purposes only, customer risk, country risk, and service risk are taken into account, when classifying the risks of customers and operations:

a) Customer risk:
   - Customers whose occupation relies mainly on cash.
   - Politically Exposed Persons (PEPs).
   - Offshore companies.
   - Companies located in countries known to be tax havens.
   - Non face-to-face customers.
   - Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
   - Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.

b) Country risk:
   - The stringency of AML/CFT laws, and the efficiency of supervisory and judiciary authorities in charge of their implementation.
   - The existence of banking secrecy.
   - The situation of the country in terms of corruption and organized crime.

c) Service risk:
   - Commercial loans.
   - Loans with insufficient cash/in-kind collaterals.

2. To put in place risk-based control measures and procedures, and to adopt, at least, for customers and beneficial owners, for PEPs\(^1\) as per FATF definition and their family members and close associates, and for operations classified as “high risk” according to risk scoring, the enhanced measures and procedures below for the purpose of risk management and mitigation:

a) To increase and prioritize control, and to conduct enhanced ongoing monitoring of the business relationship.

b) To obtain more detailed information on customers and beneficial owners (Increased KYC Levels), in particular to determine the source of their wealth.

c) To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers, and for executing operations, in a way that is commensurate to the specified level of risk.

d) To review periodically the relationship with customers.

e) To make continuous peer comparisons.

f) To set up an adequate system so as to determine whether the customer or beneficial owner is a PEP.

3. To take into account the duration and soundness of the business relationship with the customer.

4. To use software programs in order to conduct the controls needed as per the adopted scoring.

5. To have the Senior Management adopt a special policy, as well as controls and measures that are based on the requirements specified in this Article, in order to classify and mitigate risks.

6. To document risk assessment results when necessary, and to keep them for provision to the competent authorities when needed.

TENTH:

Specialized Lending Entities are required to put in place and adopt an efficient AML/CFT internal control system that includes, the appointment of a Compliance Officer at the management level, who has sufficient AML/CFT expertise, and whose mission consists of:

1. Preparing an AML/CFT procedural manual that includes provisions stipulated in this circular, with due consideration of the structure and departments of the company, and updating the manual when needed. Also, preparing the KYC form mentioned in paragraph 7 of this article, and submitting the manual and the KYC Form to senior management for approval and adoption.

2. Conducting scrutiny of operations undertaken throughout the course of the relationship with customers to ensure that the operations performed are consistent with the entity’s knowledge of the customers, their business and risk profile, including, where necessary, the source of funds.

3. Ensuring that documents, data or information collected under the CDD process are kept up-to-date and are appropriate, by reviewing the existing records, particularly for high-risk categories of customers, and providing relevant periodical reports to senior management.

4. Applying due diligence measures to existing customers on the basis of materiality and risk, and also conducting due diligence on such existing business relationships in

---

1) Politically Exposed Persons (PEPs) are foreign or domestic individuals who are or have been entrusted with prominent public functions by a foreign country or domestically, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, as well as members of senior management, i.e. directors, deputy directors and members of the Board or equivalent functions in any international organization. This definition of PEPs is not intended to cover middle ranking or more junior individuals in the aforementioned categories.
a timely manner, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.

5. Verifying the proper implementation and the efficiency of AML/CFT procedures and monitoring accounts (through adequate software programs when needed that display ML/TF indicators), in order to ensure there are no suspicious transactions, and preparing relevant periodical reports and submitting them to senior management.

6. Conducting enhanced due diligence measures that are commensurate to the level of risk, on business relationships and operations performed with natural and legal persons (including financial institutions) from countries against which the FATF calls for such action, provided that the FATF website is periodically reviewed for that purpose, especially after each FATF plenary meeting.

7. ELEVENTH:
Specialized Lending Entities are required to set and keep up-to-date centralized data repository for the information collected on money laundering and terrorist financing operations, which includes, at least, the names circulated by the SIC, and those of suspicious accounts reported to the SIC by the concerned entity.

TWELFTH:
Specialized Lending Entities are requested, as far as each is concerned, the following:

1. To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) in relation to the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorist financing; and once the designation decision is issued, to immediately freeze without delay the funds, accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly...) by these names; and to provide the SIC, within 48 hours at most, with evidence on this action, and with the information available in this respect. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

2. To notify the SIC in case of similarity between the name of a customer and any designated name and details included in the national list mentioned in paragraph (12), subparagraph (1) above.

THIRTEENTH:
Specialized Lending Entities are required:

1. To impose, when hiring employees, high standards for honesty, integrity, and skills.

2. To provide ongoing training to employees, and involving concerned officers and employees in seminars, workshops, and lectures, to keep them abreast of the latest AML/CFT methods.

3. To request its staff, subject to liability, not to inform customers when the SIC investigates or scrutinizes their operations, unless the SIC issues a decision to notify the concerned parties.

4. To ensure that their branches and majority-owned subsidiaries operating abroad apply the AML/CFT measures in force in Lebanon when the minimum requirements of the host country are less strict compared to Lebanon, to the extent permitted by the laws and regulations of the host country. If the host country does not permit the proper implementation of AML/CFT measures that are consistent with those applied in Lebanon, then the financial group should apply appropriate additional measures to manage ML/TF risks, and inform the SIC thereof.

5. To verify, when relying on a third party, that the latter is regulated and supervised, and meets the FATF due diligence and record-keeping requirements; to ensure also that the information needed to identify the customer and the beneficial owner and to understand the nature of the business, as well as copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party immediately and without delay. In all cases, the ultimate responsibility for CDD measures remains with the party relying on the third party, whether the third party is located inside or outside Lebanon, taking into consideration, upon such reliance, risk mitigation measures, in particular for risks associated with countries that do not or insufficiently apply the FATF Recommendations.

6. To identify and assess the ML/TF risks that might arise in relation to the development of new products and new business practices, including new service delivery mechanisms, and in relation to the use of new or developing technologies for both new and pre-existing products. A risk assessment should also take place prior to the launch or use of these products or business practices or technologies, and appropriate measures taken to manage and mitigate those risks.

7. To apply FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freeze without delay the funds and/or accounts, and/or operations, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; to provide the SIC, within 48 hours at most, with evidence on this action and with the information available in this respect; and in case of similarity to notify the SIC and assess the associated risks. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.
8. To provide the SIC, with a copy of the annual report prepared by the external auditor, on verifying the AML/CFT measures implemented at the concerned institution, and assessing their efficiency.

9. To apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by the institution itself. Examples of these measures include the following:
   • To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers.
   • To increase and prioritize control.
   • To not establish branches or subsidiaries or representation offices for the institution in these countries.
   • To not rely on third parties located in these countries.
10. To ensure that customer due diligence information and transaction records are swiftly provided to the SIC upon request, within three business days at most.

FOURTEENTH:
Specialized Lending Entities are required to consider for indicative purposes only, that the indicators listed below point out to the possible existence ML/FT offences:
• Settling a loan with a single payment shortly after receiving the loan.
• Settling a loan through third parties transfers.
• Payments for loan settlement inconsistent with the customer’s financial status.
• Loan type and amount inconsistent with the customer’s needs or differ from previously requested loans that were granted.
• Requesting to transfer a loan amount to overseas accounts.
• No clear relationship between the beneficial owner and the loan applicant.
• The source of funds used to settle the loan is unclear.
• The customer’s willingness to pay unusual expenses to secure the loan.
• The customer makes unjustified inquiries, particularly with respect to the adopted due diligence measures.
• Revoking the loan application when additional documents or information are requested from the customer.

FIFTEENTH:
To verify that AML/CFT programs are implemented across the Financial group and covers all branches and majority-owned subsidiaries of that group. These programs should include the following measures:
• The appointment of a Compliance officer at the group management level.
• Policies and procedures for sharing information on customer due diligence and ML/TF risk management.
• The provision of customer, account, and operation information from branches and majority-owned subsidiaries to the compliance officer at the group level when necessary for AML/CFT purposes including information, analytical reports, and reports on activities that appear unusual. Similarly, branches and subsidiaries should receive such information from the Compliance officer at the group-level, as relevant and appropriate to risk management, analysis of information, reports and unusual operations.
• Putting in place adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent informing or tipping-off the customer.

Beirut, January 21, 2016
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No. 3
Implementation Rules of the Law regulating the Money Changer Profession

(These regulations were amended by BDL Intermediate Circular No. 632 dated 19/07/2022 and BDL Intermediate Circular No. 625 dated 27/05/2022)

SECTION V - MISCELLANEOUS PROVISIONS

Article 9
Exchange institutions are required to send promptly to the concerned bank a notification including:
1. Information about any check issued by the exchange institution and drawn on the concerned bank, or about any banking transaction performed through the said bank on behalf of the exchange institution’s customers, particularly whether or not the check-related transaction or the banking transaction was performed against an amount received in cash, in addition to information about the source and destination of funds, and the identity of both the beneficiary and the economic right owner, when the check or transaction exceeds USD 10,000 or its equivalent.
2. The information mentioned in Paragraph 1 of this Article, concerning any transfer performed through the bank in favor of third persons in Lebanon and resulting from an exchange operation or cross-border transportation of cash and/or precious metals, regardless of the amount being transferred.
Article 10
The exchange institution is prohibited from opening bank accounts at a bank where any of the institution’s owners, partners, shareholders, directors or authorized signatories holds an account. The spouse and the dependent ascendants and descendants of these persons shall be considered as a single person. Accounts held by exchange institutions at banks shall be used solely to perform exchange operations.

Article 11
All exchange institutions must:
• Communicate to the Banking Control Commission the name of the banks where they hold accounts and notify it of any subsequent change therein.
• Take the required measures to communicate to the Banking Control Commission the names of the banks where any of the persons mentioned in Article 10 above holds an account, and notify it of any subsequent change therein.

Article 12
All exchange institutions are required, when receiving from a customer cash amounts and/or metal coins and bullion (hereafter precious metals”) to be converted into other currencies and/or precious metals, or when undertaking cross-border transportation of cash and/or precious metals, to carry out these operations solely in one of the following manners:
• by delivering cash amounts and/or precious metals to the customer, according to the case
• by issuing a check in the customer’s name payable to the first beneficiary only
• by a transfer order to the concerned customer’s account in a bank operating in Lebanon or abroad, with no request to make a transfer to a third person except within Lebanon, and provided the obligation mentioned in Paragraph 2 of Article 9 of these Rules is fulfilled, regardless of the amount being transferred.

Article 13
1. All exchange institutions are prohibited from:
   • Making direct cash deposits in their customers’ bank accounts.
   • Accepting any proxy on behalf of their customers.
2. Exchange institutions classified as Category A are prohibited from making any transfer in excess of 1,500 US dollars that does not result from an exchange operation or a cross-border transport operation, when the transfer consists of receiving cash amounts from customers then transferring them to third persons whether in Lebanon or abroad through the institution’s bank accounts.
3. Exchange institutions are prohibited from performing any kind of exchange or non exchange operation, whether recorded in or off-balance sheet, with companies or mutual funds whose stocks or shares are fully or partially issued in bearer form, or that are directly or indirectly owned by companies or mutual funds whose stocks and shares are fully or partially issued in bearer form.

Article 14
In the course of their activities, all exchange institutions must comply with the following:
• Not open any kind of deposit accounts for customers, whether temporary or transitional, against the cash amounts it receives from the latter.
• Perform the operations that fall within their legally authorized duties, solely through their bank accounts and without using the personal accounts held by any of the persons mentioned in Article 10 above.

Article 15
FIRST:
The following expressions shall mean:
• “Customer”: Any natural or legal person, whether a company or an institution of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (mutual funds, cooperatives, welfare centers, charities, clubs, etc.).
• “Beneficial Owner”: Any natural person who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the customer and/or the natural person on whose behalf operations are carried out. Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

SECOND:
As far as each is concerned, exchange institutions are required:
1. To apply to customers and beneficial owners, regardless of the value of the operation, due diligence measures which include verifying the identity of their permanent and occasional customers, whether resident or non-resident, determining the nature of their business, understanding the ownership structure and/or control over the legal person, understanding and identifying the purpose and nature of the business relationship, obtaining data on that purpose when needed, identifying the beneficial owner and the source of funds, and conducting ongoing monitoring of operations, particularly in the following cases:
   a) Before or when a business relationship is being established or started.
   b) When carrying out a single operation or several linked operations, whose total is equal to, or above USD 10,000 or its equivalent.
c) Whenever a customer is suspected to attempt a money laundering or terrorist financing operation.

2. To apply due diligence measures to existing customers on the basis of materiality and risk, and also to conduct due diligence on such existing business relationships in a timely manner, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.

3. To request the official documents or data stated below, for the purpose of verifying the identity of the customer and of the beneficial owner:
   a) For a natural person: a passport, ID card, extract of Civil Status, or residence permit.
   b) For a legal person, whether a company or an institution or a legal arrangement, a duly certified copy of the bylaws, the registration certificate, the ownership structure, the list showing the distribution of equities or shares (directly or indirectly), the list of authorized signatories, in addition to a copy of identity for the legal representative, the managers, and the natural persons who own, directly or indirectly, a controlling interest in the company’s management.
   c) If the operation is carried out through a proxy or a person acting on behalf of the customer: the original power of attorney or a certified copy thereof, or a document proving that this person is authorized to act as such, in addition to the identity documents of the customer, the proxy and the person acting on the customer’s behalf, and these documents must be verified. The due diligence measures specified in Subparagraph (1) of this Paragraph “Second” must also be applied to the non-professional proxy.

4. Whenever due diligence measures required towards customers and beneficial owners cannot be satisfactorily conducted, then no relationship should be started or operation performed, or the existing business relationship should be terminated; and notifying the SIC should be considered.

5. To keep special records for each operation above the amount of USD 10,000 or its equivalent.

6. To maintain all the records obtained through CDD measures towards the customer and the beneficial owner, in particular the full name, occupation, and residential address, the address of the registered office for the legal person, or, if different, the principal place of business, and the financial situation, as well as the account files for at least five years after the account is closed or the business relationship is ended, and all records on operations, including business correspondence and the results of any analysis undertaken, for at least five years after the date of the operation. Such records must be sufficient to permit reconstruction of individual operations, so as to provide, if necessary, evidence for legal action and prosecution of criminal activity.

7. To put in place and adopt an efficient AML/CFT internal control system that includes, at least, the following:
   a) Efficient and effective AML/CFT guidelines, approved and adopted by the Senior Management, and including, as a minimum, the due diligence measures required for customers with recurrent operations rising above a defined threshold.
   b) When hiring employees, imposing high standards for honesty, integrity, and skills.
   c) The appointment of a Compliance Officer at the management level, who has sufficient AML/CFT expertise, constantly attends training sessions in this respect, holds specialized certificates such as the CAMS-Certified Anti-Money Laundering Specialist certificate specified in Basic Decision 9286 of 9 March 2006 attached to Basic Circular 103, and whose mission consists in:
      • Providing ongoing training to employees, and involving concerned officers and employees in seminars, workshops, and lectures, to keep them abreast of the latest AML/CFT methods.
      • Preparing periodic reports on a risk-based supervision of operations, and the extent of compliance with the required measures.
      • Conducting scrutiny of operations undertaken throughout the course of the relationship with customers to ensure that the operations performed are consistent with the institution’s knowledge of the customers, their business and risk profile, including, where necessary, the source of funds.
      • Ensuring that documents, data or information collected under the CDD process are kept up-to-date and are appropriate, by reviewing the existing records, particularly for high-risk categories of customers.
      • Conducting enhanced due diligence measures that are commensurate to the level of risk, on business relationships and operations performed with natural and legal persons (including financial institutions) from countries against which the FATF calls for such action, provided that the FATF website is periodically reviewed for that purpose, especially after each FATF plenary meeting.
      • Setting and keeping up-to-date a centralized data repository for the information collected on money laundering and terrorist financing operations, which includes, at least, the names circulated by the SIC, and those reported to the SIC by the concerned institution.

8. To take appropriate steps to identify, assess and understand their ML/TF risks, and to apply, based on risk understanding, a risk-based approach to classify
customers and operations according to the level of risk (low, medium, and high risk).

For indicative purposes only, customer risk, country risk, and service risk are taken into account when classifying the risks of customers and operations:

a) Customer Risk:
   • Customers whose occupation relies mainly on cash.
   • Politically Exposed Persons (PEPs).
   • Offshore companies.
   • Companies located in countries known to be tax havens.
   • Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
   • Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.

b) Country Risk:
   • The stringency of AML/CFT laws, and the efficiency of supervisory and judiciary authorities in charge of their implementation.
   • The existence of banking secrecy.
   • The situation of the country in terms of corruption and organized crime.
   • Conflict zones.

c) Service Risk:
   • Hawala business.
   • Currency shipment.

9. To put in place risk-based control measures and procedures, and at least to adopt for customers and beneficial owners, for PEPs as per FATF definition and their family members and close associates, and for operations classified as “high risk” according to risk scoring, the enhanced measures and procedures below for the purpose of risk management and mitigation:
   • To increase and prioritize control, and to conduct enhanced ongoing monitoring of the business relationship.
   • To obtain more detailed information on customers and beneficial owners (Increased KYC Levels), in particular to determine the source of their wealth.
   • To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers, and for executing operations, in a way that is commensurate to the specified level of risk.
   • To review periodically the relationship with customers.
   • To make continuous peer comparisons.
   • To set up an adequate system so as to determine whether the customer or beneficial owner is a PEP.

10. To take into account the duration and soundness of the business relationship with the customer.

11. To use software programs in order to conduct the controls needed as per the adopted scoring.

12. To have the Senior Management adopt a special policy as well as controls and measures that are based on the requirements specified in this Article, in order to classify and mitigate risks.

13. To document risk assessment results when necessary, and to keep them for provision to the competent authorities when needed.

14. To verify, when relying on a third party, that the latter is regulated and supervised, and meets the FATF due diligence and record-keeping requirements; to ensure also that the information needed to identify the customer and the beneficial owner and to understand the nature of the business, as well as copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party immediately and without delay. In all cases, the ultimate responsibility for CDD measures remains with the party relying on the third party, whether the third party is located inside or outside Lebanon, taking into consideration, upon such reliance, risk mitigation measures, in particular for risks associated with countries that do not or insufficiently apply the FATF Recommendations.

15. To identify and assess the ML/TF risks that might arise in relation to the development of new products and new business practices, including new service delivery mechanisms, and in relation to the use of new or developing technologies for both new and pre-existing products. A risk assessment should also take place prior to the launch or use of these products or business practices or technologies, and appropriate measures taken to manage and mitigate those risks.

16. To promptly notify the Governor of Banque du Liban in his capacity as Chairman of the Special Investigation Commission, whenever they suspect or believe, based on reasonable or objective grounds, that the executed or attempted operation is related to money laundering or associated predicate offences, or to terrorist
financing, terrorist acts, or terrorist organizations, regardless of the amount involved. Additionally, if money laundering or terrorist financing is suspected, and if they reasonably believe that performing the CDD measures will tip off the customer, it is then permitted not to pursue the CDD process and the SIC should be notified without delay.

17. To request their staff, subject to liability, not to inform customers when the SIC investigates or scrutinizes their operations, until the SIC issues a decision to this effect.

18. To ensure that their branches and majority-owned subsidiaries operating abroad apply the AML/CFT measures in force in Lebanon when the minimum requirements of the host country are less strict compared to Lebanon, to the extent permitted by the laws and regulations of the host country. If the host country does not permit the proper implementation of AML/CFT measures that are consistent with those applied in Lebanon, then the financial group should apply appropriate additional measures to manage ML/TF risks, and inform the SIC thereof.

19. To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) in relation to the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorist financing; and once the designation decision is issued, to immediately freeze without delay the funds, accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly...) by these names; and to provide the SIC, within 48 hours at most, with evidence on this action, and with the information available in this respect. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

20. To notify the SIC in case of similarity between the name of a customer and any designated name and details included in the national list mentioned in Subparagraph 19 above.

21. To apply FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freeze without delay the funds and/or accounts, and/or operations, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; to provide the SIC, within 48 hours at most, with evidence on this action and with the information available in this respect; and in case of similarity to notify the SIC and assess the associated risks. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

22. To consider for indicative purposes only, that the indicators listed below, if not justified, point out to the possible existence of ML/TF offences, particularly for Hawala operations:
   - Recurrent exchange operations unjustified by the nature of the customer’s activity.
   - Frequent exchange of small-denomination bills for large-denomination bills.
   - Recurrent attempt to exchange counterfeit banknotes.
   - Executing and/or requesting to execute recurrent transfers that are inconsistent with the customer’s financial situation.
   - Executing and/or requesting to execute a large number of transfers to the order of third parties for no apparent reason.
   - The value of incoming transfers is inconsistent with the customer’s business.
   - Transfers in which fictitious names or third parties are used.
   - Moving to a location far from the home or work address in order to execute the transfer.
   - Inaccurate information held by the customer about the transfer beneficiary.
   - Offering a bribe.
   - Customer’s readiness to pay unusual expenses to have the transfer executed.
   - Customer makes unjustified inquiries, particularly on the controls in place.
   - Customer has no knowledge of the amount to be transferred.
   - Engineering the transfers in a way to keep them below the reporting threshold.
   - Sudden change in the customer’s accustomed volume and number of transfers.
   - Cancelling the operation as soon as additional documents or information are requested from the customer.
   - Increase in the volume of operations during drug export seasons.

23. To provide the SIC, by the end of the month of April following the previous fiscal year, with a copy of the annual report prepared by the external auditor, on verifying the AML/CFT measures implemented at the concerned institution, and assessing their efficiency.

24. To apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by the institution itself. Examples of these measures include the following:
   - To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers.
To increase and prioritize control.
To not establish branches or subsidiaries or representation offices for the institution in these countries.
To not rely on third parties located in these countries.

25. To ensure that customer due diligence information and transaction records are swiftly provided to the SIC upon request, within three business days at most.

26. Financial groups must implement programs against money laundering and terrorist financing across the group including at all branches and majority-owned subsidiaries of that group. These programs should include the following measures:
• The appointment of a Compliance officer at the group management level.
• Policies and procedures for sharing information on customer due diligence and ML/TF risk management.
• The provision of customer, account, and operation information from branches and majority-owned subsidiaries to the compliance officer at the group level when necessary for AML/CFT purposes including information, analytical reports, and reports on activities that appear unusual. Similarly, branches and subsidiaries should receive such information from the Compliance officer at the group-level, as relevant and appropriate to risk management, analysis of information, reports, and unusual operations.
• Putting in place adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent informing or tipping off the customer.

Article 16
Upon the identification of the beneficial owner:

1. With respect to the customer that is a legal person, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:
   a) Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.
   b) In case of doubt as to whether the natural person(s) identified pursuant to Subparagraph (a) above is (are) the beneficial owner(s), or when no natural person holds 20% or more of the customer’s capital, it is required to identify the natural persons who exercise control over the legal person through other means (e.g. holding a majority of voting rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities…).
   c) When no natural person is identified pursuant to Subparagraphs (a) and (b) above, reasonable measures must be taken in order to identify and verify the identity of the persons holding senior management positions.

2. With respect to customers that are legal arrangements, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:
   a) For trusts, each of the persons below must be identified:
      • The Settlor.
      • The Trustee.
      • The Protector.
      • The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.
      • Any other natural person who exercises an effective control over the trust through direct or indirect ownership or through other means.
   b) For other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Subparagraph (2-a) must be identified.

3. Upon the identification of the beneficial owner, it is required to conduct the same due diligence measures applicable to customers, including those issued by the Special Investigation Commission (SIC).

Article 17
Institutions are required to promptly notify Banque du Liban of any amendment or change in the information mentioned in the detailed list of exchange institutions posted on BDL website.

Beirut, September 27, 2001
The Governor of the Banque du Liban
Riad Toufic Salamé
**BDL Basic Circular No. 63**

**Addressed to Banks and Companies authorized to Issue Credit and Debit Cards**

(Provisions of Article 2 bis were added as per BDL Intermediate Circulars No. 415 dated March 24, 2016 and No. 418 dated April 22, 2016 and Provisions of Article 5 bis were added as per BDL Intermediate Circular No. 498 dated June 13, 2018)

**Article 2 bis**

Banks and institutions that issue credit and debit cards are prohibited from issuing or promoting prepaid cards.

Under this Article, the cards listed below shall not be considered as prepaid cards which issuance is prohibited:

- Cards linked to a bank account and issued in the name of a specific person (such as cards linked to a customer’s account and issued in the latter’s name or in the name of one of his/her family members, as well as cards issued upon an employer’s request to pay employees’ wages or allowances, whether the employer is a natural person or legal entity).
- Cards issued upon the request of legitimate international organizations and allocated to local humanitarian and social aid, contingent upon BDL approval.

**Article 5 bis**

Institutions that issue credit and debit cards shall comply with the applicable laws and with BDL regulations, particularly AML/CFT laws and regulations, including with respect to the definition and identification of the Beneficial Owner.

**Beirut, June 10, 1999**

*The Governor of the Banque du Liban*

*Riad Toufic Salamé*

---

**BDL Basic Circular No. 69**

**Addressed to Banks, Financial Institutions and Institutions performing Electronic Banking and Financial Operations**

(These regulations were amended by BDL Intermediate Circular No. 630 dated 19/07/2022 and BDL Intermediate Circular No. 625 dated 27/05/2022)

**Article 5**

All non-banking institutions which perform domestic electronic transfers of cash in Lebanon shall:

8. Comply with applicable laws and with BDL regulations, particularly AML/CFT laws and regulations, including the definition and identification of the Beneficial Owner.

15. Ensure, upon hiring and periodically, the high qualifications, skills, and ethics of their own employees or those of the points of electronic transfers operating at their branches or through sub-agents or through any institution with whom a contract is made.

21. Post on their website a list with the points of electronic transfers and any modification thereto upon its occurrence. This list must include at least the following information: the head office name and address (Caza, locality, street), the name of the head office’s officer, the phone number…

**Article 9**

Institutions performing electronic funds transfers must accurately insert in the transfer order and attached messages, the full identity of the ordering party (name and address), the account number or reference number in the absence of an account number, the sources of the funds, their destination and purpose, in addition to the identity of the beneficiary and the economic right owner, as the case may be.

These institutions shall provide the competent authorities with all the above information within three working days from their request date.

**Article 9 bis**

**FIRST:**

The following expressions shall mean:

- “Customer”: Any natural or legal person, whether a company or an institution of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (mutual funds, cooperatives, welfare centers, charities, clubs, etc.).
- “Beneficial Owner”: Any natural person who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the customer and/or the natural person on whose behalf operations are carried out. Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

**SECOND:**

Any of the institutions specified in Paragraphs 3 and 4 of Article 2 of this Decision, and performing electronic transfers of cash, must comply at least with the following:

1. To apply to customers and beneficial owners, regardless of the value of the operation, due diligence measures which include verifying the identity of their permanent and occasional customers, whether resident or non-resident, determining the nature of their business, understanding the ownership structure and/or control
To maintain all the records obtained through CDD measures toward the customer and the beneficial owner, in particular the full name, occupation, and residential address, the address of the registered office for the legal entity, or, if different, the principal place of business, and the financial situation, as well as the account files for at least five years after the account is closed or the business relationship is ended, and all records on operations, including business correspondence and the results of any analysis undertaken, for at least five years after the date of the operation. Such records must be sufficient to permit reconstruction of individual operations, so as to provide, if necessary, evidence for legal action and prosecution of criminal activity.

2. To apply due diligence measures to existing customers on the basis of materiality and risk, and also to conduct due diligence on such existing business relationships in a timely manner, taking into account whether and when these measures have previously been undertaken, and the adequacy of data obtained.

3. To request the official documents or data below, for the purpose of verifying the identity of the customer and of the beneficial owner:
   a) For a natural person: a passport, ID card, extract of Civil Status, or residence permit.
   b) For a legal person, whether a company or an institution or a legal arrangement, a duly authenticated copy of the bylaws, the registration certificate, the ownership structure, the list showing the distribution of equities or shares (directly or indirectly), the list of authorized signatories, in addition to a copy of identity for the legal representative, the managers, and the natural persons who own, directly or indirectly, a controlling interest in the company’s management.

4. When the due diligence measures required toward customers and beneficial owners cannot be satisfactorily conducted, nor all the requested information obtained and kept, particularly those specified in this Article 9 (bis), then no relationship should be started or operation performed, or the existing business relationship should be terminated; and notifying the SIC should be considered.

5. To keep special records for each operation above the amount of USD 10,000 or its equivalent.

6. To request from the customer or the person acting on the latter’s behalf, the original power of attorney or a certified copy thereof, or a document proving that this person is authorized to act as such, in addition to the identity documents of the customer, the proxy, and the person acting on the customer’s behalf, and to verify these documents. The due diligence measures specified in Paragraph “Second”-1, must also be applied to the non-professional proxy.

7. To maintain all the records obtained through CDD measures toward the customer and the beneficial owner, comprising: the date of the operation, the purpose and nature of the business relationship, identifying the beneficial owner and the source of funds, obtaining data on that purpose when needed, and conducting ongoing monitoring of operations, particularly in the following cases:
   a) Before or when a business relationship is being established or started.
   b) When carrying out a single operation or several linked operations, whose total is equal to, or above USD 10,000 or its equivalent.
   c) Whenever a customer is suspected to attempt a money laundering or terrorist financing operation.

8. To promptly notify the Governor of Banque du Liban in his capacity as Chairman of the Special Investigation Commission, whenever they suspect or believe, based on reasonable or objective grounds, that the executed or attempted operation is related to money laundering or associated predicate offences, or to terrorist financing, terrorist acts, or terrorist organizations, regardless of the amount involved. Additionally, if money laundering or terrorist financing is suspected, and if they reasonably believe that performing the CDD measures will tip off the customer, it is then permitted not to pursue the CDD process and the SIC should be notified without delay.

9. To put in place and adopt an efficient AML/CFT internal control system that includes, at least, the following:
   a) Efficient and effective AML/CFT guidelines, approved and adopted by the Senior Management, and including, as a minimum, the due diligence measures required for customers with recurrent operations above a designated threshold.
   b) The appointment of a Compliance Officer at the management level, who has sufficient AML/CFT expertise, constantly attends training sessions in this respect, and whose mission consists in:
      • Training employees and sub-agents periodically on AML/CFT programs and methods.
      • Using software programs in order to monitor operations.
      • Preparing periodic reports on a risk-based supervision of operations, and the extent of compliance with required measures. These reports should cover as well sub-agents’ compliance with measures and regulations.
      • Involving sub-agents in AML/CFT programs.
      • Ensuring that information collected under the CDD process is kept up-to-date.
      • Conducting enhanced due diligence measures that are commensurate to the level of risk, on business relationships and operations performed with natural and legal persons (including financial institutions) from countries against which the
FATF calls for such action, provided that the FATF website is periodically reviewed for that purpose, especially after each FATF plenary meeting.

- Setting and keeping up-to-date a centralized data repository for the information collected on money laundering and terrorist financing, which includes, at least, the names circulated by the SIC, and those reported to the SIC by the concerned institution.
- To scrutinize transactions undertaken throughout the course of the relationship with customers so as to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customers, their business and risk profile, including, where necessary, the source of funds.
- To ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher-risk categories of customers.

10. To take appropriate steps to identify, assess and understand its ML/TF risks, and to apply, based on risk understanding, a risk-based approach to classify customers and operations according to the level of risk (low, medium, and high risk).

For indicative purposes only, customer risk, country risk, and service risk are taken into account when classifying the risks of customers and operations:

a) Customer Risk:
- Customers whose occupation relies mainly on cash.
- Politically Exposed Persons (PEPs).
- Offshore companies.
- Companies located in countries known to be tax havens.
- Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
- Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.

b) Country Risk:
- The stringency of AML/CFT laws, and the efficiency of supervisory and judiciary authorities in charge of their implementation.
- The existence of banking secrecy.
- The situation of the country in terms of corruption and organized crime.
- Conflict zones.

c) Service Risk:
- Cross-border transfers.

11. To put in place risk-based control measures and procedures, and at least to adopt for customers and beneficial owners, for PEPs as per FATF definition and their family members and close associates, and for operations classified as “high risk” according to risk scoring, the enhanced measures and procedures below for the purpose of risk management and mitigation:

- To increase and prioritize control, and to conduct enhanced ongoing monitoring of the business relationship.
- To obtain more detailed information on customers and beneficial owners (Increased KYC Levels), in particular to determine the source of their wealth.
- To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers, and for executing operations, in a way that is commensurate to the specified level of risk.
- To review periodically the relationship with customers.
- To make continuous peer comparisons.
- To set up an adequate system so as to determine whether the customer or beneficial owner is a PEP.
- To take into account the duration and soundness of the business relationship with the customer.
- To use software programs in order to conduct the controls needed as per the adopted scoring.
- To have the Senior Management adopt a special policy as well as controls and measures that are based on the requirements specified in this Article, in order to classify and mitigate risks.
- To document risk assessment results when necessary, and to keep them for provision to the competent authorities when needed.
- To ensure that customer due diligence information and transaction records are swiftly provided to the SIC upon request, within three business days at most.

12. To verify, when relying on a third party, that the latter is regulated and supervised, and meets the FATF due diligence and record-keeping criteria; to ensure also

1 Politically Exposed Persons (PEPs) are foreign or domestic individuals who are or have been entrusted with prominent public functions by a foreign country or domestically, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, as well as members of senior management, i.e. directors, deputy directors and members of the Board or equivalent functions in any international organization”. This definition of PEPs is not intended to cover middle ranking or more junior individuals in the aforementioned categories.
that the information needed to identify the customer and the beneficial owner and to understand the nature of the business, as well as copies of identification data and other relevant documentation relating to the CDD requirements, will be made available from the third party immediately and without delay.

In all cases, the ultimate responsibility for CDD measures remains with the party relying on the third party, whether the third party is located inside or outside Lebanon, taking into consideration, upon such reliance, risk mitigation measures, in particular for risks associated with countries that do not or insufficiently apply the FATF Recommendations.

13. To identify and assess the ML/TF risks that might arise in relation to the development of new products and new business practices, including new service delivery mechanisms, and in relation to the use of new or developing technologies for both new and pre-existing products. A risk assessment should also take place prior to the launch or use of these products or business practices or technologies, and appropriate measures taken to manage and mitigate those risks.

14. To request its staff, subject to liability, to abide by absolute secrecy and not to inform or permit to inform customers or any other party that the institution has notified or will notify the SIC, in case it suspects or believes the existence of a money laundering or terrorist financing operation, or when the SIC investigates or scrutinizes their operations or accounts, until the SIC issues a decision to lift banking secrecy of these accounts and to notify the concerned parties.

15. To ensure that its branches and majority-owned subsidiaries operating abroad apply the AML/CFT measures in force in Lebanon when the minimum requirements of the host country are less strict compared to Lebanon, to the extent permitted by the laws and regulations of the host country. If the host country does not permit the proper implementation of AML/CFT measures that are consistent with those applied in Lebanon, then the financial group should apply appropriate additional measures to manage ML/TF risks, and inform the SIC thereof.

16. Financial groups must implement programs against money laundering and terrorist financing across the group including at all branches and majority-owned subsidiaries of that group. These programs should include the following measures:

- The appointment of a Compliance officer at the group management level.
- Policies and procedures for sharing information on customer due diligence and ML/TF risk management.
- The provision of customer, account, and operation information from branches and majority-owned subsidiaries to the compliance officer at the group level when necessary for AML/CFT purposes including information, analytical reports, and reports on activities that appear unusual. Similarly, branches and subsidiaries should receive such information from the Compliance officer at the group level, as relevant and appropriate to risk management, analysis of information, reports, and unusual operations.

- Putting in place adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent informing or tipping off the customer.

17. If the originating institution of a transfer from Lebanon is at the same time the recipient institution in another country, it is required to collect all information on both the transfer ordering customer and the beneficiary so as to determine whether or not to notify the SIC, and if the institution decides to notify the latter, all the relevant information must be submitted with the notification.

18. To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) in relation to the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorist financing; and once the designation decision is issued, to immediately freeze without delay the funds, accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly...) by these names; and to provide the SIC, within 48 hours at most, with evidence on this action, and with the information available in this respect. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

The SIC should be notified in case of similarity between the name of a customer and any designated name and details included in the national list mentioned in this Subparagraph 18.

19. To apply FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freeze without delay the funds and/or accounts, and/or operations, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; to provide the SIC, within 48 hours at most, with evidence on this action and with the information available in this respect; and in case of similarity to notify the SIC and assess the associated risks. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.

20. To consider for indicative purposes only, that the indicators listed below, if not justified, point out to the possible existence of ML/TF offences:
a) Indicators related to the customer:
- Moving to a location far from the home or work address in order to execute the transfer.
- Inaccurate information held by the customer about the transfer beneficiary.
- Offering a bribe.
- Transfers in which fictitious names or third parties are used.
- Customer’s readiness to pay unusual expenses to have the transfer executed.
- Executing and/or requesting to execute recurrent transfers that are inconsistent with the customer’s financial situation.
- Executing and/or requesting to execute a large number of transfers to the order of third parties for no apparent reason.
- Customer makes unjustified inquiries, particularly on the controls in place.
- Customer has no knowledge of the amount to be transferred.
- The value of incoming transfers is inconsistent with the customer’s business.

b) Indicators related to operations:
- Splitting transfers in a way to keep them below the reporting threshold.
- Executing multiple transfers for a single beneficiary through several customers.
- A sudden change in the customer’s accustomed volume and number of transfers.
- The same address is used by several customers.
- Cancelling the operation as soon as additional documents or information are requested from the customer.

c) Indicators related to sub-agents:
- Presence of the sub-agent in high-risk geographical areas.
- Unjustified change in the sub-agent’s volume of operations.
- The volume of incoming transfers does not correspond to that of outgoing transfers.
- Increase in the sub-agent’s volume of operations during drug export seasons.

21. To apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by the institution itself. Examples of these measures include the following:
- To obtain the approval of the Senior Management for entering into, or continuing, a business relationship with customers.
- To increase and prioritize control.
- To not establish branches or subsidiaries or representation offices for the institution in these countries.
- To not rely on third parties located in these countries.

22. Upon the identification of the beneficial owner:

1. With respect to the customer that is a legal person, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:
   a) Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.
   b) In case of doubt as to whether the natural person(s) identified pursuant to Subparagraph (a) above is (are) the beneficial owner(s), or when no natural person holds 20% or more of the customer’s capital, it is required to identify the natural persons who exercise control over the legal person through other means (e.g. holding a majority of voting rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities...).
   c) When no natural person is identified pursuant to Subparagraphs (a) and (b) above, reasonable measures must be taken in order to identify and verify the identity of the persons holding senior management positions.

2. With respect to customers that are legal arrangements, the beneficial owners shall be identified and reasonable measures taken to identify them in the following manner:
   a) For trusts, each of the persons below must be identified:
      • The Settlor.
      • The Trustee.
      • The Protector.
      • The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.
      • Any other natural person who exercises an effective control over the trust through direct or indirect ownership or through other means.

      The definitions included in the glossary of the FATF 40 Recommendations shall be adopted to identify the persons mentioned in this Subparagraph (a).
   b) For other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Subparagraph (a) above, must be identified.
3. Upon the identification of the beneficial owner, it is required to conduct the same due diligence measures applicable to customers, including those issued by the Special Investigation Commission (SIC).

Article 19 bis

FIRST:
Institutions performing (domestic or international) electronic transfers must accurately include in the transfer order and accompanying messages, during all the phases of the operation, and regardless of the value of the transfer, the full identity and address of the originator, with a special reference number, as well as the identity of the beneficiary with a special reference number.

When several international electronic transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file must include the required and accurate originator information, and full beneficiary information, in a way to be fully traceable within the recipient country. The institution is also required to include a unique transaction reference number and shall refrain from performing electronic transfers if it fails to implement all the requirements specified in this Paragraph First.

SECOND:
Recipient institutions performing electronic transfers must take reasonable measures in order to identify cross-border transfers that lack the information required on the originator or beneficiary. Such measures may include post-event monitoring or real-time monitoring where feasible.

The recipient institution must have in place risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information, as well as appropriate follow-up action, and must also verify the beneficiary’s identity if it has not been previously verified.

THIRD:
Intermediary institutions performing electronic transfers are required to:
- Ensure that all originator and beneficiary information are attached to the electronic transfer.
- Take reasonable measures to identify electronic transfers that lack required originator or beneficiary information. Such measures should be consistent with straight-through processing.
- Have in place effective risk-based policies and procedures for determining when to execute, reject, or suspend an electronic transfer lacking required originator or beneficiary information, as well as the appropriate follow-up action.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border electronic transfer from remaining with a related domestic electronic transfer, the intermediary institution is required to keep, for at least five years, all the information received by the originating institution or by other intermediary institutions.

Beirut, March 30, 2000
The Governor of the Banque du Liban
Riad Toufic Salamé
not adjusted during that time limit. Otherwise, they shall deposit, in a non-interest-bearing blocked account at Banque du Liban, a special reserve that is equal to the amount of the loan and in the same currency as the loan, until the loan situation is adjusted.

Beirut, February 21, 2001
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No.89

Addressed to Banks and Exchange Institutions
Cross-border transportation of cash and precious metals
(These Provisions were added as per BDL Intermediate Circular No.263 dated May 21, 2011)

Article 1
Exchange institutions that undertake cross-border transportation of cash and/or metal coins and bullion (hereafter “precious metals”) from and to Lebanon must comply with the following conditions simultaneously:

1. They must belong to Category A and the capital they allocate to the head office and branches must not be less than five billion Lebanese pounds.
2. They must appoint an external auditor selected among internationally renowned audit firms.
3. They must separate the accounting entries relating to cross-border transportation of cash and/or precious metals from the accounting entries of their other operations.
4. They must comply with the provisions of the Law on Fighting Money Laundering and with all other relevant regulations issued by Banque du Liban and the Special Investigation Commission (SIC), particularly the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing (AML/CFT), where applicable.
5. They must appoint a Compliance Officer or a Compliance Unit in order to control the institution’s compliance with the laws in force and the regulations and recommendations issued by Banque du Liban, the Banking Control Commission and the SIC, particularly the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, where applicable.
6. The Compliance Officer or the Head of the Compliance Unit must attend, on a continuous basis, AML/CFT training sessions or obtain specialized AML/CFT certificates such as the CAMS-Certified Anti-Money Laundering Specialist-specified in Basic Decision No.9286 of March 9, 2006 attached to Basic Circular No.103.
7. They must appoint an Internal Audit Officer to perform internal audit on their operations.
   The concerned institutions are granted a time limit ending on December 31, 2011 to comply with the provisions of paragraphs 2, 3, 5 and 7 of this Article, and another time limit ending on March 31, 2012 to comply with the provisions of paragraph 1 thereof.

Article 2
Banks and exchange institutions that undertake cross-border transportation of cash and/or precious metals from and to Lebanon must provide the Banking Control Commission and the BDL Money Services Business Department, at the end of each month and for each currency and each metal, with the following:

a) a monthly position prepared according to Form No.1 exhibiting clearly the total volume of cross-border transport operations of cash and/or precious metals, from and to Lebanon.
b) a monthly position prepared according to Form No.2 exhibiting clearly the number of cross-border transport operations of cash and/or precious metals from and to Lebanon.
c) a monthly position prepared according to Form No.3 exhibiting the total transportation volume of cash and/or precious metals inside Lebanon, computed on the basis of operations performed among these institutions, and between these institutions and the banks and institutions regulated by Banque du Liban and not undertaking cross-border transportation of cash and/or precious metals.
d) a monthly position prepared according to Form No.4 exhibiting all transport operations inside Lebanon of cash and/or precious metals whose amount is equivalent to or in excess of US dollar 10,000.

Article 3
Banks that do not undertake cross-border transportation of cash and/or precious metals from and to Lebanon must provide the Banking Control Commission and the BDL Money Services Business Department with a monthly position prepared according to Form No.3, exhibiting the transportation volume of cash and/or precious metals inside Lebanon, computed on the basis of operations performed among these banks, and between these banks and the institutions regulated by Banque du Liban and not undertaking cross-border transportation of cash and/or precious metals.

Article 4
The monthly positions mentioned in Articles 2 and 3 above shall be sent on compact discs within ten days from the end of the reported month, whether or not cross-border transport operations of cash and/or precious metals from
and to Lebanon or transport operations of cash and/or precious metals inside Lebanon have taken place.

Article 5
This Decision shall come into force upon its issuance.

Article 6
This Decision shall be published in the Official Gazette.

Beirut, January 11, 2002
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No.111

Addressed to Banks, Financial Institutions, Financial Intermediation Institutions, Leasing Companies, Exchange Institutions, and the Public

Cash Transfers according to the Hawala System

(These regulations were amended by BDL Intermediate Circular No.337 dated September 20, 2013)

Article 1
For the purposes of implementing the provisions of this Decision, the term “Hawala” shall mean informal systems for money transferring, which are outside the conventional financial sector and are used by institutions and individuals, including Hawala brokers and intermediaries (Hawala Dar).

Article 2
Exchange institutions of Category A shall be the only institutions entitled to perform Hawala cash transfers, whether for their own account or on behalf of a third party. Therefore, while performing Hawala transactions, these institutions are prohibited from carrying out any of the banking transactions specified in the Code of Money and Credit, particularly from receiving deposits. Furthermore, pursuant to Law No. 347 of August 6, 2001 on Regulating the Money Changer Profession in Lebanon, these institutions are also prohibited from performing transactions that do not fall within the scope of the exchange business, such as commercial financing, lending, and the management of funds, among others.

Article 3
Any exchange institution of Category “A” wishing to carry out “Hawala” cash transfers must:
1. Send to Banque du Liban a prior written notification.
2. Retain, for a minimum five-year period, Hawala records that include, at least, the information mentioned in the Form attached to this Decision, in addition to photocopies of official documents pertaining to concerned clients.

Article 4
The value of an incoming or outgoing Hawala transaction must not exceed USD 20,000 or its equivalent in any other currency, provided the total amount of Hawala transactions in a single year does not exceed, at any time, tenfold the capital of the exchange institution.

Article 5
Any exchange institution that performs Hawala transactions must take all the procedures and measures needed to implement the obligations imposed by the applicable legal provisions, particularly the AML Law and all other regulations issued by Banque du Liban, the Banking Control Commission and the SIC (Special Investigation Commission). It must specifically comply with the requirements of Basic Decision No.11323 of January 12, 2013 relating to the Establishment of a Compliance Department, and adopt risk-based procedures and measures when checking the details of each incoming or outgoing Hawala transaction.

Article 6
When receiving from their correspondents cash transfer orders pursuant to the Hawala system, exchange institutions are prohibited from paying the amount of these transfers through a swap operation, by checks or bank transfers to the account of the Hawala’s beneficiary. These institutions must open a sub-account allocated to clearing transactions performed with correspondents abroad as a result of Hawala transactions.

Article 7
Institutions whose status is inconsistent with Article 5 of this Decision are granted a time limit ending on March 31, 2014 to comply with its provisions and regularize their situation accordingly.

Article 8
This Decision shall come into effect upon its issuance.

Article 9
This Decision shall be published in the Official Gazette.

Beirut, September 24, 2007
The Governor of the Banque du Liban
Riad Toufic Salamé
**BDL Basic Circular No.126**

**Addressed to Banks and Financial Institutions**

The Relationship between Banks and Financial Institutions and their Correspondents

**Article 1**

Banks and financial institutions operating in Lebanon must:

1. Implement strictly the Regulations for the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, particularly with customers who request the conduct of cross-border operations by way of correspondent banks and financial institutions, by:
   a) Adopting a risk-based approach and vetting the identity of both the customers and the economic right owner and obtaining the requisite information and setting procedures for monitoring their operations and accounts on an ongoing basis.
   b) Updating their database for money laundering and terrorism financing operations, in conformity with the provisions of this Decision.
   c) Notifying the Special Investigation Commission of any operation suspected of contravening the obligations set out in this Decision.

2. Be fully informed of the laws and regulations governing their correspondents abroad, and 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.

Within this scope, banks and financial institutions must adopt the utmost accuracy and due diligence to vet the identity of the economic right owner in the operations conducted.

The provisions of this Article shall govern any dealings between banks and financial institutions operating in Lebanon, and their branches, subsidiaries or sister companies abroad.

3. Control the transactions on payable-through accounts and strictly implement the enhanced due diligence measures on concerned customers.

**Article 2**

External auditors must check banks and financial institutions’ compliance with the provisions of this Decision. They must also insert in their report on the procedures adopted to control financial and banking operations for fighting money laundering and terrorism financing, detailed information about their inspection of the adopted procedures, the results of their audit, and their remarks in this regard.

**Article 3**

Any party violating the provisions of this Decision shall incur the administrative sanctions stipulated in the applicable laws and regulations, particularly the sanctions stipulated in Article 208 of the Code of Money and Credit.

**Article 4**

This Decision shall come into force upon its issuance.

**Article 5**

This Decision shall be published in the Official Gazette.

*Beirut, April 5, 2012*

*The Governor of the Banque du Liban*

*Riad Toufic Salame*

---

**BDL Basic Circular No.136**

**Addressed to Banks and Financial Institutions and all other institutions licensed or supervised by Banque du Liban**

(The provision of article 1 was amended by BDL Intermediate Circular No. 625 dated 27/05/2022)

**Article 1**

Banks, Financial Institutions and all other institutions licensed or supervised by Banque du Liban, are requested, as far as each is concerned:

1. To review constantly, on the UN Security Council website, any update in relation to the names designated on the
lists issued pursuant to UN Security Council Resolution 1267/1999, Resolution 1988/2011, and Resolution 1989/2011, and the relevant successor resolutions, and/or the lists issued by the relevant Sanctions Committees, and to freeze automatically, without delay and without prior notice, within a matter of hours from the issuance of the designation decision, the funds or accounts or operations or other assets, if any, owned in any form (directly or indirectly, jointly…) by these names, and to provide the SIC, within 48 hours at most, with evidence on this action, and with the information available in this respect.

The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds or other assets that are owned or controlled by designated persons or entities.

2. To report to the Special Investigation Commission in case of similarity between the name of a customer and any designated name and details included in the lists issued pursuant to the UN Security Council Resolutions referred to in Paragraph 1 above and/or issued by the Special Sanctions Committees.

Article 2
The provisions of this Circular shall be applicable to branches, sister institutions and subsidiaries abroad.

Article 3
Any party violating the provisions of this Circular shall incur the sanctions stipulated in Article 13 of Law No. 44 of November 24, 2015, particularly for non-compliance with the immediate freezing obligation referred to in Article 1, paragraph 1 above.

Article 4
This Decision shall enter into force upon its issuance.

Article 5
This Decision shall be published in the Official Gazette.

Beirut, December 22, 2015
The Governor of the Banque du Liban
Riad Toufic Salamé
BDL Basic Circular No. 138

Addressed to Banks and Financial Institutions

Exchange of Tax Information covered by Banking Secrecy, in line with international standards

Article 1
As far as each is concerned, banks and financial institutions shall take at their own full responsibility the appropriate administrative and technical measures required to provide the Special Investigation Commission (SIC) with the information that the concerned foreign authorities request from the Lebanese Ministry of Finance regarding the accounts of residents in the requesting countries. Any such request of information shall take place within the tax information exchange framework, in compliance with the recommendations issued by the Global Forum on Transparency and Exchange of Information for Tax Purposes and by the OECD, and according to the regulatory mechanism to be set for that purpose by the SIC in coordination with Banque du Liban.

Article 2
This Decision shall come into force upon its issuance.

Article 3
This Decision shall be published in the Official Gazette.

Beirut, August 5, 2016
The Governor of the Banque du Liban
Riad Toufic Salamé

BDL Basic Circular No. 139

Addressed to Banks and Financial Institutions

Common Reporting Standard

(These regulations were amended by BDL Intermediate Circular No. 548 dated March 31, 2020)

Article 1: Definitions

FIRST:
For the purpose of implementing the provisions of Law No 55 of 27 October 2016 (Exchange of Information for Tax Purposes) and the provisions of this Decision, the following definitions shall be adopted:

1. **Law:** Law No. 55 of 27 October 2016.
2. **Decree:** The Decree relating to the detailed implementation of Subparagraph 3, Paragraph Sixth of Law No. 55 of 27 October 2016 (Exchange of Information for Tax Purposes),
3. **Standard:** The Common Reporting Standard for the automatic exchange of information and the related commentaries, which was approved by the OECD Council on 15 July 2014, and contains the reporting and due diligence procedures for the automatic exchange of information, including any subsequent amendment and explanation thereto published by the OECD.

4. **Participating jurisdiction:** any jurisdiction listed in Table 3 of the Decree.

5. **Financial Institution:**
   a) Any bank, financial institution, company, or organism regulated by Banque du Liban and performing activities that are similar to those of the financial institution as defined in Section VIII of the Standard.
   b) This definition excludes the branches located outside Lebanon of the financial institutions defined in Clause (a) above.
   c) The definition in Clause (a) includes the branches operating in Lebanon of financial institutions that are not resident in Lebanon, and which perform the activities of the Financial Institution as defined in Section VIII of the Standard.

6. **Reporting Financial Institution:** any Financial Institution that is not a Non-Reporting Financial Institution, as defined below.

7. **Non-reporting Financial Institution:**
   a) Any Financial Institution as defined in Section VIII, Subparagraphs [B1 (a), (b), (d) and (e)] of the Standard; or
   b) Any entity listed in Table 2 of the Decree.

8. **Financial account:** any account as defined in Section VIII of the Standard.

9. **Pre-existing account:** any financial account maintained by a Reporting Financial Institution on 30 June 2017.

10. **New account:** a Financial Account opened at a Reporting Financial Institution on or after 1 July 2017.

11. **High-value account:** a Pre-existing Account held by one or more natural persons/individuals, whose aggregate balance or value exceeds the amount of USD 1,000,000 on 30 June 2017 and 31 December 2017, or on 31 December of any subsequent year.

12. **Lower-value account:** a Pre-existing Account held by one or more natural persons/individuals, whose aggregate balance or value does not exceed the amount of USD 1,000,000 on 30 June 2017.

13. **Excluded account:**
   a) Any account as defined in Section VIII, Subparagraphs [C17 (a) to (f)] of the Standard; or
   b) Any account listed as an Excluded Account in Table 1 of the Decree.
For the purpose of implementing this Decision, the

2. For the purpose of determining the balance or value of
   an account opened at a Reporting Financial Institution,
   to convert the account's balance or value into the US
   dollar, at the official exchange rate set by Banque
du Liban, so as to identify the accounts subject to a
   threshold on 30 June 2017, 31 December 2017, or 31
   December of any subsequent year.

f) For the purpose of this Decision, to treat a Financial
   Account held by a person as partner in a partnership, and
   used by that person in that capacity, as an entity account.

g) Whenever a Reporting Financial Institution relies
   on information collected pursuant to AML/KYC
   procedures in order to identify the Controlling
   Person of the New Entity Account Holder (Section
   VI, Subparagraph [A2 (b)] of the Standard), these
   procedures must be consistent with the FATF-
   Financial Action Task Force Recommendations 10
   and 25 (as adopted in February 2012).

SECOND:
1. For the purpose of implementing Section I of the
   Standard, Reportable Jurisdiction shall mean any
   jurisdiction listed in Table 4 of the Decree.

2. For the purpose of implementing the due diligence
   procedures specified in Sections II through VII of the
   Standard and in this Decision, Reportable Jurisdiction
   shall mean any jurisdiction other than Lebanon and the
   United States of America.

3. For the purpose of implementing this Decision, the
date to be specified in the definition of “Qualified Credit
Card Issuer” in Section VIII, Subparagraph [B8] of the
Standard, shall be 1 July 2017 inclusively.

THIRD:
Any term or expression defined in the Standard but not in
Paragraph “Second” of the Law or in this Decision, shall
have the same meaning set forth in the Standard.

Article 2: Due Diligence Obligations
1. Reporting Financial Institutions shall comply with the
   following:
   a) To establish, keep, and document the due diligence
      procedures stipulated in Sections II through VII of
      the Standard, as well as the procedures stipulated in
      Articles 2 and 3 of this Decision.
   b) To identify reportable accounts by implementing the
due diligence procedures stipulated in Sections II
   through VII of the Standard, without prejudice to
   Paragraph 2 of this Article.
   c) To treat the financial account as a reportable
      account, as of the date it is identified as such, in
      accordance with the due diligence procedures
   stipulated in Sections II through VII of the Standard.
In case no other time-limit is set, the account-related
information shall be reported annually, as of the year
following the year to which the information relates.

d) For the purpose of this Decision, to treat an account
   with a negative balance or value as an account with
   a balance or value equal to nil.

e) For the purpose of determining the balance or value of
   an account opened at a Reporting Financial Institution,
   to convert the account's balance or value into the US
dollar, at the official exchange rate set by Banque
du Liban, so as to identify the accounts subject to a
threshold on 30 June 2017, 31 December 2017, or 31
December of any subsequent year.

f) For the purpose of this Decision, to treat a Financial
   Account held by a person as partner in a partnership, and
   used by that person in that capacity, as an entity account.

g) Whenever a Reporting Financial Institution relies
   on information collected pursuant to AML/KYC
   procedures in order to identify the Controlling
   Person of the New Entity Account Holder (Section
   VI, Subparagraph [A2 (b)] of the Standard), these
   procedures must be consistent with the FATF-
   Financial Action Task Force Recommendations 10
   and 25 (as adopted in February 2012).

2. Reporting Financial Institutions may adopt the following
   procedures:
   a) To apply the Residence Address Test to Lower Value
      Accounts held by natural persons/individuals, as defined
   b) To apply Section V, Paragraphs [A to C] of the
      Standard, to determine whether a Pre-existing Entity
      Account is subject to the due diligence procedures
      specified in Section V of the Standard.
   c) Regarding New Entity Accounts, to rely solely on a
      self-certification from the Account Holder or from
      the Controlling Person, so as to determine whether a
      Controlling Person of a Passive NFE is a Reportable
      Person, as defined in Section VIII of the Standard.

3. The due diligence procedures with respect to the
   Standard’s Sections and Paragraphs enumerated below,
   shall be implemented according to the following dates:
   a) Section III “Due diligence for Pre-existing Individual
      Accounts”:
      1. Subparagraph [C6]: 30 June 2017
      2. Paragraph D: 31 December 2017 for High Value
         Accounts; and 31 December 2018 for Lower
         Value Accounts.
   b) Section V “Due diligence for Pre-existing Entity
      Accounts”:
      1. Paragraph A: 30 June 2017
      2. Paragraph B: 30 June 2017 concerning both dates
3. Paragraph E:
   • Subparagraph [E1]: 30 June 2017 and 31 December 2018, respectively.
   • Subparagraph [E2]: 30 June 2017

c) Upon the implementation of the Standard, Section III-Subparagraph [C6], Section V-Paragraphs A and B and Subparagraph [E2], and Section VIII-Subparagraph [C15], and only for that purpose, the expressions “the last day of any subsequent year” and “31 December of any subsequent year” shall mean “31 December 2017 and 31 December of any subsequent year”.

4. Upon the identification of the Controlling Person, the definition of the Beneficial Owner, specified in the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorist Financing attached to Basic Decision No 7818 of 18 May 2001, shall be adopted, as well as its identification mechanism mentioned in the said Regulations.

Article 3: Reporting Obligation

1. The Reporting Financial Institution shall directly submit to the Ministry of Finance an Information Return that contains the information relating to the calendar year 2017 and to each subsequent calendar year, with respect to each financial account identified as a reportable account maintained by the Reporting Financial Institution at any time during the year. Banque du Liban shall remain the sole regulatory body in charge of the sound implementation of the Law, the Decree, and this Decision.

2. In case a Reporting Financial Institution applies, during a calendar year, the due diligence procedures set forth in Article 2 of this Decision, and if no account is identified as a reportable account maintained by the Reporting Financial Institution at any time during the year. Banque du Liban shall remain the sole regulatory body in charge of the sound implementation of the Law, the Decree, and this Decision.

3. The Reporting Financial Institution shall submit an electronic Information Return directly to the Ministry of Finance, no later than 30 June of the year following the reporting calendar year. This Information Return shall then be forwarded to the competent authority of the relevant jurisdiction specified in Table 4 of the Decree, no later than 30 September of the year following the reporting calendar year, provided the first information exchange takes place at the latest by 30 September 2018.

Article 4: Records

1. Each Reporting Financial Institution must retain the records it has received or has prepared pursuant to the provisions of this Decision, including any documentary evidence and self-certification submitted by the account-related person.

2. Under this Decision, each Reporting Financial Institution that retains electronic records must keep these records in an electronically readable format throughout the period specified in Paragraph 4 below.

3. Under this Decision, each Reporting Financial Institution that has obtained or has created records in a language other than Arabic, must provide, upon request and at its own expense, a translation of such records into Arabic.

4. Under this Decision, each Reporting Financial Institution must keep the records and documents relating to the entries received or created pursuant to this Decision, for a minimum period of 10 years:
   a) For the self-certification submitted by the account-related person: starting from the closing date of the concerned Financial Account.
   b) In all other cases: starting from the end of the last calendar year referred to in the record.

Article 5: Control and Review of Books and Records

In addition to their respective authority and for the purpose of controlling the proper implementation of this Decision, Banque du Liban and/or the Special Investigation Commission (SIC) may request the Reporting Financial Institution to provide, within a period of no less than 14 days, any information and copies of any books, records, or documents.

Article 6: Anti-avoidance

If a person enters in any arrangements or engages in practices that could be considered as being mainly or secondarily intended to avoid any obligations imposed by law or under this Decision, that person shall remain subject to the obligation he/she has attempted to avoid, as if he/she has neither entered in any such arrangements nor engaged in any such practices.

Article 7: Sanctions

Each Reporting Financial Institution that contravenes the provisions of this Decision or fails to comply with the obligations thereof, shall be subject to the fine stipulated in the applicable laws, without prejudice to the right of Banque du Liban and/or the SIC to impose administrative sanctions and financial penalties pursuant to the Code of Money and Credit and to Law No. 44 of 24 November 2015.

Article 8: Interpretation

The provisions of this Decision must be read and implemented in accordance with the Standard and its commentaries and with each amendment thereto.
**Article 9: Date of Enforcement**  
This Decision shall come into effect as of 1 July 2017.

**Article 10**  
This Decision shall be published in the Official Gazette.

Beirut, July 21, 2017  
The Governor of the Banque du Liban  
Riad Toufic Salamé

---

**BDL Basic Circular No.144**

**Addressed to Banks and to Financial Institutions**  
Cybercrime Prevention

**FIRST: CYBERCRIME PREVENTION POLICIES AND PROCEDURES**

**Article 1**  
Banks and financial institutions must set policies and adopt measures and procedures relating to cybercrime prevention, and comprising at least:

I. General policies prescribing the following actions:
   1. To analyze potential cybercrime risks, and to follow up the latest updates concerning cybersecurity technologies.
   2. To allocate the necessary funds and budget in order to set and implement cybersecurity policy, systems, and rules.
   3. To prepare insurance contracts that cover cybercrime risks.
   4. To set and continuously update the plans needed for cybercrime prevention (e.g. incident response planning, disaster recovery and business continuity plan, first responder training plan…).
   5. To create a task force for cybercrime prevention.
   6. To exchange information on cybercrime with the concerned parties inside or outside the bank/financial institution.
   7. To raise awareness among employees and customers regarding cybercrime prevention.
   8. To monitor changes in employees’ habits and behavior, particularly employees having elevated privileges to access IT systems.
   9. To be vigilant and cautious when selecting contractors for tasks related to IT systems, and to make sure that these contractors do not in turn outsource these tasks to less reliable parties.

II. Technical procedures encompassing the following actions:

1. To adopt a minimum two-factor authentication technique, particularly to check the right of outside users to access the system of the bank/financial institution.
2. To use an end-to-end, high-grade encryption for crucial data, to avoid loss and tampering of such data.
3. To adopt tight rules for filtering incoming e-mails and for controlling external access to mailboxes.
4. To update the systems of all computers, and to check the safety of the computers assigned for the external use of the bank/financial institution’s employees.
5. To carry on penetration tests to detect any possible vulnerabilities in the network.
6. To monitor the network traffic in order to detect any unusual behavior, whether through the quality or the number of sent batches.
7. To check and monitor data integrity, in order to detect any illegal tampering with data, and to trace back the source of the illegal access to such data.

**SECOND: FINANCIAL CYBERCRIME PREVENTION PROCEDURES**

**Article 2**  
As far as each is concerned, banks and financial institutions must adopt in general and on their own responsibility, the appropriate administrative, technical and judicial procedures which enable them to remain vigilant, to monitor and combat financial cybercrime. They must particularly:

1. Consider the guidelines specified in the Cybercrime Prevention Guide, Part 1, Section 1, as cybercrime indicators.
3. Set specific internal systems and procedures regarding the execution of funds transfer orders received electronically (through e-mail, e-banking, etc.)
4. To incorporate in the contract signed with the customer specific provisions that determine, apart from e-mail, other means of communication with the customer (such as phone calls), in order to validate transfer orders received electronically, provided any change in these means of communication takes place only through the contracting parties’ written agreement.
5. To inform the customer of the risks associated with transfer orders sent through e-mail, to advise him/her to use safer means, and to obtain his/her risk-bearing written consent.
6. To provide the customer with the “Guidelines for Individuals and all other Non-Financial Institutions and Entities” specified in the Cybercrime Prevention Guide, Part 2.
To request from customers to promptly report any cybercrime, whenever they become aware or detect or are notified that they have been, or were likely to be, victims of a cybercrime.

**Article 3**

Banks and financial institutions are requested, whenever they detect or become aware or are notified that they have been the victims, or that any of their customers has been the victim of a financial cybercrime, to take prompt and effective actions that include, at least, the remedial measures mentioned in the Cybercrime Prevention Guide, Part 1, Section 3, particularly:

1. To provide both the correspondent bank and the beneficiary bank/financial institution with all relevant information, and to request the cancelling and the refund of the funds transfer.

2. To communicate to the Special Investigation Commission (SIC) any relevant information and correspondence, including technical information about:
   - The customer’s IP address or the IP address used to send the suspicious funds transfer orders.
   - The name of the Internet Service Provider through which the suspicious funds transfer orders were sent.
   - The name of the Internet Service Provider used for the unauthorized access to the customer’s account, through electronic banking.

3. To advise the customer to file a report or a judicial complaint before the competent authorities.

**Article 4**

This Decision shall come into effect upon its issuance.

**Article 5**

This Decision shall be published in the Official Gazette.

Beirut, November 28, 2017
The Governor of the Banque du Liban
Riad Toufic Salamé

---

**BDL Basic Circular No. 163**

**Addressed to Banks**

**Monitoring civil servants’ accounts**

**Article 1**

For the purposes of implementing the provisions of this Decision, the definition of “civil servant” mentioned in Article 1 (1) of Law 189 of 16 October 2020 shall be adopted. The provisions of this Decision shall apply to the “civil servant”, and to the employees of each of the Ministry of Finance, Customs, Directorate of Land Registry and Cadastre, Traffic and Vehicles Management Authority, as well as to the Chairman, members, employees and staff of administrative committees and independent and regulatory bodies established by laws, all grades and categories included, if the latter are entrusted with financial duties. These provisions shall apply neither to employees of fourth-grade and below or the equivalent thereof, who are not assigned higher-level duties, nor to the teaching staff at the Lebanese University, public schools and institutes.

**Article 2**

Regardless of their ranking, according to the risk-based approach for the risk level of the customer who falls under the text and content of Article 1 above, banks are required to apply to salary domiciliation accounts, without prejudice to other measures adopted and implemented as per BDL decisions, particularly Basic Decision 7818 of 18 May 2001 notified by Basic Circular 83 to banks, if these accounts register an activity not deriving from the job (deposits or transfers from real estate or commercial investments or from sources other than job income), enhanced due diligence measures that include:

- Increasing control of accounts and operations, and conducting ongoing monitoring of the business relationship.
- Obtaining the approval of the Senior Management for a business relationship and for executing operations.

---

**BDL Basic Circular No. 147**

**The Opening of Bank Accounts**

**Addressed to Banks**

**Article 1**

Banks are required, when they open a bank account for a natural or a legal person residing in Lebanon in order to ensure the running of the latter’s commercial, professional, or service business and activities, to obtain from that person a copy of the registration certificate at the Ministry of Finance.

---

132 | Laws and Regulations
• Reviewing periodically the business relationship.
• Obtaining more detailed information on the customer and the beneficial owner.

A subaccount should also be opened to record operations that are not related to the job; this subaccount should be subject to enhanced due diligence measures and ongoing monitoring.

The KYC Form should include all the information specified in SIC Circular 13, as well as information on the civil servant’s work or job, in particular his/her employing institution, grade, salary, benefits, etc., in addition to all information on sources of income other than his/her job, on condition that the related data and evidencing documents are maintained and periodically updated.

**Article 3**

Upon the emergence of any corruption indicator, the generally acknowledged corruption indicators shall be taken as reference, including but not limited to those below:

- The wealth and source of funds are inconsistent with the date of employment, experience, or age.
- High-balance accounts are maintained, while no supporting documents are submitted for justification.
- Unjustified and unusual high-value cross-border transfers are performed, particularly to tax haven jurisdictions.
- Unusual high-value cash operations are performed, while no supporting documents are submitted for justification.
- Payments are received from companies, individuals, or non-governmental entities that have benefited or benefit from public contracts/procurements.
- Checks issued by public entities are cashed and their value deposited in private accounts.
- Multisource and matching negative reports relating to bad reputation, unethical or illegal behavior, are issued by media outlets.
- Convictions or formal ongoing or previous investigations related to corruption.
- Illegal payments are received or loans are repaid by a third party without justification.
- High-value international transfers are received from companies’ accounts and/or personal accounts without justification.
- Funds are received in bank accounts held by persons or legal entities known to be under the control of, or related to the civil servant, with no justification submitted.
- Representatives or proxies (e.g. lawyer, accountant, or a third party) perform banking operations on behalf of a civil servant with the intention of dodging due diligence procedures.

**Article 4**

The existence of one or more indicators does not mean in itself the existence of corruption acts, and if any, available information on the relevant operations, or customer’s data and account movement should be reviewed and assessed, and the required decision taken as to whether or not to file a Suspicious Transaction Report (STR) to the SIC, pursuant to the provisions of Law 44 of 24 November 2015. In case of any suspicion or doubt about an operation or accounts linked to corruption acts, the related STR must include at least:

a) Red flag indicators: by mentioning one or more of the above-mentioned indicators on the basis of which the report was filed.

b) Suspicious operations or accounts: by identifying the inconsistencies between the concerned operations and the KYC Form data, or those for which the employee refrained from giving the bank any additional clarifications.

**Article 5**

Enhanced due diligence measures shall also apply to any of the bank’s customers who are found to have important banking operations with, or in relation to the civil servant, in order to make sure that such operations are justified.

**Article 6**

The provisions of Article 13 of Law 44 of 24 November 2015 shall apply to banks violating the provisions of this Decision.

**Article 7**

This Decision shall come into force upon its issuance.

**Article 8**

This Decision shall be published in the Official Gazette.

*Beirut, May 27, 2022*

*Riad Toufic Salamé*

---

**Capital Markets Authority**

**Series 2000 & 3000**

**Addressed to Financial Intermediation Institutions**


**Article 2103**

Securities business activities

(Series 2000 dated January 19, 2017)

2. In order to carry out their activities, financial intermediation institutions have the right to undertake other operations that are complementary to their main objective. They are however prohibited from undertaking:
i) Exchange operations, except when such operations are complementary or related to those performed, within the limits of their objects, on behalf of their clients.

ii) Cross-border transportation of cash, metal coins, bullion and specie.

iii) Any commercial or industrial activity or any activity not related to financial intermediation.

**Article 3506**

Procedures to deal with the customer’s funds
(Series 3000 dated November 10, 2016)

1. An approved institution must receive funds from its customer through checks or Banker’s checks or electronic transfer only.

2. An approved institution may execute, at their customers’ request, outgoing or incoming transfers from abroad or from Lebanon in favour of third parties in Lebanon or abroad, provided the amount of each transfer doesn’t exceed USD /1,500/.

---

**Special Investigation Commission Circular 2**

Addressed to Banks and Other Institutions Bound to Report on Money Laundering Operations

Pursuant to the Decision taken by the Special Investigation Commission (SIC) in its meeting of 10/7/2001, pursuant to the provisions of Article 7, Paragraph 1, and Article 11 of Law 318 of 20/4/2001 on Fighting Money Laundering, and to the provisions of Article 6 of the Regulation on the Control of Financial and Banking Operations for Fighting Money Laundering, attached to BDL Decision 7818 of 18/5/2001, all banks and other institutions bound to report on money laundering operations, when reporting details of operations suspected or ascertained to be involving money laundering, must send information in a sealed envelope on which the expression “Strictly Confidential” is clearly indicated. The envelope should be addressed, as specified by law and regulations according to the case, to the Secretariat of the SIC Chairman/Governor of the Banque du Liban, or to the SIC Secretariat.

This Circular shall be published in the Official Gazette and shall be effective upon its publication.

Beirut, July 20, 2001
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
SIC Circular 13

Pursuant to the provisions of BDL Basic Decision No. 7818 of May 18, 2001 (Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing), particularly Articles 3 and 4 thereof, with reference to SIC Circular 4 of September 18, 2003 addressed to banks and financial institutions, and pursuant to the SIC Decision taken in its meeting of May 26, 2011, the informative statement attached to the above-mentioned Circular 4 is replaced with statements No. 1 and No. 2 attached to this Circular.

Beirut, May 27, 2011
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

SIC Circular 12

Pursuant to the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, attached to BDL Basic Decision No. 7818 of May 18, 2001, particularly Article 13 thereof, with reference to SIC Circular No. 5 of April 29, 2004 addressed to external auditors, and pursuant to the SIC decision taken in its meeting of May 26, 2011, the annex attached to the above-mentioned SIC Circular 5 is replaced with the annex attached to this Circular.

Beirut, May 27, 2011
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Attachment To SIC Circular 5

I. To verify whether or not banks/financial institutions comply with the following obligations:

1. Making sure, when establishing a relation with a foreign correspondent bank, that the latter is not a shell bank, that it really exists, based on submitted documentary evidence, that it does not deal with shell banks, has a good reputation, is subject to a good control and implements sufficient and effective procedures to fight money laundering and terrorism financing.

2. Adopting the KYC Form that must include, at least, basic information about customers, as required by amended SIC Circular No. 4; checking the identity of permanent customers, and taking all necessary steps to verify the information provided by the customers.

SIC Circular 5 amended by Circular 12

Addressed to External Auditors
and transient customers, residents and non-residents, and the identity of their proxies; obtaining from natural persons documents proving their identity, and from legal entities duly authenticated documents about their statutes, the registration certificate, the ownership structure, a list showing the distribution of stock or shares (whether directly or indirectly), a list with the names of authorized signatories, a copy of the identity of the legal representative, the directors and the natural persons owning, whether directly or indirectly, a share that gives them effective control over the company’s management; and implementing due diligence measures on the non-professional proxy.

3. Checking periodically the identity of customers and re-determining the identity of economic right owners, including the owners of accounts opened before the promulgation of the Law on fighting money laundering; and preparing timed action plans for the fulfillment of these obligations.

4. Adopting a special Form for determining the economic right owner’s identity and the source of funds, as stipulated in Articles 4 and 7 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, and circulating this Form to all branches for using it in case of doubt about the economic right owner’s identity or the source of funds.

5. Retaining 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. Retaining as well copies of all operations-related documents, for at least five years after performing the operation.

6. Establishing the Special Committee for Fighting Money Laundering and Terrorism Financing stipulated in Article 10, Paragraph 1 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, and specifying its tasks pursuant to Article 11 of these Regulations. The fulfillment of these tasks must be verified by the external auditor.

7. Establishing “the Compliance Unit” stipulated in Article 10, Paragraph 2 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, and specifying its tasks pursuant to Article 11 of these Regulations. The fulfillment of these tasks must be verified by the external auditor, based on the reports prepared by this Unit.

8. Establishing a computerized central archive for collected information that includes, at least, the names circulated by the SIC, and those of holders of doubtful accounts reported by the bank or financial institution. This archive must be updated on a continuous basis.

9. Using a special register or a software program that records the names of persons who open or activate accounts by proxy.

10. Using specialized software programs that enable the retrieval of periodical reports for monitoring customers’ accounts and the operations to which apply, for indicative purposes and not restrictively, the indicators specified in Article 8 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing.

11. Appointing, in each of the bank/financial institution’s branch, an Officer responsible for the control of operations, who shall fulfill his duties, particularly, in monitoring cash operations, transfers and any other operations.

12. Reporting to the Governor of Banque du Liban, in his capacity as SIC Chairman, any operation suspected of involving money laundering and terrorism financing.

13. Ensuring the continuous training of the concerned staff and officers and their participation in seminars, workshops and conferences, so as to keep them abreast of AML/CFT methods.

14. Preparing a procedure guide about the obligations stipulated in the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing. This guide must take into account the structure of the bank/financial institution and its departments, and must be communicated to all employees and branches for adoption.


16. Adopting a risk-based approach to classify customers and operations according to risk levels, and establishing risk-based control measures and procedures, as specified in Article 9 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing.

II. To verify, in the bank/financial institution, that the Internal Audit Director, the Officer responsible for operations control at the branch, the Head of Transfers and Checks Sections, the cashiers, and the branch director are fulfilling their obligations, as stipulated in Article 11 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing.

III. To verify whether the decision taken by the director of the bank/financial institution’s branch to exempt some
customers from filling the cash transaction slip (CTS) and to set ceilings for such exemptions was based on valid criteria that justify these exemptions and ceilings, and to make sure that the CTS is filled by non-exempted customers.

IV. To verify basic obligations that are not included in the procedure guide stipulated in Article 11, Paragraph 1, Subparagraph (a) of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, or that are in contradiction with the said guide.

Special Investigation Commission Circular 7

Addressed to Financial Brokerage Firms

Pursuant to Law No. 318 of April 20, 2001 on Fighting Money Laundering and its amendments, particularly Article 4 and Article 7 (paragraph 1), financial brokerage firms are requested to comply with the following provisions as a minimum:

1. To ascertain the identity and business of correspondent banks and require them to produce documented evidence proving they are not shell banks.

2. To check the identity of permanent and transient clients, residents and non-residents, and that of their proxies. To obtain from individuals documents proving their identity and residence, and from legal entities registration documents, statutes and addresses, in addition to the identity of persons authorized to sign on their behalf. To adopt, for this purpose, a KYC Form (KYC: Know Your Customer) that should include, as a minimum, basic information about the client (full name, date and place of birth, nationality, address, social status, detailed occupation, financial status, beneficial owner, signature and date).

3. To recheck periodically, particularly when suspicion arises, the identity of clients and beneficial owner, including the holders of accounts opened before the promulgation of the Law on Fighting Money Laundering, for the purpose of updating the information of KYC Forms and obtaining the documents needed for evidence.

4. To keep the documents related to the clients and operations mentioned in Paragraph 2, for at least five years after closing the account or carrying out the operation.

5. To appoint a Compliance Officer entrusted with the following duties:
   • To prepare an anti-money laundering manual that includes provisions stipulated in this Circular, with due consideration of the structure and departments of the financial brokerage firm, and to update the manual when needed. Also, to prepare the KYC Form mentioned in paragraph 2 above, and to submit the manual and the KYC Form to the Board of Directors for approval.
   • To monitor accounts, implementation, and efficiency of anti-money laundering procedures (through adequate software programs when needed, that display money-laundering indicators), in order to identify suspicious transactions; and to provide relevant periodical reports to the Board of Directors.
   • To train personnel on procedures and methods to fight money laundering.

6. To fill the cash transaction slip (CTS) that includes a special section showing the source of funds exceeding USD 10,000 or its equivalent. The Compliance Officer may exempt some clients from this procedure after setting a ceiling, such exemptions must be based on justifiable criteria.

7. To establish a database for collected information and update it continuously. This database should include, at least, the names communicated by the Special Investigation Commission, and those of holders of suspicious accounts and reported by the institution. To notify the SIC about any account opened subsequently by any of these persons, whether directly, indirectly, or by proxy.

8. To keep a special register or software program for recording the names of persons who open or activate accounts by proxy.

9. To refrain from closing a suspicious account before referring to the SIC.

10. To prohibit staff, under disciplinary sanctions, from tipping-off the concerned customers subject an investigation by the SIC, before the latter takes a decision to inform the related parties.

11. To report to the Governor of Banque du Liban, in his capacity of Chairman of the Special Investigation Commission, any operation suspected to involve money laundering.

This Circular shall be published in the Official Gazette and shall be effective upon its issuing.

Beirut, August 18, 2005
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
PART VIII

Money Laundering            Terrorism

PART IX

Reporting Indication: [ ] Yes              [ ] No

PART XI

SUSPICIOUS TRANSACTION

Date of Transaction:
Nature of Transaction:
Type of Transaction:
Amount in LBP:
Status of Transaction:
Attempted
Executed

Outcome of Transaction:

In Case the transaction is a Wire Transfer:

• Name of Reporting individual:
• Phone Number:
• Address:
• Nature of Business:
• Building:
• Street:
City:
Governate:

Cash              Credit / Debit Card
Check

Cash transactions:

1. Name of the Customer or Beneficiary:
2. Payment Method:
3. Date of Transaction:
4. Source of Funds:
5. Purpose of relationship:
6. Nationality:
7. Type:
   a. Legal Person
   b. Affiliate
   c. Other Relationship
8. Date & Place of birth:
9. Phone:
10. Additional Customer Due Diligence Measures:

Additional information:

1. Who initiated the transactions:
2. Owner of account:
3. Purpose of the relationship:
4. Purpose of the transaction:

Additional comments:

1. How was the activity detected:
2. How was the activity initiated:
3. How was the activity performed:
4. Is the legal person:
   a. Senior Manager
   b. Board Member
   c. Other

Electronic Suspicious Transaction Report

[Form No. 1]

[Form No. 2]
Special Investigation Commission
Circular 8

Addressed to Banks and Financial Institutions

Pursuant to the provisions of Law 318 of April 20, 2001, on Fighting Money Laundering, particularly those stipulated by Article 6, Paragraph 4,

Pursuant to the provisions of Article 12, Paragraph 6, of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering, attached to Basic Decision No. 7818 of May 18, 2001, and

Pursuant to the Decision of the Special Investigation Commission, taken in its meeting of November 2, 2006, Banks and financial institutions are requested:

• To rigorously implement the provisions of Article 12, Paragraph 6, of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering, attached to Basic Decision No. 7818 of May 18, 2001. In this respect, they must ascertain that all their staff and employees are complying with the obligation to refrain from disclosing information to any client concerning SIC actions related to the client, whether in the form of enquiry, accounts auditing or temporary freezing.

• To take constantly into account that SIC enquiries and audits do not prevent banks and financial institutions from normally dealing or continuing to deal with “the client”, as long as the SIC does not decide the contrary.

• To comply with the above-mentioned procedures, knowing that the Chairman of the Board will be held responsible for non-compliance.

Beirut, November 7, 2006
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Special Investigation Commission
Circular 9

Addressed to Banks

Pursuant to the provisions of Law 318 of April 20, 2001, on Fighting Money Laundering, particularly Article 6, Paragraph 4 thereof,

Pursuant to the provisions of Article 11, Paragraph 7, Subparagraph (c) of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering, attached to Basic Decision No. 7818 of May 18, 2001, and

Pursuant to the Decision of the Special Investigation Commission, taken in its meeting of December 4, 2008, Banks are requested to carry out in a strict manner the provisions of Article 11, Paragraph 7, Subparagraph (c) of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering. They have to make sure that no check is credited to the concerned account before being definitively collected from the issuing bank.

Beirut, January 2, 2009
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Special Investigation Commission
Circular 10

Addressed to Banks

With reference to SIC Decisions, notably those relating to traceable accounts, and in order to avoid any confusion and facilitate the SIC mission in tracking the movement of accounts suspected of concealing money laundering and terrorism financing, all banks must, regarding accounts classified as traceable by an SIC decision, comply with the following:

1. Concerning checks

• To prohibit the payment in cash of a check or a payment order drawn on a traceable account, whether the beneficiary of the check or payment order is the holder of the said account or a third party.

• To prohibit the payment of a check or a payment order drawn on the traceable account to any party other than the first beneficiary, on condition that the check is crossed.

• To prohibit the issuance of a cashier’s check drawn on the traceable account to the benefit of the account’s holder or any third party, unless the check is crossed and includes the expression “payable only to the first beneficiary”.

2. Concerning credit and debit cards

To limit to points of sale the use of credit and/or debit cards issued in relation with the traceable account, and to prohibit their use on ATMs.

3. Concerning cashier’s counters

To prohibit the holder of the traceable account from withdrawing directly any amount on the cashier’s counter of the bank where the said account is held.

Beirut, July 9, 2009
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
**Addressed to Banks**

As per section 4 of article 6 of Law 318 dated 20/4/2001 on fighting Money Laundering,

All banks are required to provide, as per the detailed attached form, the Special Investigation Commission with the requested statements of accounts relating to ongoing investigations concerning clients.

The said form should be prepared using Microsoft Excel Workbook, and in instances where the client has more than one account, each account should be designated with a separate sheet.

The statements of accounts prepared as per the above mentioned form are to be sent to the Special Investigation Commission using its information exchange program (PGP) and in its absence via CD.

This Circular shall be published in the Official Gazette and shall be effective upon its publication.

*Beirut, February 27, 2010*

Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

---

**Addressed to External Auditors Appointed at Category “A” Exchange Institutions**

Pursuant to Law 347 of August 6, 2001 on Regulating the Money Exchange Profession in Lebanon, and to Law 318 of April 20, 2001 on Fighting Money Laundering,

Pursuant to BDL Basic Decision No. 7933 of September 27, 2001 on Regulating the Money Exchange Profession,

Pursuant to BDL Basic Decision No. 9708 of September 24, 2007 on Cash Transfers in accordance with Hawala System, and

Pursuant to the SIC Decision taken in its meeting of May 26, 2011,

External auditors appointed at exchange institutions of Category “A” are required to prepare an annual report and to submit it to the SIC Secretariat by the end of March following the audited fiscal year, provided the report indicates whether or not these institutions have complied with the following obligations:

1. Checking the customers’ identity and addresses based on formal documents.
2. Keeping special records for operations which value exceeds USD 10,000 or its equivalent.
3. Retaining, for five years at least, copies of formal documents (customers’ identity and address) and copies of documents concerning the operations whose value exceeds USD 10,000 or its equivalent.
4. Sending to the bank a special notification (on the nature and object of the operation, the source and destination of funds, the beneficiery and the economic right owner’s identity) when the exchange institution performs in favor of its customers any banking operation through the bank (transfer, check issuance…) whose value exceeds USD 10,000 or its equivalent.
5. Informing Banque du Liban beforehand and in writing that it will undertake cash transfers in accordance with Hawala System; and retaining, for five years at least, the records of these operations and copies of the formal documents related to the concerned customers.
6. Reporting to the SIC the details of the operations suspected of concealing money laundering or terrorism financing, in case they take place.

*Beirut, May 27, 2011*

Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
Pursuant to the provisions of Law No. 318 of April 20, 2001 on Fighting Money Laundering and Terrorism Financing, particularly Paragraph 4 of Article 6 and Paragraph 1 of Article 7, thereof,
Pursuant to the provisions of Paragraphs 1 and 6 of Article 12, of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering attached to Basic Decision No. 7818 of May 18, 2001,
Pursuant to the provisions of Article 181 of the Code of Obligations and Contracts concerning the conditions for refraining from entering into a contract and there resulting liability,
Without prejudice to depositors and customers’ rights and interests in case the provisions of SIC Circular No. 8 are not implemented, and
Pursuant to the Decision taken by the SIC in its meeting of May 20, 2014,
We remind banks and financial institutions of the need to strictly implement the provisions of SIC Circular No. 8 of November 7, 2006, particularly in what follows:
• To ascertain that all their staff and employees comply with the obligation to refrain from disclosing to a customer any information about SIC actions related to the customer’s accounts, whether in the form of enquiry, auditing or temporary freeze.
• To take constantly into consideration that SIC enquiries and audits do not prevent banks and financial institutions from normally dealing or continuing to deal with customers, as long as the SIC does not decide the contrary.
Any bank or financial institution that violates the provisions of this Circular shall incur the administrative penalties that the Higher Banking Commission may impose in accordance with Article 208 of the Code of Money and Credit. These penalties shall not preclude the enforcement of penal sanctions and civil liability against the violating entity.

Beirut, May 26, 2014
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
• The concerned banks benefit from reductions in the Statutory Reserve, pursuant to Basic Decision No. 7835 of June 2, 2001.

This Circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, September 18, 2014
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Special Investigation Commission
Circular 19

Addressed to the concerned Institutions and Parties mentioned in Article 5 of Law No. 44 of November 24, 2015, and to Financial Intermediation Institutions, and Collective Investment Schemes, on the Implementation of UN Security Council Resolutions 1267 (1999), 1988 (2011) and 1989 (2011) and successor resolutions

Pursuant to Law No. 44 of November 24, 2015 (Fighting Money Laundering and Terrorism Financing), notably the provisions of Article 6, Paragraphs 2 and 5 thereof; and Pursuant to the Decision of the Special Investigation Commission, taken in its meeting of December 3, 2015,

FIRST:
The concerned institutions and parties mentioned in Article 5 of Law No. 44 of November 24, 2015, as well as financial intermediation institutions and collective investment schemes, are requested, as far as each is concerned:

1. To review constantly any update on the UN Security Council Website concerning the names designated in the lists issued pursuant to UN Security Council Resolutions 1267 (1999), 1988 (2011), 1989 (2011), and related successor resolutions and/or issued by the Special Sanctions Committees; and to automatically and immediately freeze, without delay and without any prior notice, the funds, accounts, operations, or other assets in whatever form (direct or indirect, joint…) related to these names, as soon as such names are listed; and to inform the Special Investigation Commission of this action and provide it with any information in this respect within a period not exceeding 48 hours.

2. To report to the Special Investigation Commission in case of similarity between the name of a customer and any designated name and details included in the lists issued pursuant to the UN Security Council Resolutions referred to in Paragraph 1 above and/or issued by the Special Sanctions Committees.

SECOND:
The provisions of this Circular shall be applicable to branches, sister institutions and subsidiaries abroad.

THIRD:
Any party violating the provisions of this Circular shall incur the sanctions stipulated in Article 13 of Law No. 44 of November 24, 2015, particularly for non-compliance with the immediate freezing obligation referred to in Paragraph 1, Subparagraph 1 above.

FOURTH:
This Circular shall be published in the Official Gazette and shall enter into force upon its publication.

Beirut, December 22, 2015
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Special Investigation Commission
Circular 20

Addressed to Banks, Financial Institutions and all other Reporting Entities

Pursuant to the provisions of Law No. 44 of November 24, 2015 (Fighting Money Laundering and Terrorism Financing), notably Articles 4, 5, 6, 7, and 13 thereof; Pursuant to the provisions of Article 12, Paragraph “First”, Subparagraph 3 of BDL Basic Decision No. 7818 of May 18, 2001 and its amendments, attached to Basic Circular No. 83 (Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing); and

In order to clarify and implement the provisions of Article 1, Paragraph "Second" of BDL Basic Decision No. 12253 of May 3, 2016, attached to Basic Circular No. 137 (Dealing with the US Act of December 18, 2015 and with its implementation regulations to prevent Hizballah from gaining access to international financial and other institutions);

Whereas, with a view to prevent any arbitrary procedure or measure that may cause harm to depositors and clients’ interests, particularly whenever closing the account of any depositor or client, or whenever refraining from opening an account in their names or from dealing with them, in an unjustified manner or under the pretext of de-risking;

Within the efforts made by Banque du Liban to foster financial inclusion;

In order to safeguard the utmost national interest; and Pursuant to the Decision taken by the Special Investigation Commission (SIC) in its meeting of May 26, 2016,
The following is decided:

Article 1

FIRST:
Banks, financial institutions, financial intermediation institutions, and all other reporting entities are requested not to take any measure, in terms of closing any account held by any client, or refraining from dealing with or from opening any account to any such client, before the elapse of 30 days from filing a report with the SIC. This report must justify the reasons for taking these procedures and measures (KYC; the account movement or frequency or size;…)

SECOND:
If no reply is received from the SIC within the above-mentioned time limit, the concerned banks and institutions shall be entitled to take the relevant measures in this regard.

THIRD:
These procedures shall not apply in case of accounts held by persons or institutions designated in any of the lists issued with respect to the implementation of the above-mentioned US Act of December 18, 2015.

Article 2

Any party violating the provisions of this Circular shall be prosecuted before the Higher Banking Commission.

Article 3

This Circular shall be published in the Official Gazette and shall enter into force on May 3, 2016.

Beirut, May 26, 2016
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
• The policy is inconsistent with the policyholder’s needs or it differs from prior policies issued upon the latter’s request.
• Purchasing a life insurance policy through a single large premium.
• Purchasing a life insurance policy by a non-resident, non-Lebanese individual.
• Setting life insurance premiums through large and/or repeated cash payments, or through payments inconsistent with the policyholder’s financial status.
• Payments from unclear sources.
• Funding the life insurance policy through one large booster payment.
• Overfunding the life insurance policy with additional and repeated unusual payments.
• Paying life insurance premiums with funds from abroad.
• Requesting withdrawals on the life insurance cash value, in order to obtain cheques from the insurance company just a short period after the policy issuance.
• Requesting transfers from the life insurance cash value towards accounts held abroad.
• Cancelling the life insurance policy, regardless of penalties, in order to obtain cheques from the insurance company.

4. To report to the SIC, according to the mechanism mentioned in SIC Circular No. 17 of September 16, 2014, the details of suspicious transactions that may involve money laundering or terrorist financing, provided these reports cover suspicious transactions carried out by the concerned agents and insurance brokers.

5. To request from their staff, subject to liability, to refrain from notifying the customers that the SIC investigates or inquires about their operations, unless the SIC decides otherwise.

6. To take the necessary actions and measures in order to prevent the misuse of technological developments for money laundering or terrorist financing purposes, as well as when dealing with high-risk clients, and when correspondent banking relationships are initiated; and to comply accordingly with the relevant Circulars and Announcements issued by BDL and the SIC.

7. All the persons mentioned in Article 5 of Law No. 44 of November 24, 2015, shall be governed by the provisions of this Circular, where applicable.

This Circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, September 9, 2016
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
Special Investigation Commission
Circular 23

Addressed to Banks, Financial Institutions and other Institutions Bound to Report on Money Laundering and Terrorism Financing Operations

Pursuant to Article 7 of Law No. 44 of November 24, 2015 on Fighting Money Laundering and Terrorism Financing,
Pursuant to Article 5 of the Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorism Financing, attached to Basic Circular Decision No. 83 of May 18, 2001,
Pursuant to the SIC decision taken in its meeting of October 19, 2017,
1. Banks, financial institutions and other institutions concerned with Article 4 of Law No. 44 of November 24, 2015 are requested, when reporting to the SIC any operations suspected or ascertained to be involving money laundering or terrorism financing, as stipulated in Law No. 44 of November 24, 2015, to fill in Form No. 1 (E-STR) attached to this Circular and to send it to the SIC, together with all relevant documents.
2. All other institutions and parties concerned with Article 5 of Law No. 44 of November 24, 2015 are requested, when reporting to the SIC any operations suspected or ascertained to be involving money laundering or terrorism financing, as stipulated in Law No. 44 of November 24, 2015, to enclose, with a letter addressed to the SIC Chairman, a report on the concerned operation, to be prepared according to Form No. 2 attached to this Circular, together with all relevant documents.

This Circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, November 6, 2017
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Special Investigation Commission
Circular 24

Addressed to the Parties and Individuals mentioned in Article 5 of Law 44 of 24 November 2015

Defining and Identifying the "Beneficial Owner"

Pursuant to Law 44 of 24 November 2015 (Fighting Money Laundering and Terrorism Financing), particularly Articles 5 and 6 thereof;
Whereas the parties and individuals mentioned in Article 5 of Law 44, of which insurance companies, are required to comply with the stipulations of Article 4 of that Law and with the regulations and recommendations issued by the SIC for the purpose of implementing the provisions thereof;
Pursuant to the FATF recommendations and the relevant interpretive notes; and
Pursuant to the Decision of the SIC, taken in its meeting of 14 June 2018,
The following is decided:

Article 1
The following expressions shall mean:
1. Customer: any natural or legal person, whether a company or a partnership of any type, or any legal arrangement (e.g. a trust), or any body, organization or non-profit organization (mutual funds, cooperatives, welfare centers, charities, clubs, etc.).
2. Beneficial Owner: any individual who ultimately owns or who exercises ultimate effective control, whether directly or indirectly, over the Customer and/or the individual on whose behalf a transaction is carried out.

Indirect ownership and/or control include the situations where the ownership and/or control is exercised through a chain of ownership or by means of control other than direct control.

This expression shall also apply to the beneficial owner of the beneficiary of a life insurance policy or of any other Unit-Linked Investment and Capitalization insurance policies.

Article 2
With respect to the Customer that is a legal person, the Beneficial Owners shall be identified and reasonable measures taken to identify them in the following manner:
1. Identify each natural person who holds, whether directly or indirectly, 20% or more of the capital of the legal person.
2. In case of doubt as to whether the natural person(s) identified pursuant to Subparagraph 1 above is (are) the Beneficial Owner(s), or when no natural person holds 20% or more of the Customer’s capital, the natural person who exercises control over the legal person through other means (e.g. holding a majority of voting
rights or the rights to appoint or dismiss the majority of the administrative or regulatory body at affiliated entities...

3. When no natural person is identified pursuant to Subparagraphs (1) and (2) above, reasonable measures shall be taken in order to identify and verify the identity of the persons holding senior management positions.

Article 3
With respect to Customers that are legal arrangements, the Beneficial Owners shall be identified and reasonable measures taken to identify them, in the following manner:

1. With regard to trusts, each of the persons below shall be identified:
   - The Settlor
   - The Trustee
   - The Protector
   - The Beneficiary; and if the latter’s identity is not determined or verified, then the class of beneficiaries in whose favor the legal arrangement was established.
   - Any other natural person exercising an effective control over the trust through direct or indirect ownership or through other means.

   The definitions stated in the glossary attached to the FATF 40 Recommendations shall be adopted to identify the persons mentioned in this Subparagraph 1.

2. With respect to other types of legal arrangements, including those arrangements similar to trusts, the persons holding positions similar to the positions specified in Subparagraph 1 of this article, shall be identified.

Article 4
The concerned parties and individuals shall, as far as each is concerned, apply the due diligence measures which are specified in AML/CFT Law 44 of 24 November 2015, and which must include verifying the identity of each of their permanent and transient customers, whether resident or non-resident, and determining the nature of their business; understanding the ownership structure and/or control over the legal person, the purpose and nature of the business relation and/or the account opening; identifying the Beneficial Owner and the source of funds; and ensuring the ongoing control of operations.

These parties and individuals are required to verify the identity of the Beneficial Owner before or during the course of establishing a business relationship or of conducting transactions for transient customers. They are also required to check that any person purporting to act on behalf of the customer is so authorized, and to identify and verify the identity of that person.

Article 5
Upon identifying the “Beneficial Owner”, the same Due Diligence measures applicable to “Customers” shall apply, including those issued by the Special Investigation Commission.

Article 6
This Circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, June 14, 2018
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé

Addressed to Banks, Institutions and Parties referred to in Articles 4 & 5 of Law No. 44 dated November 24, 2015

On the National ML & TF Risk Assessment (NRA)

Pursuant to Article 6, Paragraph 2, Sub-paragraph 4 of Law No. 44 of November 24, 2015 that empowers the Special Investigation Commission to issue regulations on the implementation of the provisions of the said Law, and to issue recommendations to all concerned parties, and,

Pursuant to Articles 4 and 5 of AML/CFT Law No. 44 of November 24, 2015, which require continuous monitoring, review of business relationships, and to take into consideration indicators that flag the possible existence of money laundering and terrorism financing, and,

Based on the outcomes of the second National ML and TF Risk Assessment of year 2019, in which a methodology (that includes quantitative and qualitative information, and covers private sector reporting entities) was used to identify threats and vulnerabilities, and carry out the analysis and assessment thereof in light of their consequences, so as to identify risk levels of ML/TF offences associated with predicate offences stipulated in Law No. 44 of November 24, 2015, and,

Based on the strategic plan for risk mitigation that was discussed during the meetings of the National Committee for coordinating AML Policies and the National Committee on suppressing terrorism financing, both established by the Council of Ministers, and,

With a view of having a common understanding of identified risks between relevant national authorities, and,

In order to strengthen the understanding of identified risks at banks, institutions and parties referred to in Articles 4 and 5 of Law No. 44 of November 24, 2015, that are most
susceptible to the possible occurrence of the high risk crimes through them, and,

With a view of having the most efficient use and allocation of resources, and,

In order to assist in taking the necessary risk mitigation measures, while focusing on higher risk areas identified as a result of the NRA, and;

Pursuant to the Decision of the Special Investigation Commission, taken in its meeting of September 18, 2019,

The following is requested:

FIRST:

Banks, institutions and parties referred to in the above-mentioned Articles 4 and 5 must consider, when assessing their own risks (customers, services/products, countries) and when applying the risk based approach, that terrorism financing, and money laundering crimes associated with corruption, tax evasion, and drug trafficking, resulting mainly from local predicate offences, in addition to cybercrimes are high risk crimes, and must adopt measures and controls commensurate with these risks.

SECOND:

Financial sector entities, particularly banks, category “A” exchange institutions, and money remittance companies, must adopt, as far as each is concerned, controls and the necessary risk mitigation measures to reduce the possible occurrence of high risk crimes identified in paragraph “First” above through them, and to reduce the possible misuse of products and services offered, particularly those related to cash operations, “Hawala” operations, and accounts of legal persons, especially offshore companies where the beneficial owner and the source of funds are difficult to identify, in addition to instances of non face-to-face dealings or dealings through third parties.

THIRD:

Designated Non Financial Businesses and Professions (DNFBPs) must adopt controls and the necessary risk mitigation measures to reduce the possible occurrence of high risk crimes identified in paragraph “First” above through them, and to reduce the possible misuse of products and services offered, particularly those related to cash operations, “Hawala” operations, and accounts of legal persons, especially offshore companies where the beneficial owner and the source of funds are difficult to identify, in addition to instances of non face-to-face dealings or dealings through third parties.

This Circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, September 18, 2019
Chairman of the Special Investigation Commission
The Governor of the Banque du Liban
Riad Toufic Salamé
To implement AML/CFT programs including group-wide programs that cover all branches and majority-owned subsidiaries of that group. These programs must be tested by an independent audit function and must include the following measures:

- Adopting AML/CFT guidelines (also at the group level) approved by the Senior Management, which include the adopted policies and procedures in addition to ML/TF risk management requirements.
- Documenting and retaining the results of the ML/TF risk assessment, updating the latter when necessary, and adopting a mechanism that allows providing it to the supervisory authorities when needed. This risk assessment must contain identification and evaluation of the risks that may arise either from the use of new technologies, newly offered products, business practices and new delivery mechanisms or from the development of pre-existing ones. A risk assessment must be done prior to the launch, or use of such products, practices and technologies, and the necessary risk mitigating measures must be adopted. Senior management should approve the policies, controls and procedures adopted for this purpose, and should monitor its implementation and enhancement.
- Implementing an on-going AML/CFT training programs for all concerned employees.
- Adopting policies and procedures that enable sharing the required information for CDD purposes within the group and making it possible to provide this information when necessary for AML/CFT purposes, to the compliance officers across the group whether at the level of the branches or its majority owned subsidiaries. This should include information on customers, accounts, and transactions, including analysis reports and activities which appear unusual. The branches and the subsidiaries should also be able to receive such information in a manner that is appropriate and commensurate with the risk management measures. Additionally, there must be in place adequate procedures that provide sufficient safeguards concerning the confidentiality and the use of this information, which safeguards against not informing or tipping-off the customer.
- Requesting from foreign branches and majority owned subsidiaries operating abroad, in which the parties and individuals mentioned in Article 5 of Law no. 44/2015 own a majority, to adopt and apply at a minimum the AML/CFT measures required in Lebanon. In the event that this is not possible as a result of conflict with the provisions of binding laws and regulations in force at the location of the branch or subsidiary, appropriate additional measures to manage the ML/TF risks should be applied and concerned Lebanese supervisory authorities should be informed.

4. The AML/CFT Compliance Officer, appointed at the management level, must ensure the sound implementation of the required AML/CFT programs and procedures, particularly the following:

- CDD measures are applied on existing business relationships on the basis of materiality and risk; and these measures were applied at the appropriate times, taking into consideration whether these measures have previously been undertaken, when undertaken and the adequacy of data obtained.
- Transactions conducted are consistent with the information available on customers, their activities and risk profile. Information collected on the purpose of the relation, source of funds; and documents and/or data and/or information collected under the CDD process should be kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.
- Enhanced due diligence measures applied are commensurate to the risks of business relationships and transactions conducted with natural and legal persons (including financial institutions) from countries against which FATF has called for action. In this respect, the FATF website is periodically reviewed, especially after each plenary meeting.

5. To verify, when dealing with a third party, that the latter is regulated and supervised by official authorities and meets the FATF criteria on customer due diligence and record keeping procedures; and ensure that it is possible to obtain immediately and without delay, any information
needed to identify the customer and the beneficial owner and to understand the nature of the business, as well as obtain copies of the customer’s identification data and documents related to CDD procedures. The ultimate responsibility for CDD measures, shall remain with the party relying on the third party whether the latter is located inside or outside Lebanon, taking into consideration that when dealing with the third party, all risk mitigation measures shall be taken, particularly those associated with countries that do not apply, or apply partly the FATF Recommendations.

6. To review constantly through available software any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) concerning the names designated on the national list of natural persons, legal persons, and entities involved in terrorist operations or terrorism financing. Immediately freeze without delay the funds and/or accounts and/or operations related to these names, including attempted operations, in addition to other assets owned or controlled by these names in whatever form (direct, indirect, joint...). Inform the Special Investigation Commission of this action and provide it with any information in this respect within a period not exceeding 48 hours. Report to the Special Investigation Commission in case of similarity between the name of a customer and any designated name and details included in the national list referred to above.

7. To implement FATF Recommendation 7 in terms of conducting the necessary reviews, and immediately freeze without delay the funds and/or related accounts and/or transactions (including attempted ones), and/or other assets, and inform the Special Investigation Commission of this action and provide it with any information in this respect within a period not exceeding 48 hours. Report to the Special Investigation Commission in case of similarity between the name of a customer and any designated name and conduct related risk assessments.

8. With respect to insurance companies, to take into consideration the element of “the beneficiary” of a life insurance policy as a relevant risk factor when assessing risks, and should implement CDD measures on the said beneficiary and of other insurance products, as soon as that beneficiary, whether a natural person, legal person or legal arrangement is identified or designated. In addition to the identification of the beneficiary, those measures should include the verification of the said beneficiary identity at the time of payout. If a beneficiary is identified by characteristics or by class or by other means, sufficient information must be obtained concerning the beneficiary to satisfy the insurance company that it will be able to determine the identity of the beneficiary at the time of the payout. Insurance companies should also determine at least at the time of payout whether the beneficiaries and/ or beneficial owners are PEPs, and should where higher risk are identified, inform senior management before the payout of the proceeds; conduct careful review of the business relationship and consider filing a suspicious transaction report to the SIC. In case the insurance company classifies the beneficiary who is a legal person or a legal arrangement as “high risk”, enhanced measures shall be applied, which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Casino du Liban must implement the required CDD measures, in particular when customers engage in financial transactions that equal or exceed USD 3,000 or its equivalent, and in accordance with the requirements of FATF Recommendation 22. Casino du Liban must cross-check information obtained through CDD measures with customers’ transactions.

10. To promptly report to the SIC in case of assertions or suspicion, based on reasonable or objective grounds, when the executed or attempted transaction is related to money laundering or related predicate offences or terrorism financing or terrorist acts or terrorist organizations. In cases where a suspicion of money laundering or terrorism financing is formed, and there is reason to believe that performing the CDD requirements will tip-off the customer, it is permitted not to pursue these requirements, and file a suspicious transaction report to the SIC.

11. This circular shall apply to all parties and individuals mentioned in Article 5 of Law 44 of 24 November 2015, where applicable. This circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, 24 November 2021
Chairman of the Special Investigation Commission
The Governor of Banque du Liban
Riad Toufic Salamé
Addressed to the Parties and Individuals mentioned in Article 5 of Law No. 44 dated 24/11/2015

Pursuant to Law No. 44 of November 24, 2015 (Fighting Money Laundering and Terrorism Financing), notably Articles 5, 6, and 7 thereof;

With reference to SIC Circular 19 dated December 22, 2015 and Circular 26 dated November 24, 2021 addressed to the parties and individuals mentioned in Article 5 of Law No. 44/2015;

Considering that parties and individuals not subject to the Banking Secrecy Law of September 3, 1956 that are mentioned in Article 5 of Law No. 44/2015, must comply with the requirements of Article 4 of the said law and with the regulatory texts and recommendations issued by the SIC for the purpose of implementing its provisions;

Pursuant to the Decision of the SIC taken in its meeting of May 19, 2022;

FIRST:

1. The text of the last paragraph of section (1) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

   “Additionally, enhanced due diligence measures must be applied on transactions, as well as on customers and beneficial owners classified as high-risk, and also on PEPs classified as per FATF definition, their family members and close associates, whether they are customers or beneficial owners, as to be determined by the risk management system in place. The enhanced due diligence measures include obtaining senior management approval for establishing or continuing the business relationship, conducting enhanced ongoing monitoring on the relationship and determining the source of wealth.”

2. The text of the second part of paragraph (2) of section (2) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

   “Additionally, all information related to the customer and the beneficial owner must be retained, particularly the information obtained through CDD measures, as well as copies of all the documents used to verify the foregoing, and the records of accounts for at least five years following the closure of the account or the termination of the business relationship, or after the legal person ceases to exist. All records of transactions should also be retained, including business correspondence and the results of any analysis undertaken, for at least five years following the completion of the transaction. These records should be sufficient to permit the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution in case of criminal activity.”

3. The text of paragraph (5) of section (3) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

   “Requesting from branches and subsidiaries operating abroad, in which the parties and individuals mentioned in Article 5 of Law No. 44/2015 own a majority, to adopt and apply the AML/CFT measures required in Lebanon, where the minimum AML/CFT requirements of the host country are less strict than those of Lebanon, to the extent that the host country laws and regulations permit. In the event that this is not possible as a result of conflict with the provisions of binding laws and regulations in force at the location of the branch or subsidiary, appropriate additional measures to manage the ML/TF risks should be applied and concerned Lebanese supervisory authorities should be informed.”

4. The text of paragraph (2) of section (4) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

   “Transactions conducted are consistent throughout the course of the relationship with the information available on customers, their activities and risk profile. Information is collected on the purpose of the relation and source of funds; and documents and/or data and/or information collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.”

5. The text of section (6) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

   “To review constantly, through available software, any update on the website of the General Directorate of Internal Security Forces (www.isf.gov.lb) concerning the names designated on the national list of natural persons, legal persons, and entities involved in terrorism or terrorism financing; and once the designation decision is issued, to immediately freeze without delay the funds, or accounts, or operations, including attempted ones, or other assets, if any, owned or controlled in any form (directly or indirectly, jointly...) by these names; and to inform the Special Investigation Commission of this action and provide it with any information in this respect within a period not exceeding 48 hours; and to report to the Special Investigation Commission in case of similarity between the name of a customer and any designated name and details included in the national list referred to above. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.”

6. The text of section (7) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:
“To implement FATF Recommendation 7 in terms of conducting the necessary reviews and immediately freezing without delay the related funds and/or accounts, and/or transactions, including attempted ones, or other assets, within a matter of hours from the issuance of the designation decision; and to inform the SIC of this action and provide it with any information in this respect within a period not exceeding 48 hours; and to report to the SIC in case of similarity between the name of a customer and any designated name, and conduct related risk assessments. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds and other assets that are owned or controlled by designated persons or entities.”

7. The text of section (10) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

“To promptly report to the SIC in case of assertions or suspicion, based on reasonable or objective grounds, when the executed or attempted transaction is related to money laundering or related predicate offences or terrorism financing or terrorist acts or terrorist organizations, regardless of the amount involved. In cases where a suspicion of money laundering or terrorism financing is formed, and there is reason to believe that performing the CDD requirements will tip-off the customer, it is permitted then not to pursue the CDD requirements, and file a suspicious transaction report to the SIC immediately.”

8. The text of paragraph (1) of section First of SIC Circular 19 dated 22/12/2015 is repealed and replaced with the text below:

“To review constantly, on the UN Security Council website, any update in relation to the names designated on the lists issued pursuant to UN Security Council Resolution 1267/1999, Resolution 1988/2011, and Resolution 1989/2011, and the relevant successor resolutions, and/or the lists issued by the Special Sanctions Committees, and to automatically and immediately freeze, without delay and without prior notice, within a matter of hours from the issuance of the designation decision, the funds or accounts or operations or other assets, if any, related to these names in any form (directly or indirectly, jointly...), and to inform the Special Investigation Commission of this action and provide it with any information in this respect within a period not exceeding 48 hours. The term “freeze” means to prohibit the transfer, conversion, disposition or movement of funds or other assets that are owned or controlled by designated persons or entities.”

9. Section (11) of SIC Circular 26 dated 24/11/2021 is numbered (13).

SECOND:

10. Section (11) shall be added to SIC Circular 26 dated 24/11/2021, and shall read as follows:

“All parties and individuals mentioned in Article 5 of Law No. 44/2015 of 24 November 2015 are required to apply countermeasures that are proportionate to the level of risk, whether to countries against which the FATF calls for such action or on the basis of concerns identified by these parties themselves. Examples of these measures include but are not limited to: obtaining the approval of the Senior Management for entering into, or continuing a business relationship with customers, increasing and prioritizing control, not establishing branches or subsidiaries or representative offices in these countries, and not relying on third parties located in these countries.”

11. Section (12) shall be added to SIC Circular 26 dated 24/11/2021, and shall read as follows:

“All parties and individuals mentioned in Article 5 of Law No. 44/2015 of 24 November 2015 are required to ensure that customer due diligence information and transaction records are swiftly available to the supervisory authorities upon request, within three business days at most.”

This circular shall be published in the Official Gazette and shall enter into force upon its issuance.

Beirut, 19 May 2022
Chairman of the Special Investigation Commission
The Governor of Banque du Liban
Riad Toufic Salamé
“To obtain the following official documents or records so as to verify the identity of the customer and the beneficial owner:

- In the case of a natural person, the original passport or the identity card or an extract from the Civil Status or a residence permit.”

2. The text of paragraphs (1), (2), (3) and (4) of section (3), of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

- “Adopting policies, controls and procedures approved by the senior management for combating ML/TF and for the sharing of required information for CDD purposes and for ML/TF risk management and mitigation, including at the group level.”
- “Documenting and retaining the results of the ML/TF risk assessment, updating the latter when necessary, and adopting a mechanism that allows providing it to competent authorities and/or self-regulatory bodies (as far as each is concerned) when needed. This risk assessment must contain identification and evaluation of the risks that may arise either from the use of new technologies, newly offered products, business practices and new delivery mechanisms or from the development of pre-existing ones. A risk assessment must also be conducted prior to the launch, or use of such products, practices and technologies, and the necessary risk mitigating measures must be adopted. Senior management should approve the policies, controls and procedures adopted for this purpose, and should monitor its implementation and enhancement.”
- “Implementing an on-going AML/CFT training programs for all employees and concerned parties.”
- “Adopting procedures that enable the provision of information on customers, accounts and transactions from branches and majority-owned subsidiaries of the group to the compliance officer at the group level. This should include information and analysis reports or activities which appear unusual. The branches and the subsidiaries should also be able to receive such information from the compliance officer at the group level in a manner that is appropriate and commensurate with the risk management measures. Additionally, there must be in place adequate procedures that provide sufficient safeguards concerning the confidentiality and the use of this information, which safeguards against not informing or tipping-off the customer.”

3. The text of section (3) of SIC Circular 27 dated 19/5/2022 is repealed and replaced with the text below:

“Requesting from branches and subsidiaries operating abroad, in which the parties and individuals mentioned in Article 5 of Law No. 44/2015 own a majority, to adopt and apply the AML/CFT measures required in Lebanon, where the minimum AML/CFT requirements of the host country are less strict than those of Lebanon, to the extent that the host country laws and regulations permit. In the event that the host country does not permit the proper implementation of AML/CFT measures consistent with those in Lebanon, therefore, appropriate additional measures to manage the ML/TF risks should be applied and concerned Lebanese supervisory authorities should be informed.”

4. The text of paragraph (1) of section (4) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

“CDD measures are applied on existing customers on the basis of materiality and risk; and these measures must be applied at appropriate times on such existing relationships taking into consideration whether and when these measures have previously been undertaken and the adequacy of data obtained.”

5. The text of section (5) of SIC Circular 26 dated 24/11/2021 is repealed and replaced with the text below:

“To verify, when dealing with a third party, that the latter is regulated and supervised by official authorities and meets the FATF due diligence and record-keeping requirements; and to obtain immediately and without delay, any information needed to identify the customer and the beneficial owner and understand the nature of the business, as well as obtain copies of the customer’s identification data and documents related to CDD procedures. The ultimate responsibility for CDD measures, shall remain with the party relying on the third party whether the latter is located inside or outside Lebanon, taking into consideration when dealing with the third party the information on the risk level associated with these countries specifically those that do not apply, or apply partly the FATF Recommendations.”

SECOND:

6. Section (14) shall be added to SIC Circular 26 dated 24/11/2021, and shall read as follows:

“All parties and individuals mentioned in Article 5 of Law No. 44 of 24 November 2015 are requested to adopt high standards of competence when hiring employees.”

7. Section (15) shall be added to SIC Circular 26 dated 24/11/2021, and shall read as follows:

- “In addition to the required obligations including from insurance companies, parties and individuals mentioned in Article 5 of law No. 44 dated 24/11/2015 must also take into account, for indicative purposes only, the customer, country, and service risks when classifying the risk of customers and operations:”
1. Customer Risk:
   a) Customers whose occupations rely mainly on cash
   b) Politically Exposed Persons (PEPs)
   c) Offshore companies.
   d) Companies located in countries known to be tax haven.
   e) Customers who are nationals or residents of countries that do not or insufficiently apply the FATF Recommendations.
   f) Non-profit organizations (NPOs), particularly newly established NPOs that do not have clear programs or clear funding sources.

2. Country Risk:
   a) The stringency of AML/CFT laws, and the efficiency of the supervisory and judiciary authorities in charge of their implementation.
   b) The existence of banking secrecy.
   c) The situation of the country in terms of corruption and organized crime.

3. Service Risk:
   a) With respect to Lawyers, Notaries and Accountants: «The services mentioned in Article 5 of AML/CFT Law No. 44/2015».
   b) With respect to Jewelers: «The trade of Diamond and Gold Bar».
   c) With respect to Real Estate Dealers and Agents: «The sale or purchase of real estate without passing through a bank».
   d) With respect to Casino du Liban: «Gambling tables».

This circular shall be published in the Official Gazette and shall enter into force upon its issuance.

*Beirut, 21 July 2022*

*Chairman of the Special Investigation Commission*

*The Governor of Banque du Liban*

*Riad Toufic Salamé*
ANNEX

2019 ML & TF National Risk Assessment
Summary

Foreword 156
1. Introduction 158
2. Methodology 159
3. ML/TF Threats 161
   3.1 Money Laundering Threats 161
   3.2 Terrorist Financing Threats 162
4. Inherent ML/TF Vulnerabilities 164
5. Financial Sector and DNFBPs 164
   5.1 Financial Sector 164
   5.2 Designated Non-Financial Businesses & Professions 166
6. Legal Persons & Arrangements and Non-Profit Organizations 169
   6.1 Legal Persons & Arrangements 169
   6.2 Non-Profit Organizations 170
7. ML/TF Risks 171
8. Risk Mitigation Measures - AML/CFT Regime 172
9. Looking Forward 175

ML & TF National Risk Assessment
2022 Update 176
Lebanon enjoys a free market economy, a vibrant financial sector and long-standing ties with the global financial system, which naturally expose any country to risks from illicit financial flows. The effective implementation of AML/CFT laws and regulations is thus necessary to disrupt criminal activity and mitigate money laundering and terrorist financing risks. The presence of robust risk-based AML/CFT supervision and strong enforcement measures are equally important. Efforts continue to be geared to this end, and Lebanon currently enjoys a comprehensive AML/CFT regime that safeguards both the financial and non-financial sectors from potential misuse. There is room for some improvements to advance the ongoing efforts to disrupt ML & TF activities and further mitigate risk. In this regard, the SIC - Lebanon’s FIU, along with other AML/CFT stakeholders continue to work tirelessly to keep the regime at par with international standards. This in turn helps preserve the important role banks play in our economy, and ensures that Lebanon continues to be a safe and attractive country for both foreign direct investment and legitimate business.

Illicit proceeds from money laundering predicate crimes such as corruption and tax evasion deprive the government from desperately needed funds. The impact of such crimes on the economy and society is detrimental. The spillover effects from the neighboring conflict and the refugees’ situation continues to affect Lebanon in many ways. Since the beginning of this conflict, numerous terrorist attacks killed and injured many Lebanese, and caused grave devastation. These are constant reminders of the importance of having an effective AML/CFT regime that tackles criminality and deprives terrorists from funds needed to execute their attacks and cause destruction. As ML & TF risks continue to evolve, so must our countermeasures and responses. To this extent, we have committed significant resources and continue to work with international partners on numerous initiatives, including participating in the work undertaken by the FATF, MENAFATF and the Egmont Group, as well as the CIFG within the Global Coalition against Daesh. Significant efforts also continue to be exerted locally, including important work on identifying ML/TF threats & vulnerabilities, as well as taking necessary risk mitigating measures.

In 2013, the Special Investigation Commission highlighted to the Prime Minister the importance of complying with the 2012 strengthened FATF recommendations against which Lebanon would be assessed. The Prime Minister in turn requested from a number of authorities to cooperate with the SIC on the ML & TF National Risk Assessment. Backed by high level political commitment, the SIC led Lebanon’s first NRA, and engaged Public sector authorities - members from the national AML and CFT Committees, including law enforcement and judicial authorities. Elements from the private sector were also approached for their input. In spite of the many hardships and challenges facing the country at the time, thanks to strong commitment and senior level involvement, Lebanon’s first NRA was completed by year-end 2014. No report was made public, however findings were shared by various means with several stakeholders including elements from the private sector. Numerous mitigating measures were also taken including introducing major amendments to the prevailing AML/CFT Law.
In 2019 Lebanon’s second NRA, which in many aspects takes reference from the FATF NRA guidance and builds on lessons and experiences learned from the first NRA, was concluded. It identified ML/TF risks based on threats and vulnerabilities, and resulted in risk mitigation measures being taken that included legislative, regulatory, and operational actions covering supervision and law enforcement. In the early stages of the second NRA and prior to its full completion, mitigating measures were taken with respect to a number of identified risks. Other risk mitigating measures were highlighted in a strategic plan that is being executed which pillars on four main lines of action:

1. Improve technical compliance where needed, i.e. legislative and regulatory updates.
2. Provide where needed certain authorities with resources to improve AML/CFT capacity.
3. Enhance AML/CFT risk-based supervision where needed, and align supervisory resources with the results of the 2019 NRA.
4. Improve the partnership with private sector reporting entities.

The effective combating of illicit financial flows necessitates addressing risks in due time. We are committed to improving the effectiveness of our AML/CFT regime by implementing the needed risk mitigation measures, including improving cooperation among various AML/CFT regime stakeholders and assessing risk on an ongoing basis.

Riad Toufic Salamé

Banque du Liban, Governor
Special Investigation Commission, Chairman
AML National Committee, Chairman
Beirut, September 2019
1. Introduction

The 2019 money laundering (ML) and terrorist financing (TF) national risk assessment (NRA) comes at an important time prior to Lebanon’s second Mutual Evaluation. However, assessing risk on a country-wide scale is not a new concept for Lebanon, as the first NRA was concluded towards the end of 2014. Several risk mitigation measures were taken following the year-end 2014 NRA, and major changes occurred in areas covering legislative, regulatory, supervisory, and law enforcement.

A new AML/CFT law was adopted in 2015 to widen the categories of predicate crimes so as to cover all 21 predicate offences as per the Financial Action Task Force (FATF) standards and to include additional categories of reporting entities, namely lawyers, notaries and certified accountants. Furthermore, a law on the cross-border transportation of money was adopted, along with amendments to the penal code to strengthen the TF offence. Numerous AML/CFT regulations were issued to reporting entities, and targeted financial sanctions (TFS) mechanisms were implemented for United Nations Security Council Resolutions (UNSCRs) 1267 and 1373, and their successor resolutions. Improvements to risk-based AML/CFT supervision were made, and following a series of joint training events, information sharing and cooperation between the Financial Intelligence Unit (FIU) and law enforcement authorities (LEAs) was strengthened. Such mitigating measures, as well as more recent ones being taken as a result of the 2019 NRA to improve supervision, enforcement, monitoring and compliance, including the issuance of additional regulations on the beneficial owner (BO) beef up our AML/CTF regime, better position us to combat illicit financial flows, and effectively mitigate ML/TF risks.

In mid-2019, Lebanon’s second NRA was concluded. The 2019 NRA was backed by high level political commitment and was led by the Special Investigation Commission (SIC), Lebanon’s FIU. The SIC, supported by senior level involvement engaged stakeholders from both the public and private sector, as well as the two national committees for AML and CFT that encompass, alongside the SIC, a number of authorities (regulatory, supervisory, law enforcement and judicial). Private sector reporting entities from the financial sector as well as Designated Non-Financial Businesses & Professions (DNFBPs) were engaged for input and to obtain experts’ opinions, as well as to gather needed information.

According to the 2019 NRA, some of the risks previously highlighted in the year-end 2014 NRA materialized, particularly in relation to the spillover effects from the neighboring conflict which resulted in an increase in terrorist and TF activities. The 2019 NRA ascertains that delays in implementing a number of risk mitigating measures concerning some previously identified high ML risk areas has resulted in a worsening situation, particularly with respect to corruption. While measures such as the implementation of the Foreign Account Tax Compliance Act (FATCA) and the OECD-Global Forum requirements mitigate risks associated with foreign origin tax crimes, money laundering risks associated with local tax evasion remained high. Other ML risks are of various risk levels, and some types of reporting entities and legal persons are inherently more vulnerable than others.
2. Methodology

The purpose of the 2019 NRA is to assess the risks facing Lebanon by identifying ML/TF threats and vulnerabilities, including gaps in the AML/CFT regime. The NRA aims to improve the said regime by shaping policy, legislative/regulatory actions, and priorities for operational decisions including resource allocation of supervisors, law enforcement and judicial authorities towards higher risk areas. It also aims to deepen their understanding of predicate crimes as well as maintain among them a common understanding of ML/TF risks. The NRA is also crucial and informative for reporting entities in the sense that it contributes to their understanding of threats and vulnerabilities, and feeds into their own risk assessments, mitigation efforts and overall implementation of the risk-based approach (RBA).

The methodology for the 2019 NRA takes reference from the FATF guidance on this topic and its three stages of identification of threats / vulnerabilities, analysis and evaluation. In line with this guidance, risk in the ML/TF context was considered as a function of three factors: threats, vulnerabilities and consequences.

Identification of Threats:
ML/TF threats are of domestic and foreign origin. They arise from predicate offences and related funds, terrorist activity and related financing, as well as from associated offenders.

Threats were identified by collecting quantitative data on yearly developments in predicate crimes under AML/CFT law no. 44 in order to decide whether or not proceeds might be laundered. Data on estimated proceeds of crime from the FIU, LEAs, and government authorities in addition to growth in ML/TF cases of local/foreign origin were reviewed, along with open source information. The work done included among other things information obtained via surveys, in addition to the review of Suspicious Transaction Reports (STRs), Requests of Assistance (ROAs), Spontaneous Disclosures (SDs), ML/TF cases & typologies, national list designations in connection with terrorism / TF, prosecutions, and convictions. Qualitative data and opinions from experts were also sought, including when quantitative data was unavailable or believed to be either incomplete, inaccurate, or not fully reliable.

Identification of Vulnerabilities:
Vulnerabilities are weaknesses in the AML/CFT regime that threats can exploit. In a broad context, they are usually associated with the main characteristics of a country such as the level of corruption, weak government reach in certain areas, size of the informal economy, the prevalence level of organized crime, capacities of AML/CFT authorities in addition to reporting entities’ AML/CFT systems/controls, and the attractiveness of products/services for ML/TF purposes.

Vulnerabilities were examined in the context of the Political, Economic, Social, Technological, Environmental/Geographical & Legislative factors (PESTEL) that ultimately affect Lebanon’s AML/CFT regime. Financial sector reporting entities and DNFBPs’ size/economic significance, products/services offered, prevalence of local and foreign origin ML/TF cases, customer base, geographic reach or presence, as well as delivery channels were reviewed. Qualitative data were also reviewed from the last mutual evaluation report and follow up reports, supervisory reports, reporting entities’ own risk assessments, and from the FIU, law enforcement and prosecution authorities. Legal persons and arrangements, including Non-Profit Organizations (NPOs) were also covered.
Analysis:
The data and information gathered under ML/TF threats and vulnerabilities were analyzed in light of the consequences (impacts/harms) they hold for Lebanon’s: (1) economy/financial system, (2) security/reputation and (3) society at large.

In the analysis phase, a better understanding of the nature and sources of the identified ML/TF risks was achieved, and consideration was given to the probability/likelihood of risks materializing before and after applying risk mitigation measures. This was followed by benchmarking and giving a relative value (risk score), ranging from low risk to high risk.

Evaluation:
The identified ML/TF risks were evaluated, and decisions were reached on priorities with respect to additional mitigation measures needed, which were consequently laid out in an action plan.
3. ML/TF Threats

The threat from domestic low level street crimes such as murder and petty theft were deemed unimportant in the ML/TF context in spite an increase in their numbers, which is associated with the spillover effects from the neighboring conflict and with a worsening economic situation. The threat associated with air and maritime piracy was also deemed unimportant.

3.1 Money Laundering Threats

Corruption is an impediment to the economy, to the business environment, and to competitiveness. It is also a major obstacle for foreign direct investment. Government contracts and public procurements can be awarded based on favoritism to connected companies and by mutual agreement with disregard to tenders. Their size represents an opportunity for corrupt wrongdoers. Tax evasion on the other hand covers areas of income tax, property registration taxes, and taxes on international trade (customs/excise) as well as value-added tax (VAT). The structural flaws in the taxation network itself and citizens’ practice of evading taxes result in losses of urgently needed funds that can be put to good use, and to benefit the public.

ML threats were identified to arise mainly from local origin criminal activity associated with corruption, tax evasion, and drug trafficking that generate significant illicit proceeds, as well as cybercrime fraud (mainly business e-mail compromise), the occurrence of which increased since the previous NRA. Other ML threats are associated with forgery, fraud and embezzlement of private funds that are relatively more reported, as well as with smuggling and counterfeited goods. Despite the lack of thorough reliable statistics on human trafficking & migrant smuggling, they remain threats based on intelligence reports and unavoidable scenarios associated with the refugees’ situations. Local capital markets are underdeveloped, a limited number of publicly listed companies exist, and large-scale securities fraud don’t exist. The limited number of ML cases investigated over the past few years in connection with insider trading were of foreign origin and did not involve sophisticated ML schemes and methods such as the creation of shell or front companies. The money laundering threat is low in connection with a number of other predicate crimes such as kidnapping for ransom and car thefts, and is medium-low for illicit arms trafficking.

ML threats originate from both predicate crimes committed in Lebanon (local origin predicate crimes) and abroad (foreign origin predicate crimes). ML threats are associated mainly with persons, rather than with professional money launderers, gangs or organized crime groups. Relatively speaking, ML activity is not overly large scale and several methods are used that can be characterized as not being complex or sophisticated, such as cash-based money laundering and commingling of illicit cash with funds from legitimate businesses. More complex methods can be associated with corruption and the misuse of legal persons, as well as tax evasion that includes methods such as manipulating shipping documents and presenting forged invoicing, in addition to tax fraud schemes covering illegal tax recovery (VAT refund). While due to fraud, bank accounts might receive transfers originating from the tax authority in connection with illegal tax recovery, corruption related funds do not necessarily need to be deposited in offenders’ own bank accounts and can be placed in accounts of trusted third parties, associates or relatives, not to mention being used to purchase high value items or assets.
3.2 Terrorist Financing Threats

The threat of terrorism from outside as well as inside the borders was considered so as to have a better understanding of the general terrorism environment and how it drives and influences TF activities. The TF threat increased in recent years after the fall of major cities in Iraq and Syria to terrorists. Terrorist groups such as Daesh (ISIL) began focusing on Lebanon to spread ideology, form sleeper cells and recruit fighters, while taking advantage of the refugees’ situation, sectarianism, and socioeconomic factors.

Combating terrorism and TF increasingly became top national priorities after Lebanon became a high-priority target for terrorist attacks and fell victim to many such attacks, including via car bombings and suicide missions. Terrorist attacks were mainly associated with the neighbouring conflict and with terrorist groups that emerged on our border and threatened our security and stability. Post 2014, the dismantling of several terrorist cells by law enforcement, and the implementation of the government’s security plan resulted in some improvements in the overall situation (15 terrorist attacks in 2014). The situation drastically improved after the 2017 military offensive cleaned up the eastern border from terrorist elements, and as a result of improvements made to interagency coordination as well as to pre-emptive operations carried out by LEAs (1 terrorist attack in 2018). Terrorist groups, namely ISIL, Jabhat Al-Nusra, Al-Qaeda, Fateh El Islam, Jund Al-sham, Ahrar Al-Sham and foreign terrorist fighters (FTFs) carried out attacks in Lebanon and presented the greatest threat. Multiple smaller offshoot terrorist groups that emerged during the ISIL and Al-Nusra occupation of small parts of mountainous areas in the Bekaa valley also presented threats. Threats are also associated with FTF returnees, violent extremism, and the overall exploitable refugees’ situation.

Terrorist financing and the assessed activities of terrorist groups/persons in connection with raising, collecting, storing and moving funds for internal or external use revealed that TF was mainly to carry out terrorist attacks in Lebanon. While some TF investigations/prosecutions involved cash from illegitimate sources relating to criminal activity associated with illicit arms trafficking, smuggling and ransom money, TF was primarily associated with cash from terrorist groups based in the conflict zone as well as cash from self-financing. TF activities also included the provision of material support such as food, shelter, medical supplies, and oil for heating, while a few stolen cars ended up being used in terrorist attacks. In addition, the misuse of a few NPOs for TF purposes included instances where some of the aid (goods & food) distributed by them to refugees in certain areas were later channeled without their knowledge to terrorists entrenched in mountainous areas on the Syrian-Lebanese border. A variety of methods were used to move funds, including smuggling cash across the border and inside the country to terrorists, illegal/unlicensed hawala activities, money remittances and to a lesser extent bank transactions.

The TF threat is high and is from both foreign and local origin sources. Nevertheless, TF activities are not large-scale, not complex or sophisticated and did not require a high level of knowledge or skill. They also did not require extensive resources and capabilities such as a wide network of supporters. Cash remains the favored method for terrorists to raise and move funds. Cash smuggled to finance local terrorist attacks were of modest values, and difficult to detect. Cash for TF purposes were mainly used to purchase explosives, arms and ammunition, and also to make payments to terrorist, as well as for logistical support. The TF threat from external sources originated mainly from terrorist groups such as ISIL and AL-Nusra that targeted Lebanon from their stronghold abroad. This at times was made easier by sympathizers, and extremists hiding or taking cover in refugee camps and among the large refugees’ communities. The threat is low with respect to TF originating from Lebanon to support overseas terrorist activities, and is primarily associated with the actions of FTFs that left Lebanon to join ISIL and other terrorist groups in the conflict zone, some of which are expected to return (FTF returnees).
<table>
<thead>
<tr>
<th>Law No. 44 ML / TF Predicate Offenses - Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
</tr>
<tr>
<td>Tax Evasion</td>
</tr>
<tr>
<td>Illicit Drug Trafficking</td>
</tr>
<tr>
<td>Fraud – Cybercrime</td>
</tr>
<tr>
<td>Smuggling &amp; Counterfeiting of Goods</td>
</tr>
<tr>
<td>Forgery, Fraud &amp; Embezzlement of Private Funds</td>
</tr>
<tr>
<td>Trafficking in Human Beings &amp; Migrant Smuggling</td>
</tr>
<tr>
<td>Insider Trading</td>
</tr>
<tr>
<td>Illicit Arms Trafficking</td>
</tr>
<tr>
<td>Organized Crimes - Car Thefts</td>
</tr>
<tr>
<td>Environmental Crimes</td>
</tr>
<tr>
<td>Kidnapping for Ransom</td>
</tr>
<tr>
<td>Offence against Ethics &amp; Public Decency (Illegal Prostitution)</td>
</tr>
<tr>
<td>Extortion</td>
</tr>
<tr>
<td>Sexual Exploitation</td>
</tr>
<tr>
<td>Terrorism &amp; Terrorist Financing</td>
</tr>
</tbody>
</table>
4. Inherent ML/TF Vulnerabilities

The legal, regulatory and supervisory framework for AML/CFT is robust and comprehensive, with room for improvement. Law enforcement and judicial authorities’ resources are affected with Lebanon’s geographic proximity to the neighboring conflict, and with the presence of large numbers of refugees with economic/social ties with jurisdictions witnessing terrorism and instability. In spite of the resource constraints, continuous efforts are exerted to close illegal border crossings and to strengthen government control over remote areas like where cannabis is grown.

The financial sector is modest in size in comparison to global or regional financial centers that attract money from across the world. However, existing inherent vulnerabilities associated with having an open economy with significant international trade, a developed banking/financial system and the wide use of cash, in addition to the presence of an informal economy (not reported for tax purposes) can be exploited by ML/TF offenders. The largest component of the financial sector is banks, their size alone exceeds 95% of the entire financial sector and they offer products and services that can be misused. DNFBPs are engaged in numerous economic activities and also offer products and services that can be misused, however, some namely art and antique dealers are insignificant. Virtual assets and activities or operations of Virtual Assets Service Providers (VASPs) are also insignificant given existing prohibitions to have such dealings. Certain types of legal persons, including NPOs can also be vulnerable to potential misuse.

5. Financial Sector and DNFBPs

5.1 Financial Sector

**BANKS**

The banking sector is comprised of commercial banks, investment banks (owned mainly by large local commercial banks), and a few Islamic banks. Some banks have overseas presence in the form of branch, subsidiary or representative office, and a few commercial banks are dominant in terms of overall market share. Commercial banks are of great economic significance and are well integrated with other sectors. The vulnerability of products/services offered vary between commercial banks and investment banks with the latter being much less vulnerable to TF risks. Banks deal with a large diverse customer base including high risk customers, and offer a range of vulnerable products and services provided through various delivery channels, such as cash operations, and operations for accounts of legal persons, including offshore companies where the beneficial owner and the source of funds are more difficult to identify or verify, as well as companies with public sector dealings, not to mention instances of non face-to-face dealings or dealings through third parties. Banks are the only deposit taking institutions and are thus inherently more vulnerable to ML/TF risks given also their size, transaction volumes, cross border nature of transactions, speed and frequency of operations, as well as the possibility of gatekeepers being used to execute transactions.
MONEY DEALERS

The main business of money dealers (MDs) is the purchase and sale of foreign currencies in exchange for other foreign currencies or Lebanese Pounds. The majority of money dealers are licensed as type “B”, are small in size with modest transaction volumes and are not permitted to engage in operations involving transfers or hawala. A smaller number of MDs are licensed as type “A”, of which a few carry out hawala operations, while a very limited few are licensed to ship banknotes. MDs geographically cover all Lebanon and their operations are associated with the prevalence of cash transactions, currency exchange, wire transfers and hawala operations. Their products and services are offered across the country to transient customers and cash generating businesses. The level of vulnerability to ML/TF risks differs between type “B” and type “A” MDs, with the latter being inherently more vulnerable to ML/TF risks, especially the sub-set offering hawala operations.

MONEY REMITTANCE COMPANIES

A number of licensed money remittance companies are currently non-operational. Three companies dominate the market in terms of volume of remittances and local geographic coverage by their sub-agents. Money remittance companies controlling the highest percentage of market share are associated with well-regulated international remittance companies based abroad, and execute remittances using their platform or network. The remittances corridors are in line with the diaspora and foreign labor work force in Lebanon. Nevertheless, identifying the source of small funds and their potential end use are challenges for money remittance companies. International typologies on the universal TF misuse of money remittance companies by FTFs, the methods of transferring proceeds of crime in small amounts from numerous originators to a single beneficiary, along with the prevalence of cash transactions and the ease in which cross border funds can be moved are inherent worldwide characteristics of the sector that contribute to making it more vulnerable to ML/TF risks.

OTHER FINANCIAL SECTOR ENTITIES

Financial Institutions, Financial Intermediaries (Brokerage Firms) and Specialized Lending Entities (Comptoirs) represent a small segment of the financial sector and are less vulnerable to ML/TF risks. They are not deposit taking institutions and are very modest in size/volumes of transactions executed. As for products and services offered by them, many brokerage firms are just providing advisory/consulting services, while financial institutions and comptoirs are mainly focused on offering small loan products. Insurance companies are also less vulnerable to ML/TF risks, especially given the modest value of insurance premiums paid against life policies with investment features that allow the option to transfer, move and store money. As for leasing companies, none existed during the last several years.
5.2 Designated Non-Financial Businesses & Professions

**JEWELERS**
Jewelers (Dealers in Precious Metals and Stones) operate all over the country, and most are small businesses with modest operations. A small number of jewelers are considered large businesses and command the largest market share in terms of value of transactions. Jewelers offer products vulnerable to misuse that are accessible to a wide range of customers and carry out considerable transactions in cash. Their operating nature allows for cash transactions against high-value commodities such as gold or diamonds to be carried out by transit customers with a degree of privacy. Jewelers’ products also store value and can be transported and exchanged for similar amounts thus contributing to their vulnerability.

**REAL ESTATE DEALERS & AGENTS**
The value of built and unbuilt property transactions has been on the decline, and the real estate sector has been in recession for several years, with annual drops in prices and limited demand on supplied property. The relative resilience in prices can be attributed to Banque du Liban (BDL) subsidized lending and incentives schemes. Players involved in real estate transactions are of various sizes and include the developer or seller, the investor or buyer and brokers, as well as the bank providing the loan to either sides of the transaction. Real estate transactions carried out mainly involve banks that are subject to robust AML/CFT requirements and supervision. Other parties involved in real estate transactions are notaries and possibly lawyers in a limited number of transactions.

The real estate sector typically involves large-value transactions and assets that store value, nevertheless restrictions in Lebanon on foreigners to own real estate along with the prevalence of subsidized loans that are subject to tough vetting requirements are dominant risk mitigation features of the real estate sector. Illicit funds might be invested in real estate to conceal its origin or the beneficial owner. As such, the sector can be used as a conduit for ML, but rarely for TF. Real estate dealers & agents are involved in a modest share of the overall real estate transactions.

**CASINO DU LIBAN**
Casino du Liban (CDL) is a Lebanese shareholding company that has the exclusive privilege and right to administer gambling games in Lebanon. The contract with the Ministry of Finance (MOF) entitles the latter to receive 50% of all slot and casino gaming wins (the amount retained by the casino from the amount spent by customers). The largest shareholder is Intra Investment Co., in which BDL and the Government are majority owners. CDL visitors and revenues have been on the decline mainly as a result of the downturn in the economic situation and drop in number of tourists. CDL does not offer clients the ability to receive or transfer funds electronically and does not issue third party checks. When cash exceeding a certain amount is exchanged for chips, CDL returns first the same amount in cash before paying out any winnings. The ownership structure and restrictions on the mode of operations, in addition to not offering online gambling services contribute to CDL being the least vulnerable among DNFBPs.
CERTIFIED PUBLIC ACCOUNTANTS

The Lebanese Association of Certified Public Accountants (LACPA) is a self-regulatory body encompassing a sizeable number of practitioners operating across the country. By virtue of law, Certified Public Accountants (CPAs) are not allowed to establish companies for their clients and are prohibited from combining their profession with commercial professions. Their work is mostly of domestic nature and does not involve anonymity, including when transacting on behalf of customers. Public Accountants have specialized expertise in financial and tax matters that can be exploited by clients of varying risk levels (high net worth individuals, cash intensive businesses, etc.). They can also encounter in their day-to-day work shell companies, over or under invoicing activities, fake invoicing, as well as real estate transactions involving undervaluation which contribute to their vulnerability.

LAWYERS

A vibrant community of sophisticated professional lawyers work across the country. They have two bar associations in Beirut and Tripoli that are self-regulatory bodies. Registering in either is a prerequisite to practice this profession. The services rendered by some lawyers include preparing for or engaging in transactions on behalf of customers, such as establishing companies, buying and selling real estate or businesses; managing funds or other assets, and establishing or managing bank accounts. Lawyers mainly know their customers first hand. They are generally aware of their customers’ risk profiles and of the risks associated with carrying out third party transactions, establishing, operating or managing legal persons whereby wrongdoers might use them in ML activities and misuse lawyers’ expertise to conceal their identity, the source of funds and the BO. Their sought-after expertise and role as gatekeepers in accessing the financial sector is an inherent vulnerability associated with this profession.

NOTARIES

The authority overseeing notaries is the Ministry of Justice (MOJ). Notaries according to their governing law are public officers authorized within their competence to perform duties prescribed in the said law. They mainly handle the authentication of documents to be made official and receive fees due to the state’s treasury. Their work includes verifying the identity of persons when issuing official documents and for establishing companies, in addition to certifying general assembly meetings, extra ordinary assembly meetings as well as board meetings that require filing with the commercial register. They also prepare power of attorneys, authenticate formal contracts for real-estate agreements and maintain related copies and documents, etc. Notaries might come across suspicion when handling contracts/transactions and when authenticating documents to be made official including for the establishment of legal persons. They also might come across sales contracts with undervalued or fictitious property pricing resulting in tax evasion which contributes to them being the most vulnerable among DNFBPs.
Some types of financial sector reporting entities and financial products/services are more vulnerable than others to ML/TF risks. Banks - the only deposit taking institutions, given the prevalence of ML/TF cases, their size, volume of transactions, geographic reach including exposure to high risk jurisdictions, wide range of products/services offered, delivery channels and their large diverse customer base that includes high risk customers are inherently the most vulnerable. Money remittance companies and type “A” money dealers are also high in terms of vulnerability to ML/TF risks (type “B” money dealers are medium). The modest size of other financial sector reporting entities (financial institutions, brokerage firms, insurance companies and comptoirs), the products/services offered by them and the regulatory restrictions in place contribute to making them less vulnerable to ML/TF risks.

Notaries in comparison to other DNFBPs are the most vulnerable to some high risk ML offences, particularly when preparing and/or carrying out real estate transactions and when establishing companies. Real estate dealers/agents, lawyers and certified public accountants are rated medium in terms of vulnerability to ML risks while jewelers are rated as medium - low. CDL was deemed the least vulnerable. In terms of vulnerability to TF risks, all DNFBPs are generally low.

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Sub-Sector</th>
<th>Vulnerable to ML/TF Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Banks</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Remittance Companies</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Dealers “Type A”</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Dealers “Type B”</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Financial Institutions</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Financial Intermediaries (Brokerage Firms)</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Specialized Lending Entities (Comptoirs)</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Insurance Companies</td>
<td>Low</td>
</tr>
<tr>
<td>DNFBPs</td>
<td>Real Estate Dealers &amp; Agents</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Jewelers (Dealers in precious metals &amp; stones)</td>
<td>Medium - Low</td>
</tr>
<tr>
<td></td>
<td>Casino du Liban</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Notaries</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Lawyers</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Certified Public Accountants</td>
<td>Medium</td>
</tr>
</tbody>
</table>
6. Legal Persons & Arrangements
and Non-Profit Organizations

6.1 Legal Persons & Arrangements

The role of legal persons in the economy is widespread and sizable. They are in the thousands and are engaged in a wide range of economic activity. Many do not have employees because they are either inactive, small neighborhood shops run by owners, offshore companies not permitted to operate in Lebanon or legal persons established to own real estate.

Legal persons including foreign companies with place of business in Lebanon must be registered with the Commercial Register (CR), with the exception of cooperatives as well as NPOs that are subject to other registration requirements. The Lebanese Code of Commerce (CoC) allows for different types of legal persons, and mandatory requirements are stipulated under commercial, tax and financial legislations. Any changes in registered information, including in the identity of the owners, managers, directors and the beneficial owners have to be submitted to the commercial register. Furthermore, according to the CoC, legal persons must at all times engage a Lebanese certified accountant (a member of LACPA) and a Lebanese lawyer (a member in any of the two Bar Associations), until the company ceases to exist. With a few exceptions, all legal persons must legally have a bank account. BO information on legal persons is also available through the AML/CFT framework under which banks and other reporting entities carry out Customer Due Diligence (CDD) measures and also through the tax framework that requires providing BO information to the tax authority (in tax returns). The commercial register is accessible to the public and contains detailed information on legal persons. Files are archived for 10 years after liquidation. With respect to cooperatives, they are subject to registration and supervision by the Directorate General of Cooperatives at the Ministry of Agriculture, and are mainly concentrated in the agricultural sector.

As for legal arrangements, the concept of trust does not exist in Lebanon, foreign trusts are not recognized and Lebanon is not a party to the Hague Convention on trusts. Nevertheless, it is possible for a foreign trust to have a bank account in Lebanon, noting that in such circumstances they are subjected to AML obligations including CDD measures and BO identification carried out by the bank. Fiduciary contracts/accounts on the other hand are maintained exclusively by banks and financial institutions and are subject to AML/CFT obligations. Lebanese legislations also allow for waqfs that are associated with religious sects.

In spite the low level of foreign ownership within legal persons, certain vulnerabilities and features of legal persons might be exploited for ML. Examples can include those having complex ownership structures, such as holding companies where the ultimate BO is harder to determine, and the BO as well as illicit proceeds can be disguised, in addition to those having public sector dealings (government contracts & public procurements). The characteristics of offshore companies having international operations and businesses makes them more vulnerable to ML risks than others. Legal persons and arrangements are generally low risk for TF.
<table>
<thead>
<tr>
<th>Type of Legal Persons (Companies)</th>
<th>% of Legal Persons (As of end March 2019)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Liability Company</td>
<td>52.81%</td>
</tr>
<tr>
<td>Joint Stock Company</td>
<td>23.6%</td>
</tr>
<tr>
<td>Partnership limited by shares</td>
<td>0.01%</td>
</tr>
<tr>
<td>General Partnership</td>
<td>1.79%</td>
</tr>
<tr>
<td>Simple Limited Partnership</td>
<td>10.1%</td>
</tr>
<tr>
<td>Civil Companies</td>
<td>0.4%</td>
</tr>
<tr>
<td>Offshore Companies</td>
<td>7.1%</td>
</tr>
<tr>
<td>Holding Companies</td>
<td>3.3%</td>
</tr>
<tr>
<td>Foreign companies (Branch)</td>
<td>0.69%</td>
</tr>
<tr>
<td>Foreign companies (Representative Office)</td>
<td>0.2%</td>
</tr>
</tbody>
</table>

### 6.2 Non-Profit Organizations

For many decades, charities, the work of civil society and philanthropy have eased the impact of poverty on many, especially in rural areas. Limited resources and ineffective underperforming official programs have historically resulted in growth in charities and the non-profit sector, which first grew during the civil war. The recent growth over the last few years in this sector can be attributed to the neighboring crisis and to the refugees’ situation that brought along enormous challenges with respect to socioeconomic factors.

The Ministry of Interior & Municipalities - Department of Politics & Electoral Affairs, Office of Politics, Parties & Associations is responsible for the “Certificate of Knowledge” needed to complete the establishment process for NPOs. Thousands of NPOs exist in Lebanon covering civil/cultural matters, human, women, children and prisoner rights, in addition to others involved in education, environmental and health care issues including cancer treatments and drug rehabilitation. NPOs involved in social development, public benefit, popularity and electoral advantages established by public figures also exist. The government’s annual contribution to this sector via some ministries is significant and is mainly channeled through NPOs towards disabled persons, elderly people, orphans, and the underprivileged. The sub-set of NPOs which fall into the FATF definition is relatively smaller.

Lebanon’s non-profit sector is domestically oriented. NPOs have access to a wide range of funding which comes from the rich community, international donors including foreign governments, as well as from individual contributions and religious duties, etc. This enables NPOs to reach poor communities in society and those in need. Non-profits with international funding such as those dedicated to Palestinians residing in refugee camps and to Syrian refugees also operate in Lebanon.

Pursuant to the ML & TF NRA, the Ministry of Interior and Municipalities published on its website a guidance on preventing the misuse of NPOs for terrorism financing. This guidance identifies the following types of NPOs, which by virtue of their activities and characteristics, may be at a higher risk of being misused for TF purposes:

- NPOs newly established, with limited expertise in programs or funding
- NPOs concerned with refugees and displaced persons
- NPOs using names implying religious affiliations, but are not so
- NPOs operating in border areas adjacent to a conflict zone

Some NPOs are more vulnerable to TF misuse, and there have been cases in which they were exploited for TF purposes. Donations to NPOs in cash makes identifying the source of funds at times difficult. The disbursement and usage of cash especially once partner organizations, intermediaries, or representatives are involved makes identifying the final usage of cash also difficult. Terrorists might infiltrate or take shelter among the existing large number of refugees’ communities. This, along with NPOs’ having operations in proximity to the neighboring conflict are challenges to NPOs. NPOs may encounter acts of abuse including diversion of foreign aid, and abuse of programs such as when aid (goods & food) are unknowingly rechanneled.
7. ML/TF Risks

It is crucial for both local authorities and the private sector to understand the ML & TF risks they face. Predicate crimes under AML/CFT Law no. 44 that were assessed took into consideration domestic and foreign origin ML/TF threats. With the exception of cybercrimes and insider trading, ML risks are mainly of local origin predicate crimes, and to a lesser extent as a result of foreign origin predicate crimes. The higher risk money laundering crimes are associated with corruption, tax evasion, and illicit drug trafficking resulting mainly from local predicate offences, as well as cybercrimes (mainly business e-mail compromise). Money laundering risks associated with other offences such as smuggling also exist, and are of various levels.

Terrorist groups such as ISIL and Al-Nusra present the biggest threat to Lebanon. The TF risk is high, it arises from both local and foreign origin sources, and cash remains the favored method for terrorists to raise and move funds, along with illegal/unlicensed hawala activity, which is the primary focus of LEAs and is being expeditiously eradicated.

Some reporting entities such as banks, category “A” money dealers primarily those offering hawala operations, and money remittance companies are inherently more vulnerable than others to the possible occurrence of high risk ML/TF crimes through them, and to the possible misuse of products and services offered. They must apply the RBA and be vigilant when executing transactions particulary when carrying out cash operations, and operations involving accounts of legal persons, especially offshore companies where the beneficial owner and the source of funds are more difficult to identify, in addition to non face-to-face dealings or dealings through third parties. Notaries are more vulnerable than other DNFBPs to the possible misuse of products or services offered, especially when preparing and/or carrying out real estate transactions and when establishing companies. DNFBPs as well as certain types of legal persons and NPOs that are vulnerable to possible misuse, must also be vigilant and adopt controls that are commensurate with risks.
8. Risk Mitigation Measures – AML/CFT Regime

Lebanon has a comprehensive AML/CFT regime in line with FATF standards that is assessed by the Middle East & North Africa Financial Action Task Force (MENAFATF) and is subject to its follow-up process. At the center of the AML/CFT regime is the SIC, the country’s multi-function financial intelligence unit and other AML/CFT stakeholders from both the public and private sectors. The AML/CFT regime rests on a number of pillars: (1) legal & regulatory, (2) domestic & international cooperation, (3) financial sector reporting entities & DNFBPs, and (4) AML/CFT supervision.

**LEGAL AND REGULATORY**

The legislative framework is based primarily on AML/CFT law no. 44 of 2015 and other legislations, including the cross-border transportation of money law and the penal code which criminalizes TF including the financing of FTF activities in accordance with UNSCR 2178. The Tax procedure law as well as the Code of Commerce place BO requirements for legal persons, and detailed AML/CFT regulations are issued to all reporting entities by BDL and the SIC. The AML/CFT law identifies financial sector institutions and DNFBPs as reporting entities including notaries, lawyers, and accountants, as well as ML/TF predicate offences, which cover crime categories as per FATF standards. It also sets requirements including for CDD measures, beneficial ownership, record keeping and reporting suspicion. The said law establishes the FIU and its powers which include freezing powers, and also designates the authorities responsible for supervision of financial sector reporting entities and DNFBPs and for issuing regulations. The AML/CFT law also sets the legal basis for mechanisms to implement targeted financial sanctions related to terrorism/TF with respect to UNSCRs 1267 & 1373, and allows for confiscation of assets and the sharing of confiscated assets with concerned countries. While the formal mutual legal assistance (MLA) channel is managed by the MOJ and the General Prosecutor, ML/TF information disseminated or shared by the SIC can be used to support local as well as foreign investigations and prosecutions. The AML/CFT law defines the relation between the SIC and the General Prosecutor, and the latter also oversees parallel financial ML/TF investigations and ensures that ML/TF crimes are prosecuted.

**DOMESTIC AND INTERNATIONAL COOPERATION**

The domestic cooperation in place between the SIC and concerned national agencies is essential to maintain an effective AML/CFT regime and to protect the integrity of the financial and non-financial sectors. Cooperation takes many forms, including prioritizing ML/TF requests of assistance, operational capacity building through joint training programs, and inter-agency work on emerging trends such as on cybercrimes and on TF. Other forms of domestic cooperation take place via the two national committees on AML and CFT that encompass several national agencies.

The SIC, the General Prosecutor, the ISF and a number of other LEAs including customs which enforces law no. 42 on the cross-border transportation of money are regime partners. Their cooperation on matters of intelligence gathering and ML/TF investigations is effective and was pivotal in disrupting numerous money laundering and terrorist financing activities. The Ministry of Interior & Municipalities has oversight with respect to NPOs and ensures that they are not being misused to finance terrorism. Domestic cooperation among various agencies covered this area and reached desirable outcomes. On tax evasion, the Ministry of Finance and the SIC complement each other’s work on matters such as OECD-Global Forum requirements. Other forms of cooperation exist, such as Customs and SIC work on the mechanism to implement law No. 42, and the SIC having direct access to cross border declaration / disclosure reports and seizures.
The high-level commitment to improve cooperation to combat TF led several intelligence agencies to establish within their respective agencies branches that focus on TF investigations. This commitment also resulted in aligning the TF offence, preventative measures, and TFS with international standards. As such, domestic cooperation on terrorist designations and freezing of terrorist assets is robust. The National Committee on Suppressing Terrorism Financing has put in place TFS mechanisms for the implementation of UNSCR 1267 & UNSCR 1373. Regulations on the “freezing without delay” with respect to UNSCR 1267 were issued by BDL and the SIC. The first designations in accordance with UNSCR 1373 were made in December 2015, and as of end-March 2019, fifty-five listings are on the terrorism/TF national list. Existing domestic cooperation on CFT matters, along with the capacity levels of authorities, supervisors and reporting entities including awareness of how products/services may be exploited for TF are current effective mitigating measures.

International cooperation is vital for ML/TF investigations given the interconnection of world economies and financial systems, as well as the broader use of new technologies that allow for the instant movement of funds around the world. Effective domestic cooperation affects international cooperation to a great extent. One area of direct impact is the quality, usefulness and timeliness of information exchanged between FIUs. Lebanon’s SIC is a member of the Egmont Group of FIUs since 2003, with its Secretary General having served as the Egmont Committee vice chair and twice as the Middle East and North Africa (MENA) region representative. The SIC actively participates in EG work such as on the ISIL project and others. Reach out efforts over the years in the form of technical assistance and other engagements were carried out by the SIC on its own or in partnership with others, and have resulted in bringing several FIUs from our region to Egmont Group membership.

Lebanon is a founding member of MENAFATF and an active participant in its work. Since its founding back in 2004, Lebanon has assumed twice the presidency of this body. As of end 2018, several SIC staff participated as assessors in eleven mutual evaluation missions for MENA countries, and more are already scheduled. The SIC has also worked with MENAFATF on a number of initiatives to improve the AML/CFT capacity of countries, including by providing training and sharing expertise on the ML & TF NRA process. More recent initiatives brought together in Beirut anti-corruption agencies and FIUs from the MENA region under the banner of the first Arab forum of anti-corruption agencies and FIUs. The aim was to improve the fight against corruption and promote cooperation between such agencies. Lebanon through the SIC continues to participate in meetings of MENAFATF, Egmont Group and the FATF, and remains actively involved in related working groups and projects. Lebanon is also an active partner in the fight against ISIL and participates in the work of the Counter ISIL Financing Group (CIFG) within the Global Coalition against Daesh.

An effective AML/CFT regime when it comes to international cooperation is best measured by the ability to confiscate and repatriate illicit proceeds related to foreign predicate crimes. In a number of cases Lebanon has repatriated funds, and Lebanon’s SIC was recognized for investigating, freezing, and successfully repatriating corruption related funds by the World Bank-UNODC Stolen Asset Recovery Initiative (STAR Award of Excellence). Furthermore, effective international cooperation is measured by information exchanged via the FIU to FIU channel, other forms of cooperation, and via the more formal MLA channel, all of which are marked with high response rates containing quality information.
The financial sector is regulated by BDL, except for insurance companies which are regulated by the Ministry of Economy & Trade, and for financial brokerage firms which are regulated by the Capital Markets Authority (CMA) that also limits the licensing of mutual funds – collective investment schemes to just banks or certain types of financial sector reporting entities. All three authorities have adopted tough licensing requirements and have implemented strong oversight measures. The SIC, aside from being the country’s FIU, is also the main AML/CFT supervisory authority for all financial sector reporting entities and a number of DNFBPs, while others, namely notaries, lawyers and accountants are regulated and supervised by the MOJ and by their respective syndicates.

Banks & other reporting entities are at the forefront in the fight against ML and TF. Internal controls and systems they adopt to monitor, detect and report suspicious transactions are at the core of the AML/CFT regime. The effective implementation of CDD measures, record keeping requirements, BO identification and the RBA by financial sector reporting entities & DNFBPs, in addition to other regulatory requirements serve as a barrier in preventing offenders from misusing these entities, placing illicit proceeds into the financial system and from exploiting it to finance terrorism. As per FATF standards, all categories of reporting entities are covered under AML/CFT law no. 44, including notaries, lawyers and accountants. As such, there are hundreds of reporting entities in Lebanon. Banks, given their size and wide range of products/services in comparison to other financial sector reporting entities, are considered the main component of the financial sector and the backbone of the economy. They enjoy robust AML/CFT controls including for sanctions screening & evasion.

Aside from being the country’s FIU, the SIC is also the main AML/CFT supervisory authority. The SIC Compliance Unit supervises banks and other financial sector reporting entities as well as a number of DNFBPs to ensure compliance with prevailing AML/CFT regulations. In this regard, it carries out onsite examinations to assess the effectiveness of AML/CFT compliance programs, CDD measures and controls adopted to monitor, detect and report suspicious transactions. The placement of the AML/CFT supervisory function within the FIU competence, and the SIC compliance Unit role in heading the SIC work within the NRA process contribute greatly to the effectiveness of the supervision it carries out.

Onsite examinations are risk based and are complemented with annual offsite work that use criteria such as compliance history, size, products/services provided, customers’ risk classifications, geographic presence, external auditors’ findings and reports filed with the SIC. All are utilized to determine the frequency/program of onsite examinations. The risk based AML/CFT compliance examinations carried out at banks, financial institutions, money dealers, money remittance companies, insurance companies, financial brokerage firms and specialized lending entities (comptoirs), as well as at a number of DNFBPs are robust and are also complemented by work done by the respective prudential supervisory authorities. External auditors also carry out their own independent AML/CFT annual examinations for banks, financial institutions, type “A” money dealers and money remittance companies. Lawyers and accountants are supervised for AML/CFT by their respective syndicates, and notaries by the MOJ.
Findings from AML/CFT onsite examinations highlight for banks and other reporting entities corrective measures to implement in order to enhance their AML/CFT compliance programs and internal controls. Remedial action plans are then prepared accordingly. The RBA for supervision of concerned sectors under AML/CFT Law no. 44 is updated by the SIC Compliance Unit when necessary to ensure both adequate coverage and more focused assessments. Furthermore, updates or new AML/CFT regulations that target reporting entities are suggested and introduced when the need arises due to either evolving risks, findings from AML/CFT compliance examinations, best practices, or according to developments in international standards. In instances where AML/CFT compliance examinations reveal non or partial compliance at financial sector reporting entities, the SIC is empowered to issue a warning, and recommend administrative penalties or monetary fines which are ultimately decided on by the higher banking commission. The SIC is also empowered in instances of non or partial compliance to correspond with the supervisory or oversight authorities for other types of reporting entities that are also subject to sanctions via other laws and regulations. Further to the above, any reporting entity, within the financial sector or other that violates certain AML/CFT provisions including failing to report ML/TF suspicion, not submitting to the SIC requested information or tipping of customers are subject to imprisonment and a monetary fine as stipulated in AML/CFT law no 44.

9. Looking Forward

Lebanon has come a long way in the fight against money laundering & terrorist financing, and our AML/CFT regime is in line with international standards. In spite of this, ML and TF offenders will try to exploit any vulnerabilities or weaknesses, thus causing harm to our national security, reputation, economy, and to society at large.

Concerned local government agencies have already benefited from the NRA outcome. By publishing its findings, and constantly updating the SIC website with ML/TF typologies, we also hope to raise public awareness, and enable the private sector to better understand the inherent ML/TF risks they face. As a result, they will become more informed, in a better position to assess the AML/CFT controls they adopt, and take the necessary risk mitigating measures.

ML & TF risks are constantly evolving, and worldwide advancements in financial technology (Fintech) are happening at a rapid pace. Their inevitable broader use is a matter of time. We are committed to updating our ML/TF national risk assessment on an ongoing basis, when needed or within a period not exceeding 3 to 4 years, which in turn enables us to take risk mitigation measures in due time and enhance the effectiveness of our AML/CFT regime.
ML & TF National Risk Assessment
2022 Update
1. Introduction

Lebanon witnessed major developments and tragic events since the 2019 NRA. The October uprising, prolonged periods of civil unrest, covid-19 pandemic, government shutdown, political deadlock, electricity outages and the Beirut port explosion were accompanied with a severe economic downturn, banking/financial crisis, and currency devaluation. This resulted in extreme poverty and higher unemployment levels, as well as a rise in crime levels. Inflation and the rising cost of living has not yet been matched with improvements in income levels, and the refugees’ situation continues to affect Lebanon’s risk-landscape and burdens the country’s resources.

The 2022 NRA update was mandated by the Prime Minister and relied on the 2019 NRA methodology that took reference from the FATF guidance on this topic and its three stages of identification of threats/vulnerabilities, analysis and evaluation. As such, risk in the ML/TF context was considered as a function of three factors: threats, vulnerabilities and consequences. The 2022 NRA update was backed by high level political commitment and was led by the SIC that engaged stakeholders from the public sector and from private sector reporting entities, as well as the two national committees for AML and CFT.

According to the 2022 NRA update, the TF risk continues to be high and the higher risk money laundering crimes remain associated with corruption, tax evasion, and illicit drug trafficking, resulting mainly from local predicate offences. The covid-19 pandemic and the subsidizing of consumer goods contributed to a rise in ML risks associated with counterfeiting of products and outward smuggling. Cybercrime risks (business e-mail compromise) associated with wire transfer fraud dropped since the 2019 NRA, and the types of reporting entities identified as being more vulnerable to ML/TF risks remain unchanged.

Even prior to the full completion of the 2022 NRA update, additional risk mitigating measures were taken. Generally speaking, additional risk mitigating measures were incorporated under the existing strategic plan adopted pursuant to the 2019 NRA that pillars on four main lines of actions:

1. Improve technical compliance where needed, i.e. legislative and regulatory updates.
2. Provide where needed, certain authorities with resources to improve AML/CFT capacity.
3. Enhance AML/CFT risk-based supervision where needed, and align supervisory resources with the results of the NRA.
4. Improve the partnership with private sector reporting entities.

By publishing the findings of the 2022 NRA update, we aim to raise public awareness on the most recent ML/TF risks, enable the public and private sector to better understand the ML/TF risks they face, and accordingly update their risk mitigating measures.
2. ML/TF Threats

2.1 Money Laundering Threats

ML threats continue to originate from both predicate crimes committed in Lebanon (local origin predicate crimes) and to a lesser extent from abroad (foreign origin predicate crimes). The current operating conditions of the banking/financial sector and the local capital markets along with the mitigating measures have decreased ML threats particularly those associated with crimes such as cybercrimes (business e-mail compromise - related to wire transfer fraud).

ML threats continue to arise mainly from criminal activity associated with corruption, tax evasion, illicit drug trafficking, and in recent years from outward smuggling, the occurrence of the latter increased since the 2019 NRA and is believed to generate significant illicit proceeds in cash. Previously, it was inward smuggling of agricultural and other products including through illegal border crossings that resulted in millions of dollars annually in lost tax and tariff revenues. Also, “suitcase traders” using personal luggage smuggled merchandise including pharmaceutical products that were cheaper abroad to sell in local markets. Smuggling activities are profitable and produce cash. Over the past few years, the trend has shifted from inward smuggling to outward smuggling which is primarily due to the adopted policy to subsidize consumer products such as food, medicine, and fuel making them much cheaper inside Lebanon than abroad. This on one hand resulted in losses, as less people benefitted from the funded subsidized products, and on the other hand, illicit gains to smugglers.

The outbreak of the covid-19 pandemic, the accompanying public health measures and lockdowns resulted in challenges and behavioral changes for individuals, the government and businesses. During the pandemic, in person banking continued to be the basis for transactions, as such no ML threats were associated with the misuse of online financial services or with bypassing CDD requirements. The same applies for the misuse of online government services that are almost inexistent due to the predominantly underdeveloped e-government infrastructure. However, new sources of revenue were exploited and ML threats became associated with an increase in counterfeited products, as the pandemic created opportunities for offenders to take advantage of the increase in demand for medical supplies and disinfectants that were in short supply. Certain counterfeited products such as medical supplies and disinfectants became more available, and this not only resulted in losses in tax revenues, but also presented health risks to citizens. Looking forward, vigilance by authorities is needed to prevent possible vaccine and vaccine cards fraudulent activities. As for other existing ML offences, their varying threat level remains unchanged.

ML threats continue to be associated mainly with persons, rather than with professional money launderers, gangs or organized crime groups. Relatively speaking, ML is not large scale and several methods are used that can be characterized as not being complex, including cash-based money laundering. More developed methods that can exploit the financial system are connected with corruption and the misuse of legal persons as well as trade based ML whereby the importer and foreign exporter of goods collude, resulting in shipping documents being manipulated and forged invoicing being presented.
2.2 Terrorist Financing Threats

Combating terrorism and TF continue to be top national priorities, especially after having fallen victim to many terrorist attacks, including via car bombs and suicide missions. The most recent terrorist attacks in Lebanon were associated with foreign terrorist fighter (FTF) returnees and involved self-financing, while another terrorist attack involved theft as a means for financing.

The review of recent TF convictions, national list designations in connection with terrorism/TF, STRs, ROAs, SDs and typologies that indicate activities in connection with raising, collecting, storing and moving funds for terrorist use, reveal that several terrorist groups such as ISIL, Al-Qaeda, and Jabhat Al-Nusra that previously carried out attacks in Lebanon, and FTFs continue to present threats. TF threats are associated with Lebanese FTFs (returnees), small cells, the presence of extremist elements in camps and the overall exploitable refugees’ situation. Wide spread sectarianism and the prevailing socioeconomic factors are believed to have contributed to the recent rise in Daesh recruitment activities that was depicted by law enforcement authorities in late 2021. The TF threat remains high and arises from both local and foreign origin sources.

TF activities are still not large-scale, not complex nor sophisticated and did not require extensive resources and capabilities such as a wide network of supporters. Cash was mainly used, and remains to be in modest values, and difficult to detect. TF was primarily associated with cash from terrorist groups based in the conflict zone directly or through another jurisdiction, as well as cash from self-financing. The usage was mainly for domestic terrorist attacks, logistical support and for recruitment. Aside from departing FTFs, the threat associated with TF activity to support terrorist attacks or terrorist groups abroad remains insignificant.

Cash remains the favoured method for terrorists to raise funds, and the methods used to move funds continue to include smuggling cash across the border, illegal/unlicensed hawala activities (active within refugees’ communities), money remittance and to a lesser extent bank transactions.
<table>
<thead>
<tr>
<th>Law No. 44 ML / TF Predicate Offenses - Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corruption</td>
</tr>
<tr>
<td>Tax Evasion</td>
</tr>
<tr>
<td>Illicit Drug Trafficking</td>
</tr>
<tr>
<td>Smuggling &amp; Counterfeiting of Goods</td>
</tr>
<tr>
<td>Forgery, Fraud &amp; Embezzlement of Private Funds</td>
</tr>
<tr>
<td>Trafficking in Human Beings &amp; Migrant Smuggling</td>
</tr>
<tr>
<td>Illicit Arms Trafficking</td>
</tr>
<tr>
<td>Fraud - Cybercrime</td>
</tr>
<tr>
<td>Insider Trading</td>
</tr>
<tr>
<td>Organized Crimes - Car Thefts</td>
</tr>
<tr>
<td>Environmental Crimes</td>
</tr>
<tr>
<td>Kidnapping for Ransom</td>
</tr>
<tr>
<td>Offence against Ethics &amp; Public Decency (Illegal Prostitution)</td>
</tr>
<tr>
<td>Extortion</td>
</tr>
<tr>
<td>Sexual Exploitation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Law No. 44 ML / TF Predicate Offenses - Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism &amp; Terrorist Financing</td>
</tr>
</tbody>
</table>
3. Inherent ML/TF Vulnerabilities

Over the past few years, the resources of government agencies that were already scarce and stretched out, became more so. Resources are now affected not only with the presence of large numbers of refugees with economic/social ties with jurisdictions witnessing terrorism and instability, but also with the domestic economic and financial crisis that has weighed heavily on government agencies particularly judicial and law enforcement authorities, and has also presented challenges to the ongoing efforts exerted to strengthen controls in some border areas.

The economic and financial crisis has resulted in a significant drop in GDP, a shrinkage in the banking/financial sector and has cut international trade by half. The now smaller-size economy has become more cash-based and continues to be largely dependent on cross border transfers from the Lebanese diaspora and on foreign aid. Nevertheless, having an open economy with international trade, an operational banking/financial system along with the wide use of cash, are considered inherent vulnerabilities that can be exploited by ML/TF offenders.

Some types of financial sector reporting entities have either become inactive or shifted to offering less vulnerable products/services such as consulting. Banks, the only deposit taking institutions, remain the largest component of the financial sector, and their size alone exceeds 95% of the entire financial sector. Their size, prevalence of ML/TF cases, volume of transactions, geographic reach including exposure to high risk jurisdictions, wide range of products/services offered, delivery channels and their large diverse customer base that includes high risk customers makes them inherently more vulnerable to ML/TF risks. Other FIs namely category “A” money dealers offering hawala operations, and money remittance companies are also more vulnerable in comparison to others within the financial sector.

As for DNFBPs, and in spite of the drop in the volume of their activities as a result of the economic and financial situation, they remain engaged in numerous economic activities and offer products and services that can be misused. Notaries remain more vulnerable than other DNFBPs to the possible misuse of products or services offered, especially when preparing and/or carrying out real estate transactions and when establishing companies. In terms of vulnerability to TF risks, DNFBPs are generally low.

The presence of foreign ownership within legal persons continues to be low and laws/regulations pertaining to the disclosure and access to BO information exist. In spite the prevailing economic/financial situation and the government’s diminishing resources, legal persons with public sector dealings (government contracts & public procurements) continue to be more vulnerable than others to possible misuse and to ML risks. Although such activity was reduced, the vulnerability level of such legal persons remains unchanged. Other vulnerabilities and features of legal persons might be exploited for ML, such as in holding companies where the ultimate beneficial owner is harder to determine and the BO as well as illicit proceeds can be disguised, in addition to offshore companies having operations and businesses abroad. The vulnerability level of legal persons continues to be low with respect to TF risk.
In spite the increase in foreign aid received by NPOs following the Beirut explosion and during the covid-19 outbreak, no changes in the types of NPOs previously identified as being more vulnerable to TF misuse was depicted. The types of NPOs at a higher risk of being misused for TF purposes remain:

- NPOs newly established, with limited expertise in programs or funding;
- NPOs concerned with refugees and displaced persons;
- NPOs using names implying religious affiliations, but are not so;
- NPOs operating in border areas adjacent to a conflict zone.

A number of instances of unlawful connections to the public electricity grid for mining activities were eradicated by law enforcement authorities. Nevertheless, the prohibitions in place with respect to Virtual Assets Service Providers (VASPs) and the banning of the banking/financial sector from any dealings in virtual assets, along with law enforcement measures remain the main contributors in making the vulnerability level of such activities insignificant in terms of ML/TF risks.

---

### Identifying types of reporting entities as being more vulnerable and at a higher risk of being misused for ML/TF does not necessarily mean insufficient compliance levels or inadequate AML/CFT regulations or supervision coverage. It simply means that they are more likely to be taken advantage of due to factors that include the vulnerable products/services offered by them. As such, they must be vigilant and apply the RBA to mitigate risks.

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Sub-Sector</th>
<th>Vulnerable to ML/TF Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Banks</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Remittance Companies</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Dealers “Type A”</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Money Dealers “Type B”</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Financial Institutions</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Financial Intermediaries (Brokerage Firms)</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Specialized Lending Entities (Comptoirs)</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Insurance Companies</td>
<td>Low</td>
</tr>
<tr>
<td>DNFBPs</td>
<td>Real Estate Dealers &amp; Agents</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Jewelers (Dealers in precious metals &amp; stones)</td>
<td>Medium - Low</td>
</tr>
<tr>
<td></td>
<td>Casino du Liban</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Notaries</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Lawyers</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Certified Public Accountants</td>
<td>Medium</td>
</tr>
</tbody>
</table>
4. ML/TF Risks

Money laundering and terrorist financing risks continue to evolve. Illicit proceeds from the high risk ML crimes associated with corruption and tax evasion continue to deprive Lebanon from desperately needed funds. ML risks associated with illicit drug trafficking remain high. Cybercrime risk (business e-mail compromise) that is associated with wire transfer fraud has dropped. While CFT efforts and mitigating measures resulted in TF cases being successfully investigated and prosecuted, the TF risk continues to be high and law enforcements authorities have recently depicted a rise in Daesh recruitment activities.

The adopted policy to subsidize consumer products such as food, medicine, and fuel resulted in a rise in ML risks associated with outward smuggling. The ML risks associated with the covid-19 pandemic are mainly from the counterfeiting of products such as medical supplies and disinfectants. The covid-19 pandemic, the default on the public debt and the current operating conditions of the banking and financial sector have pushed the economy more towards being cash-based. Vigilance by reporting entities is needed once confidence is restored and cash re-enters the financial sector, including from cash-intensive businesses. While other ML crimes exist, they remain of lower risk levels.

Some types of reporting entities, legal persons and NPOs are more vulnerable than others to possible misuse. The vulnerability level to ML/TF risks continues to differ among reporting entities with no major changes since the 2019 NRA, as they continue to maintain a similar range of vulnerable products/services, customer base and delivery channels. Banks, money remittance companies and money dealers with hawala operations continue to be more vulnerable within the financial sector to ML/TF risks. Notaries in comparison to other DNFBPs continue to be more vulnerable to some high risk ML offences, particularly when preparing and/or carrying out real estate transactions and when establishing companies. In terms of vulnerability to TF risks, DNFBPs continue to be generally low.
Lebanon has a comprehensive AML/CFT regime to mitigate ML/TF risks that is in line with the FATF standards and rests on a number of pillars: (1) legal & regulatory, (2) domestic & international cooperation, (3) financial sector reporting entities & DNFBPs, and (4) AML/CFT supervision. Several intelligence agencies working on counter-terrorism matters, including on a national CT strategy also contribute to the said regime in the sense that they have established within their respective agencies branches dedicated for TF investigations.

There is room for improvement. As such, the Lebanese government continues to emphasize among its national priorities the implementation of its National Anti-Corruption Strategy along with the relevant legislations issued.

The strategic action plan containing ML/TF risk mitigating measures that is being implemented was updated following the 2022 NRA update. Additional risk mitigating measures were incorporated for the recent risks associated with smuggling and counterfeiting of products, covering the commitment of resources towards enhancing border controls, combatting the counterfeiting of products and confiscating smuggled products, particularly subsidized ones, in addition to raising further awareness among private sector reporting entities.
6. ML/TF Typologies

The below typologies reflect instances where money laundering and terrorism financing were detected and mitigated as a result of Lebanon’s functioning AML/CFT regime.

6.1 Corruption

**Report (STR):** The SIC received two suspicious transaction reports from two local banks concerning the same customer who owns several companies in Lebanon. The compliance officers at the two banks didn’t receive any justifications or supporting documents from the said customer regarding certain accusations and suspicious account activity. The first bank became suspicious of the customer after coming across an article in the newspaper that mentioned the customer as being detained for corruption and bribing government officials in order to cover up for illicit acts committed by others, including drug trafficking. The second bank became suspicious after realizing that the customer’s companies’ accounts were being used as transitory accounts, and that almost all cash deposits were withdrawn directly in checks.

**Analysis and Investigation:** The SIC initiated its investigation by obtaining all available bank records including KYC forms, bank statements and copies of identification documents from the two reporting banks. In the first bank, multiple cash deposits below the threshold were executed on the customer’s account, and this activity was presented as being proceeds from real estate transactions. Checks deposited in his account were from individuals where no business relationship could be established. The analysis of his companies’ accounts at the second bank revealed that cash deposits were followed by cash and check withdrawals, and the relationship with the beneficiaries of the issued checks couldn’t also be established. During the investigation, further information on the suspect was received from local law enforcement authorities. The SIC decided to circulate the suspect’s name to all banks, financial institutions and money remittance companies operating in Lebanon to identify bank accounts and transactions. One additional bank reported having accounts for the suspect and his companies. The analysis performed on the accounts’ statements reflected a similar pattern of transactions.

**Subsequent Measures:** With the findings at hand, the SIC decided to lift banking secrecy off the identified bank accounts and forward the investigation findings to the General Prosecutor for further investigation.

**Report (ROA):** The SIC received a request of assistance from the Lebanese General Prosecutor concerning a suspect who is employed with a government agency. The suspect was charged with abusing his job, embezzlement of public funds, fraud and also for receiving bribes to facilitate sales contracts, fees exemption and tax evasion. Banking information among other things were needed to complement the ongoing investigation, and accordingly the SIC assistance was sought.

**Analysis and Investigation:** In order to identify transactions and bank accounts, the SIC circulated the name of the suspect to all banks, financial institutions and money remittance companies operating in Lebanon. The SIC also contacted the real estate register for information on the suspect’s real estate ownership. Two bank accounts belonging to the suspect were identified. The analysis performed on the obtained account statements revealed unjustified cash and check deposits followed by check withdrawals. One money remittance company also reported a few incoming and outgoing remittances.

**Subsequent Measures:** During the investigations, and as a precautionary measure, the SIC decided to freeze the balances of the two identified accounts, placed an encumbrance on all properties owned by the suspect, and requested from all money remittance companies not to perform any transaction for the suspect. The SIC decided to lift banking secrecy off the identified bank accounts and forward the investigation findings to the General Prosecutor for further investigation.
Report (R0A): The SIC received a request of assistance from the Lebanese General Prosecutor concerning allegations of corruption, bribery, and abuse of function brought against suspects working for a government agency. Banking information among other things were needed to complement the ongoing investigation, and accordingly the SIC assistance was sought.

Analysis and Investigation: In order to identify transactions and accounts, the SIC circulated the names of the suspects to all banks, financial institutions and money remittance companies operating in Lebanon. Accounts belonging to one of the suspects was identified in four banks along with accounts for close family members. The analysis performed on the obtained accounts revealed unjustified cash and check deposits followed by checks withdrawals. Accounts belonging to another suspect and close family members were also depicted at other banks, and the analysis performed on those accounts reflected many transactions between them. In addition, two money remittance companies reported a number of outgoing remittances in prior years.

Subsequent Measures: The SIC decided to lift banking secrecy off the identified bank accounts and forwarded the investigation findings to the General Prosecutor.

Report (STR): A bank filed a suspicious transaction report with the SIC on a customer after coming across media reports on accusations concerning an employee working for a government agency involved in corruption and bribery.

Analysis and Investigation: The SIC initiated its investigation by obtaining all available bank records including KYC forms, bank statements and copies of identification documents from the reporting bank. Documentation revealed that the customer was classified as high risk, and was subjected to enhanced CDD and monitoring measures. During KYC updating procedures, the customer presented a change of profession, but the bank continued to implement the enhanced measures. The review of the account statements revealed several cash deposits below the threshold. During SIC analysis, a request of assistance was received from the General Prosecutor mentioning ongoing investigations on acts of bribery and embezzlement of public funds committed by the same customer. The SIC decided to circulate the name of the suspect to all banks and financial institutions operating in Lebanon, and contacted both the real estate and vehicle register seeking information on any additional bank accounts, as well as real estate and vehicle ownership. Additional bank accounts were identified.

Subsequent Measures: The SIC froze the balances of the identified accounts, placed an encumbrance on identified properties, and forwarded the findings to the General Prosecutor for further investigation.
6.2 Tax Evasion

Report (STR): The AML/CFT compliance officer at a local bank, while reviewing cash transactions deposited in a customer’s account requested supporting documents from the said customer. The officer was provided with a real estate sales contract, from which he noticed that the deposited amount exceeded the figure mentioned in the sales contract. A STR was consequently filed with the SIC, for possible tax evasion.

Analysis and Investigation: The SIC initiated its investigation by analyzing the customer’s account activity and also circulated the names of both parties involved in the real estate transaction to all banks, financial institutions and money remittance companies operating in Lebanon in an attempt to identify if similar activity existed.

Subsequent Measures: The SIC decided to freeze and lift banking secrecy off related bank accounts and forward the findings to the General Prosecutor, who in turn decided to prosecute on tax evasion charges.

Report (ROA): The SIC received a request of assistance from the Lebanese General Prosecutor concerning ongoing investigations regarding acts of tax evasion committed by a Lebanese national that resulted in significant illicit proceeds.

Analysis and Investigation: The SIC circulated the name of the suspect to banks, financial institutions and money remittance companies operating in Lebanon. Findings revealed the existence of accounts at two banks. The analysis performed on the accounts revealed cash deposits that were later withdrawn with checks for the purchase of real estate. The SIC also requested additional information from the real estate register, commercial register and vehicle register. Further analysis and a search of the SIC database revealed that the suspect is related to three other suspects who were subject to previous case investigations relating to tax evasion. The three suspects had opened accounts and used them to receive by fraudulent means, illegitimate remittances from the ministry of finance in the form of TVA refunds.

Subsequent Measures: The SIC froze the identified accounts, requested all money remittance companies not to perform any transaction for the suspect, and placed an encumbrance on the identified properties. Findings were forwarded to the General Prosecutor for further investigation.
### 6.3 Illicit Drug Trafficking

**Report (STR):** A Lebanese national approached a local bank to open an account. The customer claimed that he owns a small manufacturing business and informed the bank that he will be depositing cash into the account from sales proceeds. The account was opened after CDD measures were carried out. After coming across a news article that posted names of individuals involved in a drug smuggling network arrested for trafficking and smuggling large amounts of drugs, the bank filed an STR with the SIC.

**Analysis and Investigation:** The SIC initiated its investigation by analyzing the customer’s account statements and also circulated his name to all banks, financial institutions and money remittance companies operating in Lebanon. Findings revealed the existence of two other bank accounts with similar patterns of cash and check deposits, followed by check withdrawals. One money remittance company reported the existence of incoming and outgoing remittances related to the suspect.

**Subsequent Measures:** The SIC decided to freeze the balances of the identified accounts, placed an encumbrance on all properties owned by the suspect, requested from all money remittance companies not to perform any transaction for the suspect and forwarded the findings to the Lebanese General prosecutor.

---

**Report (STR):** Two banks filed STRs after coming across news articles on a drug trafficking case that involved a suspect accused of smuggling large amounts of drugs. Law enforcement authorities had apprehended individuals and shut down suspected front projects and facilities.

**Analysis and Investigation:** A search of the SIC database revealed that the main suspect had relations with individuals who were subject to previous investigations. Those investigations resulted in the freezing of bank accounts and the forwarding of the case to the General Prosecutor for further investigation. The SIC circulated the name of the main suspect, close relatives and a related company mentioned in the STRs to all banks, financial institutions and money remittance companies in order to identify any further related financial transactions and bank accounts. The SIC also requested additional information from several national agencies including from the real estate register and the vehicle register, and was able to identify properties and vehicles. The analysis performed on the identified suspect’s bank accounts and those pertaining to close relatives and the related company revealed multiple cash deposits and checks deposits from different individuals. While working on the case, the SIC received a request of assistance from the General Prosecutor regarding the same suspect and other individuals who were arrested on drug trafficking charges. The request was integrated in the analysis and investigation work being done.

**Subsequent Measures:** The SIC froze the balances of identified accounts, requested from all money remittance companies not to perform any transaction for the suspects, and placed an encumbrance on the identified properties and vehicles. All findings were forwarded to the General Prosecutor for further investigation.
6.4 Smuggling & Counterfeiting of Products

**Report (STR):** Two banks filed STRs on a number of customers after coming across news articles and media reports mentioning names of nationals accused of monopolizing and storing for extended periods of time subsidized medicine for outward smuggling purposes.

**Analysis and Investigation:** The SIC initiated its investigation by obtaining all available bank records including KYC forms, bank statements and copies of identification documents from the two reporting banks. In the first bank, four suspects maintained accounts in their names and in the names of companies they own that trade in pharmaceutical products and medical supplies/devices. In the second bank, only one of the suspects maintained an account in the name of a company he owns. Analysis performed on the bank accounts revealed a change in activity and a decrease in turnover after the economic crises and the rise of the USD/LBP exchange rate. Additional information obtained by the SIC revealed that the suspects’ warehouses were searched by law enforcement authorities and the Ministry of Health and found to contain stored medicine and medical supplies/devices purchased at subsidized prices.

**Subsequent Measures:** The SIC decided to forward to the General Prosecutor the case findings that pointed towards suspicion of storing subsidized medicine and medical supplies/devices for the purpose of outward smuggling or selling at higher prices.

**Report (STR):** Two banks filed STRs on two customers and their related companies after coming across media reports mentioning their involvement in storing subsidized fuel products and in outward smuggling activity across the border.

**Analysis and Investigation:** The SIC initiated its investigation by searching its database and obtaining all available bank records including KYC forms, bank statements and copies of identification documents from the reporting banks. Information gathered on the two suspects revealed the existence of several accounts in their names and for the fuel companies they own.

**Subsequent Measures:** The SIC decided to freeze accounts and forwarded the findings to the General Prosecutor for further investigation.

**Report (ROA):** The SIC received a request of assistance from the Lebanese Internal Security Forces (ISF) through the General Prosecutor concerning a case involving counterfeiting of disinfectants and the selling thereof. The suspect under investigation had generated significant illicit proceeds while jeopardizing the lives of others during the Covid-19 pandemic.

**Analysis and Investigation:** The SIC circulated the name of the suspect to all banks, financial institutions and money remittance companies in order to identify related transactions and bank accounts. The SIC also requested information from several national agencies. Three banks reported having accounts for the suspect and two money remittance companies provided information on several transactions. The SIC obtained the related bank records and the transactions from the money remittance companies, and carried out the needed analysis. CDD information revealed a change in profession to involve the selling of sanitizing products in order to meet the rise in demand during the pandemic, and the analysis of the accounts revealed cash deposits below the ten thousand dollars threshold at one bank and minimal activity at the others.

**Subsequent Measures:** The SIC froze the balances of the identified accounts, requested from all money remittance companies not to perform any transaction for the suspect and forwarded the findings to the General Prosecutor for further investigation.
6.5 Terrorism Financing

**Report (ROA):** The SIC received a request of assistance from a local law enforcement authority via the Lebanese General Prosecutor regarding two individuals who were apprehended and interrogated for smuggling suspected terrorists across the borders. The LEA was seeking any information the SIC might have in its database and to assist in identifying any related bank accounts and transactions.

**Analysis and Investigation:** In an effort to identify whether or not the suspects had transactions or maintained bank accounts, the SIC circulated their names to all banks, financial institutions, and money remittance companies operating in Lebanon, and simultaneously requested a freeze on accounts and transactions if found. The SIC also requested from the real estate register and the vehicle register to attach an encumbrance on any assets related to them. Findings revealed the presence of two accounts at two financial institutions consisting of small value loans, including a car loan and an outstanding debt which was classified as uncollectable. One money remittance company also provided information on incoming and outgoing transactions in small amounts.

**Subsequent Measures:** The SIC decided to lift banking secrecy off the identified accounts and placed an encumbrance on the vehicle identified. Findings were forwarded to the Lebanese General Prosecutor for further investigation.

**Report (ROA):** A terrorist attack took place in Northern Lebanon and resulted in the death of law enforcement officers, army personnel and the injury of several civilians. The terrorist, known to be affiliated with ISIL, opened fire on army personnel, and blew himself up after a pursuit and confrontation with law enforcement officers. The Lebanese General Prosecutor sought the SIC assistance in order to identify any related bank accounts and transactions pertaining to the terrorist and related individuals arrested for interrogation.

**Analysis and Investigation:** The SIC initiated its investigation by circulating the names of the terrorist and related individuals to all banks, financial institutions and money remittance companies operating in Lebanon. No bank accounts or real estate ownership were identified for the terrorist, but two money remittance companies reported two incoming remittances in minimal amounts in prior years. A counterpart FIU was contacted in this regard. Investigations conducted by law enforcement authorities made available to the SIC revealed that in order to carry out the attack, the terrorist sold his house furniture and used the proceeds to self-finance his attack. Furthermore, the terrorist did not receive instructions from ISIL leaders but instead committed what was described as a “lone wolf” operation after having served time in jail for joining ISIL in Syria.

**Subsequent Measures:** The SIC requested from all money remittance companies not to perform any transaction for any of the related individuals under interrogation and forwarded the findings to the Lebanese General Prosecutor.
**Report (R0A):** The Lebanese General Prosecutor sought the SIC assistance in order to identify and freeze bank accounts, transactions and any movable or immovable assets pertaining to individuals involved in acts of terrorism and terrorism financing. The suspects had carried out an attack that resulted in the killing of municipality guards, and investigations that followed this act uncovered a terrorist cell associated with ISIL that underwent military training and collected arms and ammunitions. Law Enforcement investigations also revealed that the cell was preparing to execute terrorist attacks on Lebanese soil, namely through simple and easy to perpetrate terrorist attacks, such as mass shootings in public places.

**Analysis and Investigation:** The SIC initiated its investigation by circulating the names of the suspects to all banks, financial institutions, and money remittance companies. Enquiries were also made to the vehicle register and to the real estate register. Findings revealed the presence of money remittance transactions in small amounts occurring within the country, in addition to a number of transactions with several jurisdictions. No bank accounts were identified, and a few vehicles and properties were depicted. Additional findings from parallel investigations carried out by law enforcement and made available to the SIC revealed that the terrorist cell had also conducted several robberies to finance their activities.

**Subsequent Measures:** Spontaneous disclosures and requests of assistance were sent to the concerned FIUs. The SIC also attached an encumbrance on the identified vehicles and properties and requested from all money remittance companies to refrain from executing any future transactions for the involved individuals. All findings were forwarded to the Lebanese General Prosecutor.

---

**Report (STR):** While updating KYC forms for a number of dormant customers’ accounts, the compliance officer at a local bank tried to contact a customer using address details on file. The compliance officer was informed that the address details were no longer valid, and that law enforcement authorities had also tried, to no avail, to locate the said customer who has arrest warrants issued against him for being affiliated with or joining ISIL. The bank consequently filed an STR with the SIC.

**Analysis and Investigation:** The SIC initiated its investigation by obtaining all available bank records including KYC forms, bank statements and copies of identification documents from the reporting banks. The analysis of the bank account revealed that the account was dormant and that previous activity consisted of small cash deposits all below the threshold followed by withdrawals. The SIC broadened its investigation and contacted in this regard local law enforcement authorities seeking information on the case.

**Subsequent Measures:** The SIC decided to lift banking secrecy off the identified bank account and forward the findings to the General Prosecutor for further investigation.
Special Investigation Commission
Lebanon’s Financial Intelligence Unit

2022 ANNUAL REPORT