자금세탁방지 및 테러자금조달금지 제도 해설

특별권고 IX 관련 내용 수록 개정판

THE WORLD BANK

Paul Allan Schott
자금세탁방지 및 테러자금조달금지 제도 해설

특별권고 IX 관련 내용 수록 개정판

THE WORLD BANK

Paul Allan Schott
이 책은 2006년에 세계은행에서 "자금세탁방지 및 테러자금조달방지 제도 해설"이라는 이름으로 영문으로 출판된 것을 2011년 한국 금융 정보공사에서 번역·출간한 것이다. 한국 금융정보공사 측의 도움을 받아, 원문과 상이한 점이 있을 수 있음을 미리 알려드립니다.

이 책에 포함된 텍스트 및 건본은 저자의 견해이며, 세계은행의 공식 또는 그 동료들이 대변하는 국가의 견해를 반영할 수 있는 것은 아닙니다.

세계은행은 이 책에 포함된 자료의 정확성을 보장하지 않습니다. 이 책의 저자나 나라 남 경제, 역량, 영향 및 기타 정보는 어떤 시점의 본질 상태 또는 그러한 경제의 습관이나 수용과 관련한 세계은행의 역할에 대해서 어떠한 판단도 내포하지 않습니다.

This work was originally published by the World Bank in English as *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* in 2006 and was translated in Korean by KoFIU in 2011. This Korean translation was arranged by the Korea Financial Intelligence Unit. Korea Financial Intelligence Unit is responsible for the quality of the translation. In case of any discrepancies, the original Language will govern.

The findings, interpretations, and conclusions expressed herein are those of the author(s) and do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgement on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.
목  차

서  문 ........................................................................................................... 1

제 1편 : 문제와 그에 대한 국제적 대응 ................................................. 5

제 1 장 : 자금세탁 및 테러자금 정의 및 설명 .............................. 7
    A. 자금세탁 .......................................................................................... 10
    B. 테러자금조달 .................................................................................. 11
    C. 자금세탁과 테러자금조달의 관련성 ............................................. 12
    D. 자금세탁과 테러자금조달의 규모 .................................................. 13
    E. 진행과정 ........................................................................................ 14
    F. 발생장소 ........................................................................................ 16
    G. 방법 및 유형 .................................................................................. 17

제 2 장 : 자금세탁이 경제발전에 미치는 영향 ........................... 19
    A. 개발도상국에 미치는 부정적 효과 ................................................. 22
    B. 효과적인 AML/CFT 제도의 이점 .................................................... 26

제 3 장 : 국제기준제정기구 ................................................................. 29
    A. 유엔 ................................................................................................ 32
    B. FATF .............................................................................................. 37
    C. 바젤위원회 .................................................................................... 41
    D. 국제보험감독연합 ....................................................................... 44
    E. 국제증권감독위원회기구 ............................................................. 46
    F. 에그몽그룹 .................................................................................. 47
제 4 장 : 지역기구 및 관련 그룹 ........................................... 49
   A. FATF 스타일 지역기구 ........................................... 51
   B. Wolfsberg Group of Banks .................................. 54
   C. 영연방사무국 ............................................... 58
   D. 미주기구 .................................................. 59

제 2 편 : 효과적인 AML/CFT 구조의 구성요소 ............ 61

제 5 장 : 법률제도 관련 요구사항 ................................. 63
   A. 자금세탁의 범죄화 ........................................ 66
   B. 테러와 테러자금조달의 범죄화 ........................... 77
   C. 압수, 물수 및 권리의 상실 ................................ 77
   D. 포함된 단체와 개인의 유형 ................................ 81
   E. 감독 및 규제 – 신뢰성 관련 기준 ....................... 84
   F. FATF 권고사항 이행과 부합하는 법률 .................... 86
   G. 해당기관 간의 협력 .................................... 86
   H. 수사 .................................................. 87

제 6 장 : 예방조치 .................................................. 89
   A. 고객의 신원확인 및 고객확인제도 ........................ 92
   B. 기록보존 요구사항 ........................................ 103
   C. 혐의거래보고 .......................................... 105
   D. 과액현금거래보고 ....................................... 109
   E. 보고 및 공개 요구사항과 비밀보호법과의 균형 맞추기 .... 111
   F. 내부통제 ................................................. 112
   G. 규제 및 감독 – 신뢰성 관련 기준 ....................... 113
   H. 법인 및 법적계약 ........................................ 113

- ii -
제 7 장 : FIU ................................................................. 115
   A. FIU의 정의 ........................................................................... 119
   B. 핵심 기능 ........................................................................... 120
   C. FIU 유형 ........................................................................... 124
   D. 추가 기능 ........................................................................... 129
   E. FIU 설립 ........................................................................... 131
   F. 비밀보호 장치 .................................................................... 133
   G. 정보와 피드백 .................................................................... 136

제 8 장 : 국제협력 .................................................................. 137
   A. 효과적인 국제협력의 전체조건 ........................................ 140
   B. 자금세탁 대응을 위한 국제협력의 일반원칙 ...................... 142
   C. FIU간의 국제협력 ............................................................ 143
   D. 금융감독자 간의 국제협력 ................................................ 145
   E. 법집행기관과 사법당국 간의 국제협력 ............................. 147
   F. 세입 관련 범죄에 대한 검토 .............................................. 149

제 9 장 : 테러자금조달 대응 .................................................. 151
   A. 유엔 관련 협약의 비준 및 이행 ........................................... 154
   B. 테러자금조달과 관련 자금세탁 범죄화 ............................... 156
   C. 테러 자산의 동결 및 몰수 ................................................... 156
   D. 테러 관련 혐의거래보고 .................................................... 158
   E. 국제협력 ........................................................................... 159
   F. 대체송금제도(Alternative Remittance Systems) .................. 160
   G. 전신송금(Wire Transfers) .................................................. 161
   H. 비영리기관(Non-Profit Organizations) ............................... 162
   I. 현금반출업(Cash Couriers) ................................................. 164
   J. 테러자금조달에 관한 자기평가질의서(Self-Assessment Questionnaire) ................................................................. 167
제 3 편: 국제통화기금과 세계은행의 역할 .......................... 169

제 10 장: 자금세탁과 테러자금조달 척결을 위한 세계은행과 IMF의 이니셔티브 ................................................................. 171

A. 인식제고 .................................................................................................................. 175
B. 공동의 AML/CFT 평가방법 개발 ................................................................. 176
C. 제도적 역량 개발 .............................................................................................. 177
D. 연구 및 분석 ......................................................................................................... 179

영문원판 ................................................................................................................. 183
서
문

최근 몇 년 동안 강화된 조치에 대응하여 자금세탁과 테러자금조달 시도가 급속하게 증가했다. 국제사회는 지구 곳곳에서 교묘한 방법으로 불법자금을 이동하는 것을 목격하고 있으며, 이러한 범죄 행위에 대응해야 하는 다국적인 협력의 필요성을 인정했다.

세계은행(World Bank)과 국제통화기금(IMF)은 국가들이 새로운 국제기준을 이해하는데 도움을 주기 위해 ‘자금세탁 및 테러자금조달 대응에 관한 안내서’ 2판을 제작했다. 이 참고 안내서는 자금세탁과 테러자금조달을 척결하려는 국가들에게 실질적인 정보를 찾아볼 수 있는 하나로 통일되고 종합적인 소스로서의 역할을 할 것이다. 이 안내서는 자금세탁과 테러자금조달 범죄로 야기된 문제점과 범죄 대응에 국가들이 취해야 할 특정한 조치와 세계은행, IMF 등과 같은 국제기구의 역할에 대해 논의한다.

우리는 새로운 국제기준과 우수사례에 따라 국가들의 법적 토대와 제도적 기반을 설립 및 제고하는 도구로서 이 새 버전을 제시하고자 한다. 이 두 번째 개정판과 특별권고사항 IX에 대한 부록은 광범위한 목록을 위해 아랍어, 중국어, 프랑스어, 포르투갈어, 러시아 및 스페인어로 번역될 것이다.

우리는 자금세탁과 테러자금조달에 대한 국제적 대응뿐 아니라 그 경향과 기법이 발전하기에 본 안내서를 지속적으로 검토하고, 필요할 시 업데이트 하고자 한다. 또한, 우리는 본 자료가 보다 유용하게 쓰일 수 있는 방법에 대한 여러분의 피드백과 종고를 환영한다.

Margery Waxman  
Program Director and Senior Advisor  
Financial Market Integrity  
World Bank

R. Barry Johnston  
Assistant Director  
Monetary and Financial Systems Department  
International Monetary Fund

Jean-François Thony  
Assistant General Counsel  
Legal Department  
International Monetary Fund
역자 서문

금융정보분석원은 불법적인 원천에서 비롯된 돈으로부터 우리 금융 시장을 보호하기 위하여 지속적으로 노력해 왔습니다. 특히 최근 자본이동성의 확대와 더불어 자금세탁방지 관련 국가 간 협력의 필요성이 강조되면서 우리 금융정보분석원의 업무영역도 국내를 뛰어넘어 전 세계로 확대되고 있습니다.

「자금세탁방지 및 테러자금조달금지 제도 해설」은 자금세탁방지 실무자가 보다 손쉽게 업무에 참고할 수 있도록 작성된 자금세탁방지 개론서입니다. 1편에서 자금세탁방지 및 테러자금조달금지제도의 개념과 필요성에 대하여 간략히 설명하였고, 2편에서는 자금세탁방지 국제기준 - 이른바 ‘40+9 권고 사항’의 내용 및 해설을 수록하여 자금세탁방지 실무에서 적절히 활용할 수 있도록 하였습니다. 마지막 3편에서는 자금세탁방지 및 테러자금조달금지와 관련한 세계은행과 국제통화기금의 역할에 대하여 언급함으로써 책을 끝마치고 있습니다.

이번 「자금세탁방지 및 테러자금조달 대응에 관한 안내서」의 출판을 시작으로 이 분야와 관련된 연구활동이 활성화 되기를 바라며, 아울러 2010년 4월에서부터 10월까지 6개월에 이르는 기간 동안 번역과 출판을 위하여 헌신하신 박경춘 전 심사분석실장과 최성진 심사분석실장, 이종근, 이준엽 팀장 및 박인영 영문 에디터의 노고에 격한 감사의 말씀을 전합니다.

2010년 10월

금융정보분석원장 최수현
1편: 문제와 그에 대한 국제적 대응

1장: 자금세탁 및 테러자금 정의 및 설명
2장: 자금세탁이 경제발전에 미치는 영향
3장: 국제기준제정기구
4장: 지역기구 및 관련 그룹
제1장: 자금세탁 및 테러자금 정의 및 설명

A. 자금세탁
B. 테러자금조달
C. 관련성
D. 규모
E. 진행과정
F. 발생 장소
G. 방법과 유형
제1장 자금세탁과 테러자금조달: 그 정의와 설명

<table>
<thead>
<tr>
<th>A. 자금세탁</th>
<th>E. 진행과정</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. 테러자금조달</td>
<td>1. 배치(placements)</td>
</tr>
<tr>
<td>C. 관련성</td>
<td>2. 반복/은폐(layering)</td>
</tr>
<tr>
<td>D. 규모</td>
<td>3. 통합(integration)</td>
</tr>
<tr>
<td>F. 발생 장소</td>
<td></td>
</tr>
<tr>
<td>G. 방법과 유형</td>
<td></td>
</tr>
</tbody>
</table>

대부분의 국가에게 자금세탁과 테러자금조달은 그것의 예방, 적발 및 기소와 관련하여 중대한 문제를 제기한다. 자금을 세탁하고 테러 자금을 조달하는데 이용되는 정교한 기법들은 이러한 문제에 복잡함을 보内で 있다. 이렇게 정교한 기법들에는 각기 다른 종류의 금융기관, 다수의 금융거래, 세무 자문관·회계사·위장 회사와 기타 서비스 제공자와 같은 중개인의 이용, 각기 다른 국가로, 각기 다른 국가를 통해 그리고 각기 다른 국가로부터의 송금, 각기 다른 금융상품과 또 다른 종류의 자산의 이용이 있다. 그러나 자금세탁은 기본적으로 단순한 개념이다. 이것은 범죄 활동에서 유래한 수익이 그것의 불법적인 출처를 은닉하기 위해 가정되는 과정인 것이다. 자금세탁에는 재산 자체보다는 범죄에서 유래한 재산의 수익이 수반된다.

테러자금조달 또한 기본적으로 단순한 개념이다. 테러 또는 테러를 정리, 계획 또는 테러에 관련된 자들 어떠한 형태로든 재정적으로 지원하는 것이다. 그러나 테러 자체를 정의하는 것은 단순하지가 않은데 이는 테러라는 용어가 각 국가별로 중대한 정치적, 종교적, 국내적 관련성을 가질 수 있기 때문이다. 자금세탁과 테러 자금조달은 종종 대부분은 은닉과 관련된 유사한 거래 특징을 나타낸다.
자금세탁방지 및 테러자금조달 대응에 관한 안내서

자금세탁자들은 불법자금의 출처를 은닉하기 위해 합법적인 채널을 통해 송금하는 반면 테러자금조달자들은 불법 자금의 출처와 공격적인 사용처를 은닉하기 위해 합법적인 채널을 이용해 합법적이거나 불법적인 출처에서 나온 자금을 송금하는데 이것은 테러를 지 원하는 행위에 해당한다. 그러나 이 두 행위의 결과는 같다. 즉 불법적인 행위에 대한 대가를 얻는 것이다. 범죄자들은 돈이 세탁될 때 그 행위에서 이득을 보게 된다. 이들은 불법수익을 창출하는 범죄행위를 은닉하고, 합법적인 수익으로 보이는 것의 출처를 가정하여 대가를 얻는 것이다. 이와 유사하게 테러자금 조달자들은 자신들의 자금조달의 출처를 은닉하고, 테러 전략과 공격을 수행하기 위한 재정적인 지원을 가정하여 대가를 얻는다.

A. 자금세탁


\(\boxed{\text{당해 재산이 마련 밑에 범죄 등에서 유래된 자산임을 알면서도 그 불법출처를}}\)

\(\boxed{\text{은닉하거나 가정할 목적으로 또는 관련자의 법적책임을 멸하게 하여 지원을}}\)

\(\boxed{\text{목적으로 당해 재산의 전환 또는 이체}}\)

\(\boxed{\text{당해 재산이 범죄 또는 그러한 범죄의 가담에서 유래된 자산임을 알면서도}}\)

\(\boxed{\text{것의 성질, 출처, 소재, 처분, 이동, 권리 또는 소유권의 은닉 또는 가장}}\)

\(\boxed{\text{당해 재산이 범죄 또는 그러한 범죄의 가담에서 유래된 자산임을 수수 시점에}}\)

\(\boxed{\text{알면서도 그것의 취득, 소유 또는 사용}}\)

자금세탁방지 분야의 국제기준제정기구(setter)인 FATF는 “자금세탁”이라는 용어를 간결하게 “범죄에서 불법적으로 취득한 수익의 향법화를 위해 범죄 수익의 불법 출처를 가정하는 과정”\(^5\)으로 정의한다.

---

1) http://www.incb.org/e/conv/1988
3) 비엔나협약의 제3조(3)의 (c)(i), 칼레모협약의 제6조(1)항 조
4) 제3장 8 FATF 참조
제1장 자금세탁과 테러자금조달: 그 정의와 설명

자금세탁의 전제범죄는 세탁될 시에 창출된 수익이 자금세탁범죄로 귀결되게 하는 기초가 되는(underlying) 범죄행위이다. 비엔나협약은 전제범죄를 마약밀매로 제한한다. 따라서 마약밀매와 관련되지 않은 범죄, 예를 들면 사기, 유괴, 절도는 비엔나협약 하에서는 자금세탁범죄가 아니다. 국제사회는 해를 거듭함에 따라 자금세탁에 대한 전제범죄가 마약 밀매의 범위를 넘어가야 한다는 견해를 떠올리게 되었다. 따라서 FATF와 기타 국제기구는 비엔나협약상의 전제범죄 정의가 기타 중대 범죄도 포함하도록 확대했다. 예를 들어 금융협약은 전 회원국이 협약의 자금세탁범죄를 “가장 넓은 범위의 전제범죄”에 적용하도록 요구한다.

FATF는 자금세탁에 대응하기 위한 40개 권고사항에서 특히 비엔나협약과 금융협약에 명시된 기술적 및 법적인 자금세탁 정의를 통합하여 자금세탁에 대한 전제범죄로 반드시 포함되어야 하는 20개의 지정된 범죄를 언급하고 있다.

B. 테러자금조달


1. 자금이 다음의 행위에 이용되어야 한다는 의도를 가지고 또는 자금이 부분적 으로 또는 전체가 다음의 행위에 이용되기라는 것을 알면서도 직접적이든 간접적이든, 불법적이든 고의로, 어떠한 수단으로라도 자금을 제공하거나 모집하는 경우 본 협약 상의 범죄를 저지르는 자:
   a. 범죄에 기재된 협약 중의 하나에 나오는 범위 내에 그리고 범죄에 기재된 협약 상에서 범죄가 되는 행위, 또는

6) 제5장 A 2. 전제범죄의 범위의 논의 참조.
**C. 자금세탁과 테러자금조달의 관련성(link)**

자금세탁에 이용되는 기법은 본질적으로 테러자금조달의 출처와 그 사용을 은닉하기 위해 이용된 기법과 동일하다. 테러 자원에 이용된 자금은 합법적인 출처, 범죄 활동 또는 이 둘 다에서 비롯되었을 수 있다. 그러함에도 불구하고 그 출처의 합법여부와 관계없이 테러자금조달의 출처를 가정하는 것은 중요하다. 출처가 은닉될 수 있는 경우 앞으로의 테러자금조달 활동에 이용될 수 있다. 이와 유사하게 테러리스트들에게 자금의 사용을 은닉하는 것은 매우 중요하며, 그 결과 자금조달 활동이 적발되지 않는다.

---

10) 제3장 B FATF 참조
11) 본 안내서의 별첨 V에 전문이 나와 있음
12) id., 특별권고사항 1
이러한 이유로 FATF는 각 국이 테러자금조달, 테러행위 및 테러조직 구성의 범죄화하고 13) 이와 같은 행위들을 자금세탁의 전제범죄로 지정 14)하도록 권고했다. 마침내 FATF는 자금세탁에 관한 40개 권고사항과 통합된 9개 특별권고사항 15)이 자금세탁과 테러자금조달의 방지, 적발, 약제를 위한 기본들이 되었음을 표명했다.

국가들은 테러자금조달 대응을 위해 그들의 자금세탁방지제도의 범위를 확장하여 비영리조직, 특히 자선단체가 직접적 또는 간접적으로 테러자금을 조달하거나 지원 하는데 이용되지 않도록 자선단체를 자금세탁방지제도 범위에 포함하는 것을 검토 하도록 요구한다.16) 테러자금조달 대응을 위해서는 또한 협력과 같은 대체송금 또는 송금시스템에 대한 조사가 요구된다. 이러한 대응 노력으로는 자금세탁자와 테러리스트들이 비영리조직을 이용하는 것을 배제하도록 하기 위해 어떤 조치가 취해져야 하는 가에 대한 검토가 필요하다. 17)

위에서 언급되었듯이 자금세탁과 테러자금조달 간의 중대한 차이점은 관련된 자금이 범죄 활동뿐 아니라 합법적인 출처에서 유래할 수 있다는 것이다. 그 합법 적인 출처에는 테러 활동이나 테러조직을 지원하는데 이용되는 제단이나 자선단체 와 같은 조직들이 대한 현금기부 또는 현금증여 또는 기타 자산의 기부가 있다. 따라서 이와 같은 차이점으로 인해 테러자금조달에 대응하기 위해서는 특별법이 필요하다. 그러나 자금세탁의 전제범죄 범위에 따라 테러자금조달을 위한 자금이 불법 출처에서 유래된 범위 내의 자금은 이미 한 국가의 자금세탁방지제도에 포함 되었을 수도 있다.

D. 자금세탁과 테러자금조달의 규모

자금세탁과 테러자금조달은 자제의 성격이 보일스럽고, 통계적으로 분석하기가 어렵다. 자금세탁자들은 자신의 활동 규모를 문화화하거나 이익을 공개하지 않고, 이것은 테러자금조달자들도 마찬가지다. 다수나 이러한 활동들이 국제적으로 이루어지기 때문에 그 규모를 추정하는 것은 더욱 어렵다. 자금세탁자들은 자금세탁

13) Id., 특별권고사항 II
14) Id.
15) Id., 서문
16) 특별권고사항, VIII
17) 특별권고사항, VI
방지제도, 법집행기관의 노력 및 국제협력과 관련하여 나라마다 차이가 있다는 것을
이용하여 불법적으로 취득한 수익을 온전히 전환하기 위해 여러 국가를 이용한다. 따라서
국제적 수준에서 체계화한 자금세탁 및 테러자금조달 추진지는 없다.

자금세탁 하나만을 놓고 보면 IMF는 전 세계의 자금세탁 총액은 전 세계 GDP의
2%~5% 사이로 추정한다. 1996년 통계를 활용하면 이 수치는 대략 미화 5천90억
달러에서 1조5천억 사이가 된다.18) 따라서 자금세탁의 규모는 상당히 크고 모든
국가의 전반적인 관심을 받기에 충분하다.

E. 진행과정

자금세탁에 대한 초기 단계의 관심은 마약류의 불법 밀매와의 연관성에서 시작되
았다. 마약 밀매자들은 주로 소액차금을 합법적인 은행 예금, 금융상품 또는 기타 자산
으로 전환하는 것을 목표로 했다. 오늘날에는 다양한 범죄의 범죄활동 - 그 중에는
정치부패, 무기 불법 판매, 인신매매, 노동력 착취가 있을 - 으로 부정한 수익이 창출
된다. 자금세탁자들은 범죄의 종류와는 상관없이 불법수익을 외관상 합법적인 자금
이나 상품으로 전환하는 과정에서 배치(placement), 반복/.gmail(layering) 그리고 통
합(integration)에 의존한다.

1. 배치(Placement)

자금세탁의 첫 단계는 불법 자금을 주로 금융기관을 통해 금융제도권으로 유입
하는 것이다. 현금의 은행계좌 예금으로 유입이 이루어질 수 있다. 고액 현금은 주
의를 들 고는 소액으로 나누어 하나의 금융기관 또는 여러 금융기관의 각기 다른
지점에서 시간을 두고 예금한다. 소액은의 고액은 전화와 외화 환은이 이 단계에
서 이루어진다. 다각나 불법 자금은 환이나 수표로 전환될 수 있고, 의심을 피하기
위해 합법적인 자금과 혼합될 수도 있다. 또한 유입 과정은 증권의 현금구매 또는
보험계약으로도 이루어진다.

자금세탁방지와 테러자금조달대응에 관한 참고 안내서

자금세탁과 테러자금조달 과정

자금세탁 | 테러자금조달
---|---

범죄행위에서 유래한 현금 | 협력적인 자산 또는 범죄에서 유래한 현금

배치 현금이 계좌로 입금 | 배치 자산이 금융 제도권으로 입금

반복/은폐 자금이 출처를 은닉하기 위해 타 기관으로 이전 | 반복/은폐 자금이 출처를 은닉하기 위해 타 기관으로 이전

통합 자금이 협력적인 자산을 취득하는데 이용됨 | 통합 자금이 테러활동 자금조달에 배분됨
2. 반복/은폐(Layering)

두 번째 자금세탁 단계는 자금, 증권 또는 보험계약이 전환되거나 다른 금융
기관으로 이전되는 시점에서, 또한 이러한 자금과 불법 출처를 분리시키며 부정한
수단으로 취득된 수익이 금융제도전으로 유입되는 것이다. 그 후 자금은 다른 증
권, 보험계약 또는 전환이 용이한 투자 상품의 구매에 사용되고, 이것은 또 다른
금융기관에 관리된다. 이 자금은 또한 수표, 환 또는 무기명채권과 같은 모든 형태
의 유가증권으로 전환되거나 여러 국가에서 다른 계좌로 인터넷으로 송금될 수 있
다. 자금세탁자는 이러한 송금을 상품이나 서비스에 대한 대금지불로 가상하거나
위장회사로 자금을 송금할 수도 있다.

3. 통합(Integration)

세 번째 단계는 자금을 적법한 경제권으로 통합하는 것이다. 이것은 부동산, 증
권 또는 다른 금융자산 또는 고가의 상품과 같은 자산의 구매로 이루어진다.

물론 이 세 번째 단계는 테러자금조달에도 나타난다. 자금세탁의 세 번째 단계에
서는 범죄자금이 적법한 경제적으로 통합되는 반면 테러자금조달의 세 번째 단계에
서는 반대로 불법적인 테러리스트와 지원조직에 자금이 배분된다는 점이 다르다.

F. 발생장소

자금세탁과 테러자금조달은 전 세계 어느 국가에서라도, 특히 복잡한 금융시스템
을 보유한 국가에서 발생할 수 있고, 실제로 발생한다. 또한 엄격하지 않고, 비
효율적이며, 부패한 자금세탁 방지 및 테러자금조달 대응 기반구조가 가진 국가들
은 타깃이 될 확률이 높다. 어느 국도도 예외일 수 없다.

복잡한 국제금융거래는 자금세탁과 테러자금조달을 용이하게 하는데 역용될 수
있으므로 각기 다른 자금세탁과 테러자금조달 단계들이 여러 국가에서 발생한다.
예를 들면, 배치(placement), 반복/은폐(layering) 및 통합(integration)은 각각 3개
의 독립된 국가에서 일어날 수 있다. 또한 원래 범죄현장에서 하나 또는 모든 단
계들이 사라지기도 한다.
G. 방법 및 유형

저금은 여러 가지 방법으로 세탁될 수 있다. 그 범위는 눈에 띄지 않는 은행계좌로의 소액 현금 예금(차후의 송금을 위해)에서 자동차, 골동품, 보석과 같은 사물의 구매와 재판매에 이른다.

불법 저금은 또한 여러 건의 복잡한 국제금융거래를 통해서도 송금될 수 있다. 저금세탁자들은 매우 창의적이어서 감독자가 감독방법을 고안하면, 범죄자들은 곧 그것을 피한 또 다른 방법을 찾아낸다.

저금세탁이나 테러자금조달에 이용되는 다양한 기법은 주로 유형론이라고 부른다. 응어, 방법 또는 유형은 이들 간에 특별한 구별이 없다. 시간이 흐른 뒤에도 범죄자들이 저금세탁과 테러자금조달에 이용하는 각기 다른 방법을 정확하게 묘사하는 것은 불가능하다. 더욱이 그들의 저금세탁과 테러자금조달 방법은 경제, 금융 시장의 복잡성, 저금세탁방지제도, 법집행기관의 노력 및 국제협력과 같은 나라마다 독특한 여러 특징이나 요소들로 인해 다를 확률이 높다. 또 그 방법들은 끝임없이 변화하고 있다.

그러한 점에도 불구하고 여러 국제기구들은 저금세탁방법과 기법에 대해 훌륭한 참고 연구들을 발표했다. FATF는 연간보고서와 연간유형론 보고서에 참고자료를 실었다. 저금세탁 방법과 유형에 관한 가장 최신 정보는 이 저금세탁 방법학 사이트를 이용하도록 권고한다. 저금세탁에 대한 100건의 사례를 발표했다.

20) 제4장 참조
제2장: 자금세탁이 경제발전에 미치는 영향

A. 개발도상국에 미치는 부정적 효과

B. 효과적인 자금세탁방지와 테러자금조달 대응 제도의 이점
제2장 자금세탁이 경제발전에 미치는 영향

<table>
<thead>
<tr>
<th>A. 개발도상국에 미치는 부정적 효과</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 범죄와 부패 증가</td>
</tr>
<tr>
<td>2. 국제적인 효과와 외국투자</td>
</tr>
<tr>
<td>3. 금융기관의 취약화</td>
</tr>
<tr>
<td>4. 타협된 경제부문(Compromised economy)과 민간부문</td>
</tr>
<tr>
<td>5. 민영화 시도 좌절</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. 효과적인 자금세탁방지와 테러</th>
</tr>
</thead>
<tbody>
<tr>
<td>자금조달 대응 제도의 이점</td>
</tr>
<tr>
<td>1. 범죄와 부패 척결</td>
</tr>
<tr>
<td>2. 금융기관의 안정성 제고</td>
</tr>
<tr>
<td>3. 경제발전 촉진</td>
</tr>
</tbody>
</table>

범죄기업과 테러자금조달 활동은 그들에 자금의 출처를 은폐하고, 국내 및 국제 금융시스템을 통해 자금을 이전하여 수익을 건전하게 보이도록 할 수 있는 범위까지 계속된다. 특정 국가에서 자금세탁방지제도의 부재, 또는 입각하지 않거나 부패한 자금세탁방지제도로 인해 범죄자들과 테러자금조달자들은 범죄 활동을 확장하고, 부패, 마약일레, 인신매매 및 노동력착취, 부기일레, 일수, 테러와 같은 불법적인 활동의 조정을 통해 활동을 지속한다.

자금세탁과 테러자금조달은 어느 국가에서라도 발생할 수 있으나 개발도상국의 시장이 규모가 작아 범죄 또는 테러리스트가 야기하는 혼란에 영향을 많이 받기 때문에 개발도상국에 특히 악화된 경제적 및 사회적 영향이 있다.

자금세탁과 테러자금조달은 또한 취약한 금융시스템을 보유한 국가에 막대한 경제적 및 사회적 영향을 미치는데 이는 이러한 국가 역시 범죄 또는 테러리스트가 야기하는 혼란에 영향을 많이 받기 때문이다. 결국 자금세탁과 테러자금조달의 무게로 이동된 국가의 경제, 사회, 안보 모두가 위태로워진다.1) 그러나 국제사회 전

반에 걸쳐서 또는 특히 개별 국가에 대해 정확성을 가지고 정량화할 수 없기 때문에 이러한 역효과의 규모를 측정하기는 어렵다.

반면 효과적인 자금세탁방지제도와 테러자금조달대응 제도는 국내외적으로 큰 이익을 가져다준다. 이러한 해악에는 낮은 범죄율과 부패도, 금융기관과 금융시장의 안정성 제고, 경제발전과 국제무대에서 명성에 긍정적인 영향, 금융기관의 위험 관리법 강화 및 시장건전성 증대가 있다.

A. 개발도상국에 미치는 부정적 효과

1. 범죄와 부패도 증가

자금세탁이 성공하면 범죄 활동은 이익을 보게 된다. 이것이 범죄자들에게 보상이 되는 것이다. 따라서 어떤 국가가 자금세탁의 피난처로 간주되면 범죄자들을 유인하고 부패를 조장할 가능성이 높다. 자금세탁과 테러자금조달의 피난처는 다음과 같은 특징이 있다:

- 취약한 자금세탁방지/테러자금조달대응 제도;
- 자금세탁방지/테러자금조달대응 제도 하에서 관리되고 있는 빈번 또는 여러 종류의 금융기관;
- 자금세탁방지/테러자금조달대응 법 조항들이 거의 이행되지 않거나 불충분한 이행 또는 선택적 이행;
- 몰수를 어렵게하는 법조항을 포함하여 비효과적인 처벌;
- 제한적인 자금세탁의 전체범죄 수

한 국가에서 자금세탁이 만연하게 발생한다든 그것은 더 많은 범죄와 부패를 낳는다. 또한 자금세탁행위들은 성공적으로 하기 위한 다음과 같은 중요한 관문에서 뇌물을 빈번하게 이용하도록 만든다.

- 금융기관의 임직원,
- 변호사 및 회계사,
- 입법기관,
▶ 법집행기관,
▶ 감독 기관,
▶ 경찰,
▶ 검찰, 그리고
▶ 법원

그런 반면 포괄적이이고 효과적인 자금세탁방지/대리자금조달대응 제도는 그것의 적절한 이행 및 효과적인 집행을 통하여 이러한 범죄 활동의 수익을 상당히 감소시켜 사실상 범죄자와 데러리스트가 어떤 국가를 이용하는 것을 방해한다. 이것은 한 국가의 전반적인 자금세탁방지/대리자금조달 대응 관련 법제도에 의하여 범죄 수익이 적극적으로 줄수되는 경우에 특히 적용된다.

2. 국외적인 영향과 외국투자

자금세탁이나 대리자금조달 피난처라는 오명은 그 자체만으로 한 국가의 활전에 막대한 역효과를 유발할 수 있다. 외국금융기관은 자금세탁 피난처의 금융기관과의 거래를 제한하고, 거래에 대해 추가로 조사하여 거래 비용을 높이거나 완거래 (correspondent) 또는 대출 관계를 종결하도록 결정할 수도 있다. 자금세탁 피난처의 합법적인 기업들도 그들의 소유권, 조직 및 자배구조에 대한 추가 조사로 인해 세계시장에 진입 건수가 감소되거나 진입 비용이 높아질 수도 있다.

느슨한 자금세탁방지/대리자금조달대응 시행을 하는 것으로 알려진 국가는 외국의 민간 투자를 받을 가능성이 적다. 개발도상국인 경우 외국정부의 지원을 받을 자격 또한 임의하게 제한될 가능성이 많다.

마지막으로 FATF는 자금세탁방지 요구사항을 이행하지 않거나 자금세탁 대응 시에 충분하게 협조하지 않는 국가의 명단을 보유하고 있다. “비협조국가” 명단2)으로 알려진 이 명단에 기재되면 기재된 국가는 최소한의 기준도 수립되어 있지 않다는 것을 공개적으로 발표하는 것과 같다. 개별 FATF 회원국들은 여기에서 언급된 부정적인 영향을 덜어서 그것의 AML/CFT 절함을 고치기 위한 조치를 취하지 않는 국가에게 특정한 제재조치를 부과할 수 있다.3)

2) 제3장 FATF, The NCCT List(비협조국가리스트) 참조
3) Ibid.
3. 금융기관의 취약화

자금세탁과 테러자금조달은 여러 가지 방법으로 한 국가의 개별 금융기관의 안정성 뿐 아니라 금융부문의 건전성을 손상시킬 수 있다. 다음의 논의는 은행에 중점을 두고 있으나 동일한 효과 또는 유사한 효과가 증권회사, 보험회사, 투자관리 회사와 같은 기타 종류의 금융기관에 적용될 수 있다. 주로 평판 관련, 영업 관련, 법적 및 집중 위협으로 묶어지는 역효과는 밀접한 관계가 있다. 각각의 위험은 다음과 같은 특정 비용을 지닌다.

- 수익성 있는 사업의 손실,
- 자금 인출로 인한 유효성 문제,
- 환거래 중계,
- 조사비용 및 벌금,
- 자산 동결,
- 대출금 손실, 그리고
- 금융기관의 추가 하락. ④

평판 관련 위험은 은행의 업무와 사업관계와 관련한 불리한 평판이 그것의 정확성과는 관계없이 금융기관의 건전성에 대한 신뢰를 잃게 할 수 있다는 점에서 큰 의미를 지니는 ⑤ 투자자들이서 동시에 대출자 및 예금자인 고객들은 자금세탁이나 테러자금 조달 관련 비리나 의심으로 평판이 손상된 금융기관과는 거래를 중단한다. ⑥ 고액 대출자를 받는 것은 수익성 사업인 여신사업의 이익을 감소시키고, 전체 여신 포트폴리오의 위험을 증가시킨다. 예금자들이 자금을 인출하여 은행의 저렴한 자금조달 원천을 축소시킬 수 있다.

다구나 자금세탁자들이 은행에 예금한 자금은 인정적인 자금조달원천으로 의지할 수가 없다. 세탁된 거액의 자금은 종종 전신송금이나 다른 종류의 송금의 형식을 빌리 예상치 못하게 인출되어 잠재적인 유효성 문제를 야기한다.

⑤ Id., Para. 11.
⑥ Id.
운영 관련 위험은 내부절차, 사람이 시스템 또는 외부 사건의 부적절함이나 관리실패에서 비롯된 손실의 가능성을 의미한다.7) 위에서 언급된 바와 같이 이와 같은 손실은 금융기관이 은행 간 또는 환거래 서비스 비용을 줄이거나 없애거나 늘리는 경우 발생한다. 대출이나 자금조달 비용의 증가 또는 이러한 손실에 포함될 수 있다.

법적 위험은 손실, 비용 증대 또는 패전을 야기하는 소송, 불리한 판결, 계약 불이행, 벌금, 처벌에 대한 가능성을 의미한다.8) 자금세탁은 대부분의 세탁 과정에서 범죄가 일어난다. 따라서 합법적인 고객 또는 금융범죄의 회사가 되어 돈을 얻고, 금융기관에 변성을 위해 소송을 할 수도 있다. 벌금 및 기타 처벌 외에도 비용증가를 초래하는 은행이나 다른 법집행기관에 의한 조사가 있을 수 있다. 또한 계약 중의 몇 개의 범죄가 고객과 관련된 사기로 인해 발생되지 않을 수 있다.

집중 위험은 1인의 대출자에게 지나치게 신용 또는 이신집중에서 초래되는 손실의 가능성을 의미한다.9) 관련 규정은 통상 1인의 대출자 또는 단일 공동대출자단에 은행의 이신집중을 제한한다. 이러한 맥락에서 특정 고객, 고객의 사업, 또는 그 고객과 다른 대출자와의 관계에 대한 정보의 부족은 은행에 위험을 초래할 수 있다. 이것은 특히 관련된 상대방, 공동 대출자들 그리고 상환을 위한 수입 또는 자산이 같은 꼴인 경우 문제가 된다. 또한 계약 불이행과 가공의 인물과 제작한 계약으로 대출 손실이 초래된다.

은행과 계좌주들은 효과적인 고객확인제도가 수립되었을 시에 보호받을 수 있다.10) 한 계좌의 실소유자 확인은 효과적인 AML/CFT 제도에 필수적이다. 이와 같은 신원확인 절차는 알려진 범죄자나 태러리스트가 아니라 워장회사의 혹은 실제 사산이 없는 가공의 인물이나 법인과 맺은 사업관계로부터 고객들을 보호한다. 고객확인절차는 또한 금융기관이 고객의 사업적 관리의 상결과 기본적인 제무 문제를 이해하도록 도와준다.

7) Id. Para. 12.
8) Id. Para. 13
9) Id. Para. 14
10) 제4장, 고객확인과 고객확인제도(Customer Identification and Due Diligence), 참조
4. 타협된 경제부문과 민간부문

자금세탁자들은 "전위회사(front companies)"로, 즉 외진상 협법적으로 보이고, 또 협법적인 사업에 관여하고 있으나, 실제로는 범죄가 관리하는 회사를 이용하는 것으로 알려져 있다.

이러한 전위회사는 불법자금을 협법자금과 혼합하여 부정한 수단으로 취득한 수익을 은닉한다. 전위회사는 불법자금으로 그기의 제품과 서비스를 시장가격 이하로 매도할 수 있다. 결과적으로 협법적인 회사들은 이익 추적이 아닌 불법자금을 보존하고 보호하는 것이 유일한 목적인 전위회사와 경쟁하는 것이 어렵게 된다.

자금세탁의 수익은 전위회사와 협법적인 회사에 기타 투자를 통하여 특정한 국가의 전체 산업계나 경제를 통제하는데 활용되기도 한다. 이것은 자산 가격과 물가의 인위적인 왜곡으로 인한 자원의 부적절한 배분에 따라 금융 및 경제의 불안 정성을 증가시킬 가능성이 있다.11) 이것은 또한 다세 수단을 제공하여 한 국가의 세입을 줄인다.

5. 민영화 시도 측정

자금세탁자들은 많은 국가들이 민영화를 통해 경제를 개혁하려는 노력에 위협을 가한다.12) 이러한 범죄 조직은 입찰에서 국영기업의 협법적인 매수자들을 능가한다. 이러한 방식으로 불법수익이 투자되는 경우 범죄자들은 그 국가에서 협법적이고 시장에 기반을 둔 세금을 착실히 지불하는 기업들을 없앤 뿐 아니라 더 많은 범죄 활동과 부패에 대한 가능성을 증가시키는다.

B. 효과적인 AML/CFT 제도의 이점

1. 범죄와 부패 체결

넓은 범위의 자금세탁 전세범죄를 다루는 강력한 AML/CFT 제도는 일반적으로 범죄와 부패를 체결하는데 도움이 된다.13) 자금세탁 자체가 범죄로 될 경우 이것

---

12) Id.
은 근거가(기본) 되는 범죄를 범한 자와 불법적으로 취득한 자금을 세탁하여 그 범죄자들을 도운 자를 기소할 수 있는 또 다른 수단을 제공한다. 이와 유사하게 뇌물공여를 전제범죄로 포함하고, 효과적으로 이행되고 있는 AML/CFT 제도는 범죄자들이 뇌물을 공여하거나 다른 방식으로 공무원을 매수할 기회를 감소시킨다.

효과적인 AML 제도는 범죄 활동을 억제한다. 이러한 제도는 범죄자들이 범죄행 위에서 이득을 보는 것을 다 어렵게 만든다. 이러한 맥락에서 자금세탁 수익의 몰 수는 모든 AML 제도의 성공에 필수적이다. 자금세탁 수익의 몰수는 불법이익을 모두 없이고, 범죄 행위를 범할 동기를 감소시킨다. 따라서 자금세탁의 전제범죄 범위가 넓을수록 더 많은 혜택이 있음을 말할 필요도 없다.

2. 금융기관 안정성 제고

금융기관에 대한 대중의 신뢰와 그것의 안정성은 금융위험을 감소시키는 건전한 은행업무 관행으로 제고된다. 금융 위험에는 개인이나 금융기관이 직접적인 범죄 활동으로 인한 사기, 느슨한 내부통제, 또는 법과 규정의 위반의 결과로 손실을 입게 될 가능성이 포함된다.

고객선인원확인과 고객확인절차(KYC: Know Your Customer로 알려짐)는 효과적인 AML/CFT 제도의 일부이다. 이러한 절차들은 은행과 기타 유형의 금융기관의 안전하고 건전한 운영과 일치하고 이것을 강화한다. 이와 같은 방침과 절차는 효과적인 위험관리수단이다. 예를 들어 개인이나 법인이 외견상 독립된 것으로 보이는 여러 개의 사례를 소유하고, 한 금융기관은 KYC를 통해 그 특정 고객의 활동에 대해 종합적으로 알고 있는 경우, 그 기관은 그 대출자에 대한 이신증명을 제한할 수 있고 따라서 대출위험도 제한할 수 있다. 바젤위원회(Basel committee on Banking Supervision)는 KYC 절차의 위험관리에 대한 이점을 고려하여 자금세탁 방지와 관련한 사유와는 별도로 효과적인 은행감독을 위한 핵심원칙(Core Principles for Effective Banking Supervision)의 일부로서 KYC 방침을 통합하고 있다.14) 효과적인 AML/CFT제도는 대중의 신뢰라는 이점 외에도 그 기관이 사기로 인한 손실을 볼 수 있는 가능성을 감소시킨다. 적절한 고객선인원확인 절차와 실

---
13) 제1장, 자금세탁이란 무엇인가(What is Money Laundering) 참조: 제5장 전제범죄의 범위(Scope of the Predicate Offense) 참조
소유자 확인은 보다 합리적 계좌에 대해 구체적으로 고객확인을 수행하게 하고, 의심스러운 활동에 대한 모니터링을 하게 한다. 이렇게 신중한 내부통제는 금융기관의 안전하고 건전한 운영과 일치한다.

3. 경제발전 장려

자금세탁은 생산성이 떨어지는 활동으로 자원을 전환하여 경제성장에 직접적으로 부정적인 효과가 있다. 세탁된 불법 자금은 경제 활동에서 합법적인 자금과는 다른 경로를 따른다. 자금의 투자는 위해 생산적인 곳에 배치되기 보다는 가치를 보존하거나 송금이 더욱 용이하도록 “무익한” 곳에 종종 투자된다. 이러한 투자는 부동산, 예술품, 보석, 골동품 또는 값비싼 자동차와 같은 고가의 소비자산으로 가는 것이다. 이것은 보다 넓은 범위의 경제 분야에서 추가로 생산성을 창출하지 못한다.

더욱이 범죄조직은 수익 창출 기업이라기보다는 불법수익 세탁을 주요 목적으로 운영하여 생산적인 기업 “무익한” 투자처로 만들기도 한다. 이러한 기업은 고객의 요구나 다른 합법적이고 생산적인 자금 사용에 대응하지 못한다. 한 국가의 자원이 무익한 투자처에 집중되는 것은 다른 생산적인 목적을 추진하는 투자와는 반대로 결국 경제의 생산성을 감소시킨다.

강력한 AML/CFT 제도는 범죄자에 경제에 관여하려는 의욕을 저하시킨다. 이것은 고객의 요구에 대응하고 전체 경제의 생산성을 촉진하는 생산적인 목적에 투자가 이루어지도록 한다.
제3장: 국제기준제정기구
(International Standards Setter)

A. UN
B. FATF(Financial Action Task Force on Money Laundering)
C. 은행감독에 관한 바젤위원회(The Basel Committee on Banking Supervision)
D. 국제보험감독연합(International Association of Insurance Supervisors)
E. 국제증권감독위원회(International Organization of Securities Commissioners)
F. 에그몬트그룹(The Egmont Group of Financial Intelligence Units)
## 제3장 국제기준세정기구

### A. UN
1. 비엔나협약(Vienna Convention)
2. 폴레모협약(Palermo Convention)
3. 테러자금조달예방에관한국제협약
   (International Convention for the Suppression on the Financing of Terrorism)
4. 유엔인보리결의안 제1373호
5. 유엔인보리결의안 제1267호 및 이후의
   결의안들
6. 국제지금세탁대응프로그램
7. 태러리즘위안회(Counter Terrorism Committee)

### B. FATF(Financial Action Task Force on Money Laundering)
1. 자금세탁에 관한 40개의 권고사항
2. 회원국 모니터링
3. 자금세탁 경향 및 기법 보고
4. 비협조국가(NCCT) 리스트
5. 테러자금조달에 관한 9개 특별권고사항
6. AML/CFT 평가방법

### C. 은행감독에 관한 바젤위원회(The Basel Committee on Banking Supervision)
1. 자금세탁에 관한 원칙 발표
2. 은행 관련 핵심원칙
3. 고객확인제도

### D. 국제보험감독연합(International Association of Insurance Supervisors)

### E. 국제증권감독위원회기구(International Organization of Securities Commissioners)

### F. 에그몽그룹(The Egmont Group of Financial Intelligence Units)

국제사회의 자금세탁과 테러리스트의 활동에 관한 중대된 우려에 대응하여 여러 방면에서 움직이고 있다. 국제사회의 대부분 자금세탁과 테러자금조달이 전신송금과 같은 국제 고속송금 메커니즘을 통해 이루어지고 있음을 인식하고 있다. 따라서 범죄자와 테러리스트들의 시도를 좌절시키는데 국가 간의 협력과 협동이 필요하다.

국제사회의 노력은 마약류 밀매가 국제적인 문제이고, 다각적인 노력으로 효과적으로 대응될 수 있다는 인식과 함께 시작되었다. 따라서 자금세탁과 관련한 첫 번째 국제협약은 마약밀매를 유일한 전범죄로 지정했다(전범죄는 자금세탁 수익을 창출하는 기초가 되는 범죄). 이제는 더 많은 종류의 범죄들이 국제적인
관심의 대상이 되므로 대부분의 국가들은 높은 범위의 중대범죄를 자금세탁의 전체범죄로 다루고 있다.

이기에서 국세기준 제정기구로 간주되는 여러 국제기구들에 대해 논의한다. 또한 자금세탁방지와 테러자금조달 대응 목적으로 생산된 문서와 개발된 수단들을 대해 기술한다.

A. UN

UN은 전 세계적으로 자금세탁에 대응하기 위한 중대한 조치에 착수한 최초의 국제기구이다.1) 이러한 맥락에서 UN은 다음과 같은 사유로 중요하다. 첫째, UN은 회원국이 가장 많은 국제기구이다. 1945년 10월 설립되어 현재 191개국이 회원국이다.2) 둘째, UN은 자금세탁에 대응하기 위해 하나의 프로그램을 운영하고 있는데 이는 국제자금세탁대응프로그램(Global Programme Against Money Laundering: GPML)으로 오스트리아의 비엔나에 본부를 두고 있고, UN 마약범죄국(UN Office of Drugs and Crime: ODC) 소속이다.3) 셋째, 아마도 가장 중요한 이유로, UN은 모든 국가가 그것의 혐의와 범죄제도에 따라 조약이나 협약에 서명, 비준 및 이행하던 법적인 효력을 지니게 되는 국제조약이나 협약을 채택할 수 있다. UN인보리가 개별 국가의 특기한 부분에 대한 다른 조치와는 상관없이 안보리 결정을 통해 모든 회원국을 구속할 권한을 가지기도 한다.

1. 비엔나협약

UN은 국제마약밀매의 증가와 운영권으로 유입되는 연경난 금액의 관련 자금에 대한 우리와 가까이에 따라 UN 마약통제계획(UNDCP)을 통해 마약밀매와 자금세탁에 대응하는 국제적인 협의를 시작했다. 1988년 이러한 노력의 일환으로 비엔

1) 다른 국제적인 노력들도 있었는데 그 예로는 유럽위원회(Committee of the Council of Europe)에서 1980.6.27에 제출한 "변칙 절차에서 유래된 자금의 송금과 보관에 관한 조치(Measures Against the Transfer and Safekeeping of Funds of Criminal Origin)"가 있다. 그러나 이것은 국제사회의 자금세탁 대응 노력의 역사를 상세히 논의하려는 본 안내서의 목적을 빼앗긴다.
3) http://www.imolin.org/imolin/gpml.html 참조
나협약(United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances(1988) (Vienna Convention))이 채택되었다.  시행 지연된 도시의 이름을 띠 비엔나협약은 주로 불법마약거래와 관련 법집행 문제들에 대응하기 위한 조항을 담은; 169개국이 이 협약을 채택했다.  이 협약 상에서는 자금세탁이라는 용어를 사용하는 것을 있으나 그 개념을 정의하고, 회원국들이 자금 세탁을 범죄로 규정하도록 요구한다.  그러나 이 협약은 전범죄로 마약일체범죄를 한정하고, 자금세탁의 예방 측면에 대해서는 대응을 하지 않는다.  이것은 1990.11.11일자로 효력이 발생했다.

2. 발레모협약


▶ 자금세탁을 범죄화하고, 범행이 이루어진 경우 국내외를 막론하고 모든 중대 범죄를 자금세탁의 전범죄로 지정하며, 객관적인 사실에서 요구되는 범죄 지식이나 의도가 유추되도록 함.  
▶ 모든 형태의 자금세탁을 역제하고 적발할 수 있는 객관확인, 기록보존, 혐의 거래보고를 포함한 규제제도 수립.  
▶ 국내외적으로 행정기관, 규제당국, 법집행기관 및 기타 기관 간에 협력과 정보교환 인가 및 정보 수집, 분석 및 제공을 위해 FIU 설립 검토.  
▶ 국제협력 장려.  

5) http://www.incb.org/e/conv/1988/.
7) 비엔나협약 제3조(b), (c) (i)
9) 발레모협약 제6조.
10) Id., 제7조 (1)(a)
11) Id., 제7조 (1)(b)
12) Id., 제7조 (3)과 (4)
본 협약은 2003.9.29일자로 효력이 발생했고, 147개국이 서명하여 82개국이 비준했다.13) 본래의 협약은 그의 자금세탁방지 조항들이 FATF가 40개 권고사항에서 이전에 체택한 것과 동일한 접근법을 체택하고 있다는 점에서 중요하다.14)

3. 테러자금조달억제관한국제협약(International Convention for the Suppression on the Financing of Terrorism)


본 협약은 비준국들이 테러, 테러조직, 테러행위를 범죄화하도록 요구한다. 본 협약 하에서는 어떠한 개인이 본 협약에 부가된 기타 협약에서 규정하는 모든 종류의 테러행위를 수행하는데 (1) 그 자금이 이용될 것이라는 의도 또는 (2) 그 자금이 이용될 것임을 알고 자금을 제공하거나 모집하는 것은 불법이다.

4. 유엔안보리결의안 제1373호

UN 회원국내에서 법적인 효력을 가지기 위해서는 회원국들의 서명, 비준 및 이행이 요구되는 국제협약과는 달리 UN 환경의 제7장에 따라 국제평화와 안보에 대한 위협에 대응하여 동등한 유엔안보리결의안은 모든 UN 회원국에게 구속력을 지닌다.17) 유엔안보리는 2001.9.28에 결의한 제1373호18)를 체결했는데 이로써 회원국들은 테러자금조달 행위를 범죄화하도록 요구된다. 이 외에도 회원국들은 다음을 하도록 요구한다.

14) 이 장의 FATF 논의 참조
5. 유엔안보리결의안 제1267호 및 이후의 결의안들


1267 위원회는 자산이 동결되어야 할 개인과 단체의 명단을 발표하고, 회원국들의 제의를 근거로 명단에 추가사항 또는 삭제사항을 결정하는 절차를 보유하고 있다. 가장 최근의 명단은 1267 위원회 웹사이트에서 볼 수 있다.25)

6. 국제자금세탁방지프로그램

유엔 국제자금세탁방지프로그램(UN Global Programme against Money Laundering :GPML)은 UN 마약범죄국(ODC)에 속한다.26) 이 프로그램은 회원국들의 요청이 있을 시에 기술 관련 문헌지식, 교육훈련 및 조언을 제공하여 자금세탁방지에 대한 국제적인 조치의 효과성을 증대를 목표로 진행되는 연구지원 프로젝트이다. 이것은 다음과 같은 분야에 초점을 맞추고 있다.

UN 회원국의 핵심 인사들 간에 인식 수준 제고
- 편성법 및 대륙법을 채택하는 나라(common and civil law countries)에 기준이 되는 법 제정을 지원하여 법적인 제도 구축 촉진
- 특히 FIU의 설립으로 제도적 역량 개발
- 법조계, 사법부, 법집행 규제기관과 민간 금융부문에 교육훈련 제공
- 문제 대응에 지역적 접근방식 정리, 타기관과의 전략적 관계 발전 및 유지
- 정보 데이터베이스 유지 및 관련 정보 분석 착수

따라서 이 프로그램은 한 국가의 자금세탁방지 기반을 구축하거나 개선할 시에 그와 관련된 정보, 전문지식 및 기술 지원의 방편이다.

7. 대테러위원회(Counter Terrorism Committee)
위에서 언급되었듯이 UN 안보리는 2001.9.28에 9/11에 대한 적정적인 대응으로 결의안(제1373호)을 채택했다. 이 결의안에서는 모든 회원국들이 대러 처벌을 위한 구체적인 조치를 취하도록 요구했다. 또한 모든 회원국에게 구속력을 가지는 이 결의안은 테러에 대응하여 국제적인 역량을 거두는데 있어 회원국의 성과를 보니터하기 위해 대테러위원회(Counter Terrorism Committee)를 설립했다. 안보리는 15개 회원국으로 구성되는 대테러위원회는 범죄해결기관이 아니라; 따라서 제재조치를 발표하거나 개별 국가를 기소하거나 관련하지 않는다. 단지 제1373호의 목표를 성취하는 방법에 대해 안보리와 회원국들 간에 대화 채널을 구축한다.

제1373호는 모든 국가들이 결의안의 조치를 이행하고, 적극적으로 보고하는데 취해진 조치에 대해 대테러위원회(CTC)에 보고서를 제출하도록 요구한다. 이러한 관점에서 대테러위원회(CTC)는 각 국가가 제1373호의 요구사항과 관련하여 대러 처벌을 위한 기존의 법과 메커니즘에 대해 자가 평가를 하도록 요구한다. 대테러위원회(CTC)는 자체적으로 적정적인 지원을 제공하지는 않으나 한 국가의 법적인 토대와 기반을 강화한 필요가 있는 분야를 식별한다.

대테러위원회(CTC)는 대용 기반은 개선하려고 할 시에 도움을 구하는 국가를 위해 웹사이트에 자료방을 두고 있다. 이 자료방에서는 기준이 되는 법과 기타 유용한 자료의 사본을 볼 수 있다.

27) 유엔안보리 결의안 1373호
28) http://www.un.org/sc/stc. 참조
29) Id.
B. FATF

G-7 국가들30)에 의해 1989년 창설된 자금세탁방지에 대한 국제적 대응책을 개발하고 장려하려는 목적을 지닌 정부 간 기구이다.31) FATF는 2001년 10월에 테러자금조달 척결을 포함하도록 그것의 임무를 확장했다.32)

FATF는 한 국가의 범죄 및 규제적 자금세탁방지 및 테러자금조달 대응 개혁을 달성하기 위해 법률, 금융 및 법집행 전문가들을 불러 모으는 정책기구이다. 현재 회원국은 31개 국가와 2개의 지역기구로 구성되어 있다.33) FATF는 또한 다수의 국제기구34) 및 조직35)과 협력한다. 이와 같은 단체들은 FATF에서 옵저버 지위로 투표 자격은 없으나 총회와 실무그룹에 참가하도록 허용된다. 자금세탁과 관련한 FATF의 세 가지 주요 기능은 다음과 같다.

1. 회원국의 자금세탁방지 조치 이행 사항 모니터링
2. 자금세탁 경향, 기법 및 대응책에 대한 검토 및 보고
3. FATF의 자금세탁방지 기준의 국제적인 채택과 이행 장려

30) id. G-7 국가들에는 캐나다, 프랑스, 독일, 이탈리아, 일본, 영국, 미국이 있다.
31) FATF와 테러자금조달에 대해서는 http://www.fatf-gafi.org/
32) id. 테러자금조달에
33) 31개 회원국 : 아르헨티나, 호주, 오스트리아, 벨기에, 브라질, 캐나다, 멕시코, 루마니아, 러시아, 스페인, 스웨덴, 스위스, 캐나다, 멕시코, 루마니아, 러시아, 스페인, 스웨덴, 스위스, 루마니아, 러시아, 스페인, 스웨덴, 스위스, 루마니아, 러시아, 스페인, 스웨덴, 스위스, 루마니아, 러시아, 스페인, 스웨덴, 스위스, 루마니아, 러시아, 스페인, 스웨덴, 스위스
34) 국제기구에는 FATF와 유사한 형태와 기능을 지닌 FATF와 같은 지역기구(FSRBs)가 있다. 몇몇 회원국은 FSRBs에 참여한다. 그 예로는 아시아 태평양 그룹(Asia/Pacific Group on Money Laundering (APG)), 캐나다 FATF(CFATF), Council of Europe MONEYVAL(이전 PC-R-EV Committee), 동남아프리카자금세탁그룹(ESAMLG), 남미 FATF(GAFISUD)가 있다. 이와 같은 기구는 대한 민주주의 사법 협력의 사무국과 같은 기구에 대한 논의는 제4장의 지역기구에 관한 그룹, FATF와 같은 지역기구 참가, FATF는 또한 예결심규칙과도 협력한다.
1. 40개 권고사항

FATF는 comando적인 자금세탁방지의 기본 블록을 구성하고, 전 세계 국가들이 보편적으로 채택할 수 있도록 고안된 40개 권고사항을 제작했다.36) 40개 권고사항에는 조치에 관한 원칙이 명시되어 있다; 이 원칙들은一定程度 국가의 역할과 현행 요구사항에 따라 탄력적인 적용을 허용한다. 법안을 구속력이 있는 것은 아니나 국제 자금세탁방지 기준으로써 국제사회와 관련 기구에서 널리 인정되었다.

40개 권고사항은 어떤 국가가 국제사회에서 국제기준을 충족하는 것으로 간주하기를 원하는 경우 실질적으로 행동영역과 같다. 개별권고사항은 본 안내서 전반에 걸쳐, 특히 5, 6, 7, 8장에서 상세하게 논의된다.


2. 회원국 모니터링

40개 권고사항의 조건 이행에 대한 회원국의 상태를 모니터링 하는 것은 2단계의 과정, 즉 자가 평가 및 상호평가로 이루어진다. 자가 평가 단계에서는 각 회원국이 매년 40개 권고사항 이행에 관한 기본 질문표(standard questionnaire)를 작성한다. 상호평가 단계에서는 각 회원국이 타 회원국으로 구성된 전문가 집단에 의해 점검을 받고, 평가된다.

한 국가가 40개 권고사항 이행을 위한 적절한 조치를 취하지 않는 경우 FATF는 모든 금융기관에게 회사 및 금융기관을 포함하여 불이행 국가 출신의 개인과의 사업관계와 거래에 특별한 주의를 기울이고, 해당되는 경우, 의심스러운 거래, 즉 명백한 경제적 목적이나 가시적인 법적 목적이 없는 거래를 해당기관에 보고하도록 권고한다.37) 최종적으로는 이행을 위한 조치를 취하지 않는 경우 회원국가가 중지될 수 있다. 그러나 이러한 제재조치 이전에 타 회원국으로부터 압력이 가해진다.

37) Id., Rec. 21
3. 자금세탁 경향 및 기법 보고

FATF의 기능중 하나는 자금세탁 경향, 기법 및 방식의 기술적 유형을 검토하고 보고하는 것이다. FATF는 이 업무를 수행하기 위해 유형론보고서(Typologies Report)를 통해 자금세탁의 현황에 대해 연간보고서를 발간한다.38) 이러한 보고서는 단지 FATF 회원국만이 아니라 모든 국가가 자금세탁의 새로운 기법이나 경향과 이 분야의 기타 현황에 대해 최신정보를 취득하는데 매우 유용하다.

4. 비협조국가(NCCT) 리스트

FATF의 목표 중 하나는 전 세계 모든 국가들이 국제적인 자금세탁방지 및 탄력적조달 대응 기준을 채택하도록 장려하는 것이다. 따라서 이 업무는 FATF가 회원국에만 국한하여 세계를 가할 수 있다 하더라도 FATF 회원국이 아닌 국가에도 적용될 수 있다. 이에 모든 국가가 자금세탁의 방지, 적발 및 기소 조치를 채택하도록 장려하기 위해서, 즉 40개 권고사항을 이행하도록 하기 위해서 FATF는 국제협력에 걸림돌이 되는 국가들을 식별하는 절차를 채택했다. 이 절차는 비협조 국가를 식별하여 공개적으로 볼 수 있는 명단에 기재하는데 있어 25개의 기준을 이용하는데 이는 40개 권고사항과 일치한다.39)

비협조국가는 결함을 신속하게 처리하도록 권고된다. 비협조국가가 충분히 진전을 보이지 않는 경우 대응조치가 부가될 수 있다. 대응조치에는 비협조국가 명단에 기재된 국가에 대해 FATF 회원국들이 취하는 특정 조치들로 구성된다.

FATF는 비협조국가와의 사업관계와 거래에 특별한 주의를 기울이는 것이 외에도 절연적이고, 비례적이며, 탄력적인 방식으로 적용되는 추가 대응조치를 부가할 수 있다. 이러한 추가 조치에는 다음과 포함된다.

◆ 임격한 고객 신임확인 조건, 비협조국가의 개인이나 기업과 사업관계가 구축되기 전에 실소유자의 신원확인을 위해 특정 국가에 대한 금융 관련 권고( advisories)를 포함하여 금융기관에 대한 권고 강화

---
vi 비협조국가와의 금융거래의 의심의 가능성에 높다는 것을 전제로 관련 보고절차 강화 또는 금융거래의 체계적인 보고

▼ FATF 회원국에 은행의 자회사, 지점 또는 대표사무소 설립에 대한 승인 요청을 검토 시에 관련 은행이 비협조국가의 은행인지 고려할 것
▼ 비협조국가 내의 단체와의 거래는 자금세탁의 위험이 있을 수 있다는 것을 비금융권 사업체에 경고41.

마지막으로 이러한 대응조치에는 FATF 회원국이 비협조국가의 금융기관과의 거래중지가 있을 수 있다.

대부분의 국가들은 비협조국가의 단단에서 석재되기 위해 혼신의 노력기를 기울이는 데 이것은 그 국가의 금융기관과 사업체에 국제 평판뿐 아니라 국제거래와 관련해 서도 심각한 문제를 야기하기 때문이다.

5. 테러자금조달

FATF는 또한 테러자금조달 체결을 위한 전 세계적인 노력에 전문지식을 집중하고 있다. FATF는 이 확장된 업무를 수행하기 위해 테러자금조달에 관한 9개 특별 권고사항 (Special Recommendations on Terrorist Financing: Special Recommendations)42을 채택했다. 이러한 노력을 일환으로 FATF 회원국들은 특별권고사항 이행을 위한 조치에 대해 자가 평가 절차를 활용한다.43) FATF는 지속적으로 테러자금조달에 이는 기법과 메커니즘에 대한 지침을 개발한다. 본 안내서의 제9장에서 특별권고사항과 자가 평가 절차에 대해 보다 상세히 논의된다.

6. AML/CFT 평가방법

2002년 결의된 협의 중에 FATF, IMF, 세계은행은 FATF에 의한 상호평가와 IMF와 세계은행의 금융부문 평가 및 국제 금융센터 프로그램 평가에서 이용되는

단일 평가방법을 채택했다. 지역기구인 FSRBs는 그 방법론의 개발에 관여해 왔고, 이들 그들의 상호평가에도 그들을 이용하는데 동의했다.

2003년 제정된 이 평가방법(40개 권고사항)은 2004년에 개정된 바 있다. 여기에는 평가자들이 AML/CFT제도를 평가할 때 점검해야 하는 200개가 넘는 "필수 요건"들이 명시되어 있다. 이것은 한 국가의 법적/제도적 AML/CFT 기반을 포함하는데 여기에는 FIU도 포함된다. 또한 은행, 보험 및 증권분야에 대한 감독 및 규제 기준뿐만 아니라 유엔로지 결의안과 국제협약의 관련 요소도 포함된다. 필수요건에는 각 40개 권고사항과 9개 특별권고사항의 완전 이행에 제시될 필요가 있는 강제적인 요소들이 기술되어 있다. 이 방법에는 이상 등급을 매기는 방법에 대한 지침이 포함되어 있고, 필수요건의 이행을 기준으로 한다.

이 평가방법에는 또한 AML/CFT 제도의 강화를 위한 선택사항인 다수의 "추가 요소"가 포함된다. 이 추가 요소들의 이행 성과가 전체 평가의 일부로 검토되기는 하나 강제성이 없고, 이행 자체를 위해 평가되는 것은 아니다.

FATF, IMF, 세계은행, FSRBs가 단일하지만 종합적인 평가방법을 채택했다는 것은 국가의 이행 평가와 동급 매기기에 대한 보다 동일한 접근방식을 의미한다. 평가를 받고 있는 국가는 평가의 첫째 단계에서 이 평가방법 문서에 따라 AML/CFT 제도에 대한 각각 평가 준비하도록 요구될 것이다. 이 문서 또한 국제 기준 준수를 위해 취해야 할 필요가 있는 조치에 대해 상세하고 유용한 지침이다.44)

C. 바젤위원회(The Basel Committee on Banking Supervision)

바젤위원회45)는 10개국 그룹(Group of 10 countries) 중앙은행 총재46)에 의해 1974년 설립되었다. 개별 국가는 중앙은행이나 중앙은행이 관리 기관이 아닌 경우 은행 건전성 감독이라는 공식적인 책임을 가진 해당 기관이 대표한다. 바젤위원회

45) http://www.bis.org/index.htm.
46) 실제로는 13개국이 회원이므로 10개국 그룹은 오해이다. 바젤위원회 회원국(10개국 그룹)은 베네수엘라, 캐나다, 프랑스, 독일, 이탈리아, 일본, 룩셈부르크, 네덜란드, 스페인, 스웨덴, 스위스, 영국, 미국이다.
는 공식적인 국제감독권이거나 범죄 권한이 없다. 다만 폭넓은 감독 기준과 지침을 공식화하고, 강범죄형 중형감독 사안에 대해 우수사례를 권고한다. 이러한 기준과 지침은 각 국내에서 해당기관이 국가의 제도와 가장 잘 맞는 법령, 규제 또는 다른 방식의 세부 조치를 이행하는데 필요한 모든 조치를 취할 것이라는 기대를 가지고 체택된다. 바젤위원회의 3개 감독기준과 지침은 자금세탁과 관련된 것이다.

1. 자금세탁에 관한 원칙 발표


- 적절한 고객확인
- 높은 윤리기준과 법 준수
- 법심행기관과의 협력
- 성명서를 준수하는 방침과 절차

첫째, 은행은 은행 업무를 요청하는 모든 고객의 실제 신분을 확인하려는 합리적인 노력을 해야 한다. 신분 증명을 하지 못하는 고객과는 중요한 거래를 하지 않는다는 것이 은행의 명시적인 방침이어야 한다.

---
47) http://www.bis.org/publ/bcbsc137.pdf.
48) id., 서문 Para. 6.
49) id., 고객확인
제3장 국제기준제정자(Iternational Standards Setter) 43

둘째, 은행은 높은 올리기준에 맞추어 거래를 하고, 금융거래와 관련된 법과 규정을 준수해야 한다.50) 은행은 자금세탁과 연관되어 있다고 믿음만한 합당한 사유가 있는 경우 서비스를 제공하지 않거나 거래를 적극적으로 지원하지 않아야 한다.

셋째, 은행은 고객 기밀과 관련된 국내법이나 규정에서 허용하는 범위에서 국내의 법집행기관에 전적으로 협조해야 한다.51) 변경되었거나 불완전하거나 흐도하는 정보로 법집행기관을 속이려는 고객에게는 어떠한 지원도 제공되지 않아야 한다. 은행이 예금계좌의 자금이 범죄 활동에서 비롯된 것이거나 채결된 거래가 범죄목적을 위한 것이라는 합당한 추정이 가능한 경우 지원 거부, 고객 관계 중지 그리고 계좌 폐쇄 또는 동결을 포함하여 적절한 조치를 취해야 한다.

넷째, 은행은 이 상정시와 일관되는 공식적인 방침을 채택해야 한다.52) 또한 모든 은행직원이 은행 방침을 인지하고, 은행 방침에서 다루어지는 사안에 대한 적절한 교육이 제공되도록 보장해야 한다. 특정 고객확인 절차는 은행 방침의 일부로써 채택되어야 한다. 마지막으로 은행 내의 내부감사 기능이 효과적인 이행에 대한 검증수단으로 존재해야 한다.

2. 은행 관련 핵심원칙

1997년 바젤위원회는 효과적인 은행감독제도를 위한 종합적인 첫사진을 제공하고, 넓은 범위의 주제를 다루는 '효과적인 은행감독을 위한 핵심원칙(Core Principles for Effective Banking Supervision: Core Principles)'53)를 발표했다. 총 25개의 핵심원칙 중 하나인 핵심원칙 15는 자금세탁을 논하고 있으며, 다음과 같이 명시하고 있다.

은행감독자들은 은행이 임설한 “고객알기” 규칙을 포함하여 높은 올리기준과 전문적인 기준을 전반하는 적절한 방침, 우수거래와 절차를 수립하고 있는지를 결정하고, 고객의 요구와 상관없이 범죄 요소에 의해 이용되는 것을 방지해야 한다.54)

50) Id., 법 준수
51) Id., 법집행기관과의 협력
52) Id., 상정서 준수
54) Id., 핵심원칙 15
“고객알기” 방침과 절차는 모든 국가에 효과적인 AML/CFT의 제도적 기반을 위해 필수적인 부분이다.

바젤위원회는 핵심원칙 외에도 1999년 고객알기 방침과 절차의 적절성을 평가하는 데 도움이 되는 11개의 기준과 5개의 추가 기준이 담긴 “핵심원칙 방법론(Core Principles Methodology)”을 발표했다. 이 추가 기준에는 40개 권고사항의 이행에 대한 구체적인 참고사항이 포함되어 있다.

3. 고객확인제도

바젤위원회는 2001년 10월 은행의 고객확인제도(Customer due diligence for banks : Customer Due Diligence)라는 제목으로 고객알기에 대한 방대한 논문을 발표했다. 이 논문은 전 세계로 고객알기 절차에서 지적된 결함에 대한 대응으로 발간되었다. 이와 같은 고객알기 기준은 자금세탁 목적을 가진 범죄자들의 은행 이용방지에 관한 성명서와 핵심원칙 15에 대한 보다 구체적인 정보를 제공한다. 고객알기 기준의 필수적인 요소는 본 문서에 상세히 기술되어 있다.

고객확인제도에 명시된 고객알기 기준은 은행의 안전과 건전성 그리고 은행시스템의 장단점을 보호하여 자금세탁 측면을 넘어 은행에 해택을 주려는 의도로 만들여진 것이다. 바젤위원회는 또한 이 문서에서 “FATF 권고사항, 특히 은행과 관련된 권고사항의 채택과 이행”을 강력히 지원하고, 고객확인제도의 기준이 “FATF 권고사항과 일관되게” 할 것이다.

D. 국제보험감독연합(International Association of Insurance Supervisors)

1994년에 설립된 국제보험감독연합(I AIS)은 100개 이상의 국가들의 보험감독기관으로 구성된 조직이다.

56) Id., FATF 권고사항 인용구 별점 2.
57) Id., Para. 3.
58) Id., Para. 3.
59) 회원국 명단은 http://www.iaisweb.org/132_176_ENU_HTML.asp를 참조. 회원 명단에는 개별 회원국 웹사이트가 포함되어 있음
이 연합의 주요 목표는 다음과 같다.

- 보험감독자 간의 협력 증진
- 보험감독의 국제기준 제정
- 회원국에게 교육 제공
- 타 금융분야의 규제자들과 국제금융기관과 협력

IAIS는 회원국의 감독기관 외에도 산업계, 적당 연합, 보험 및 재보험회사, 컨설팅과 국제금융기관으로 대변되는 60개국 이상의 은저버 국가를 보유하고 있다.

IAIS가 실장 보험감독의 전 분야를 포함한 공정한 주제를 다루기는 하나 연구 논문 중의 하나에서 특히 자금세탁을 다룬다. 2002년 1월 이 연합은 저참 논문 제5호, 보험감독자들과 보험회사를 위한 자금세탁방지지침서(Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities: AML Guidance Notes)를 발간했다. 이 논문은 보험업체와 관련한 자금세탁에 관한 중요한 논의이다. 자금세탁방지지침서는 그와 유사한 유형의 다른 국제연구원과 같이 개별 국가들이 관련된 특정 보험회사, 국내에서 제공되는 상품, 국가 고유의 금융제도, 경제, 현행, 법률제도를 고려하여 이행하도록 하려는 의도를 가진다. 이 논문에는 보험회사를 위한 다음의 4가지 원칙이 담겨있다.

- 자금세탁방지법령 준수
- “책임할기” 절차 수립
- 모든 법집행기관과 협력
- 직원을 위한 내부 자금세탁방지 방침, 절차, 교육 프로그램 보유

이 네 가지 원칙은 바젤위원회의 설명서에 있는 4개의 원칙과 유사하다. 자금세탁방지지침서는 협의례보고와 기타 요구사항을 포함하여 40개 연고사항과 완전히 일치한다. 사실 40개 연고사항은 IAIS의 자금세탁방지지침서의 발전에 포함되어 있다.

60) Id., 홈페이지
61) Id., 은저버리기 구 명단은 은저버(Observers)
E. 국제증권감독위원회기구(International Organization of Securities Commissioners)

국제증권감독위원회기구(International Organization of Securities Commissioners: IOSCO)는 개별 국가에서 일상적인 증권 규정과 증권법의 관리 업무를 담당하는 증권위원회의 위원장들로 구성된 조직이다. 현재 회원국 규모는 105개국의 규제기관이며, 해당 국가의 증권법 관리를 맡은 정부기관이 없는 경우 증권거래소와 같은 자율규제기구가 투표권을 가지는 회원이 될 수 있다. 국제기구는 준회원, 자율규제기구는 가맹회원(affiliate member)이 되는데 이 둘 다 투표권은 없다.

IOSCO의 증권감독을 위한 핵심 목표는 다음과 같다.

- 투자자 보호
- 시장의 공정성, 효율성, 투명성 보장
- 시스템 위험 감소(63)

IOSCO는 자금세탁과 관련하여 1992년 “자금세탁에 관한 결의안”을 통과시켰다. 유사한 형태의 다른국기구와 마찬가지로 IOSCO는 법제정 권한이 없다. IOSCO도 바젤위원회와 IAIS와 유사하게 회원국이 그것의 권고사항을 이행하는 것에 의존한다. 그 결의안은 다음과 같이 규정하고 있다.

각 IOSCO 회원국은 다음을 겸해야 한다.

1. 자금세탁자들을 식별하고 기소하는 관련기관의 역량 강화라는 목적으로 IOSCO의 감독 하에 금융기관에 의해 고교확인정보가 수집되고 기록되는 범위
2. 증권 및 선물시장에서의 금융거래를 재현하기 위한 수단 제공이라는 측면에서 기록보존 요건의 범위와 적절성
3. 자금세탁범죄 기소를 담당하는 국내 규제자와 함께 허위거래과약 및 보고를 처리하는 적절한 방법
4. 범죄자들의 증권 및 선물 사업권 취득을 방지하기 위한 절차 수립

---

5. 증권 및 결제회사가 자금세탁의 역체와 적발을 위해 고안된 모니터링과
이행 절차를 유지하도록 보장하는 적절한 수단
6. 증권과 설립모니터를 재현하기 위한 문헌작성의 적절성과 기술을 포함하여
거래 시에 현금 또는 그에 상응하는 가치의 이용
7. 특정한 권한이 주어진 경우 자금세탁 철결을 위해 정보를 공유하는 가장
적절한 수단

F. 에그몽그룹(The Egmont Group of Financial Intelligence Units)

각 국에서는 자금세탁철결을 위한 노력의 일환으로 자금세탁보고 요건에 따라
단체와 개인이 제출하는 정보를 분석하는 기관을 설립했다. 그러한 기관은 주로
FIU(Financial Intelligent Unit)로 불린다. 이 기구는 국제 자금세탁방지 프로그램
의 중심으로 역할을 하는데 그것은 금융기관과 법집행기관 사이에 정보교환을 담
당하고 있기 때문이다. 자금세탁은 전 세계 이루어지고 있기 때문에 국제적으로도
정보공유의 필요성이 있다.

1995년 현재 FIU로 알려진 다수의 정부기관이 협력을 시작했고 에그몽그룹
(Egmont Group of Financial Intelligence Units: Egmont Group)의 개시까지
었던 브뤼셀의 에그몽을 창설했다. 이 그룹의 목적은 각국의 자금세탁방지 프로
그램에 대한 지원을 개선하고, 자금세탁방지 구상들을 조정하는 FIU를 위해 포럼
을 제공하는 것이다. 이와 같은 지원에는 금융정보 교환의 확대 및 체계화, 분석인
력의 전문지식과 역량 향상, 기술을 이용한 FIU간의 의사소통 개선 그리고 세계적
으로 FIU의 발전 원가가 포함된다.

에그몽그룹의 임무는 2004년 특히 데라자금조달에 관한 금융정보를 포함하도록
확대되었다. 에그몽그룹의 회원이 되려면 우선 에그몽그룹의 FIU 정의를 충족
해야 한다. 그 정의는 “자금세탁과 데라자금조달 철결을 위해 금융정보 접수(요

67] 제7장의 논의 참조
70] Id.
71] 회원자격 논의는 에그몽그룹 회원가입 절차와 함께 웹사이트에 있는 Egmont paper 참조,
청), 분석 및 해당기관으로 제출, (i)의심스러운 범죄수익과 테러자금조달 가능성과 관련하여, 또는 (ii)국내법에서 요구되는 경우 금융정보공개를 담당하는 중앙국가기관"이다.72) 회원국은 또한 자금세탁사건에 대해 FIU간의 정보교환원칙에 따라 것
을 시작해야 한다.73) 이러한 원칙에는 정보교환 조건, 정보의 허용된 이용에 대한
제한사항 및 기밀보장이 포함된다.

에그몽그룹의 회원은 현재 94개국이다.74) 회원국들은 정보교환을 위해 일반에게
공개되지 않는 보안웹사이트에 접속할 수 있다.

에그몽그룹은 사무국이나 영구주소지가 없는 비공식적인 기구이다. 1년에 1회
총회와 1년에 3회 실무그룹에서 회동한다. 에그몽그룹 내에서 FIU의 원장들이 회
원사절을 포함한 모든 정책을 결정한다. 연간 총회에서 선사에 실무그룹과 FIU
원장과의 조율을 돕기 위한 에그몽 위원회를 설립했다.

마지막으로 에그몽그룹은 대중도 열람할 수 있는 교육 자료를 만들었다. 회원국
의 FIUs로부터 자금세탁 적절에 대해 추려진 사례들을 모아 출간했다.75) 또한 웹
사이트에서 이용할 수 있는 에그몽 관련 문서와 비디오를 제작했다.

제4장 : 지역기구와 관련그룹

A. FATF 스타일 지역기구 (FATF-Style Regional Bodies: FSRBs)
B. Wolfsberg Group of Banks
C. 영연방사무국 (The Commonwealth Secretariat)
D. 미주기구 (Organization of American States - CICAD)
제4장 지역기구와 관련그룹

<table>
<thead>
<tr>
<th>A. FATF 스타일 지역기구 (FATF-Style Regional Bodies: FSRBs)</th>
<th>B. Wolfsberg Group of Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 아시아태평양 그룹 (Asia/Pacific Groups on Money Laundering: APG)</td>
<td>1. 프라이빗뱅킹을 위한 자금세탁방지원칙 (Anti-Money Laundering Principles for Private Banking)</td>
</tr>
<tr>
<td>2. 카리브 FATF(Caribbean Financial Action Task Force)</td>
<td>2. 테러자금조달액에 관한 성명서 (Statement on the Suppression of the Financing of Terrorism)</td>
</tr>
<tr>
<td>3. 유럽의회 (Council on Europe - MONEYVAL)</td>
<td>3. 할인거래를 위한 자금세탁방지원칙 (Anti-Money Laundering Principles for Correspondent Banking)</td>
</tr>
<tr>
<td>4. 동남아프리카 자금세탁방지그룹 (Eastern and Southern Africa Anti-Money Laundering Group)</td>
<td>C. 영국통신사무국 (The Commonwealth Secretariat)</td>
</tr>
<tr>
<td>5. 남미 FATF(Financial Action Task Force on Money Laundering in South America)</td>
<td>D. 미국기구 (Organization of American States – CICAD)</td>
</tr>
</tbody>
</table>

자금세탁과 테러자금조달 대응이라는 분야에서 제3장에서 논의된 국제기준체계 기구들 외에 중요한 역할을 하는 다른 국제기구들이 있다. 이러한 그룹들은 지역에 따라 또는 조직의 특수목적에 따라 구성되는 경향이 있다.

A. FATF 스타일 지역기구 (FATF-Style Regional Bodies: FSRBs)

FATF의 지역그룹 또는 FATF 스타일 지역기구는 각 지역에서 자금세탁방지와 테러자금조달대응 기준의 장려와 이행에 매우 중요하다. FATF가 전 세계를 무대로 하는 것처럼 FSRBs는 각각의 지역을 무대로 한다.

FSRBs는 FATF를 따르고 있고, FATF와 마찬가지로 자금세탁방지와 테러자금조달대응을 단일 목표로 한다. 이 지역기구들은 FATF의 40개 권고사항과 9개 특
법권고서장의 이행과 집행을 정리한다. 또한 취약점을 식별해서 적절한 조치를 취할 수 있도록 의도된 회원국의 상호평가를 관리한다. 마지막으로 FSRBs는 매년 생산되는 유형론 보고서(Typology Reports)에서 자금세탁 경향, 기법 및 기타 현황에 대한 정보를 회원국에게 제공한다.

FSRBs는 자발적이고 협력하는 조치이다. 그 기구의 규칙과 목표를 준수할 의사가 있는 그 지역 내의 어느 국가라도 회원으로 가입할 수 있다. FATF의 회원국 중에 및 개국은 FSRBs의 회원국이다. 투표권이 있는 회원국에 추가해 투표권이 없는 옵저버 지위도 기구의 활동에 참여하려는 국가에게 주어진다.

FATF에서 현재 속인 FSRBs는 다음과 같다.

1. 아시아 태평양 그룹(Asia/Pacific Groups on Money Laundering; APG) 2)
2. 카리브 FATF(Caribbean Financial Action Task Force; CFATF) 3)
3. 유럽회의(Council on Europe - MONEYVAL) 4)

4. 동남아프리카 자금세탁방지그룹(Eastern and Southern Africa Anti–Money Laundering Group: EASAMLLG)\(^5\)
5. 남미 FATF(Financial Action Task Force on Money Laundering in South America: GAFISUS)\(^6\)

특정 FSRBs는 자금세탁방지에 대한 자체의 협약이나 문서를 발간했다. 예를 들면 CFATF는 1990년 “아루바 권고사항(Aruba Recommendations)”을 발표했는데 이는 19개의 권고사항으로 카리브라는 지역적 관계에서 자금세탁에 대응하고, 40 개 권고사항을 보완한다.\(^7\) 이에 추가로 1992년 정관규정에서 “킹스턴 선언문(Kingston Declaration)”을 발표하게 되는데 이는 국제 자금세탁방지기준 이행에 대한 CFATF 각 정부의 서약을 확인하는 것이었다.\(^8\) 이와 유사하게 유럽회의는 1990년 “범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime(the Strasbourg Convention)”을 체결했다.\(^9\) 이것은 다른 각 지역에서 자금

4. 회원국: 알바니아, 안도라, 아르메니아, 아제르바이잔, 보스니아, 헤르체고비나, 불가리아, 크로아티아, 사이프리스, 체코, 에스토니아, 그루지아, 헝가리, 라트비아, 리히텐슈타인, 리투아니아, 말타, 몰도바, 폴란드, 루마니아, 러시아, 산마르ינו, 세르비아 몬테네그로 연방국, 슬로바키아, 슬로베니아, ‘마케도니아 구 유고슬라비아 공화국’, 우크라이나, 움직인 국가: 캐나다, 바티칸, 일본, 멕시코, 미국, 움직인 기구: 집행 위원회(Commission of the European Communities), 영연방 사무국(Commonwealth Secretariat), 유럽복합개발은행(European Bank for Reconstruction and Development(EBRD)), 국제자금세탁방지기구 FATF(Secretariat and Member Countries), 국제통화기금(International Monetary Fund:IMF), 인터폴 (Interpol), 역외은행감독기구(Offshore Group of Banking Supervisors:OGBS), 유통업립협의회회원 (Secretariat General of the Council of the European Union), 유엔범죄예방사무소(United Nations Crime Prevention and Criminal Justice Division), 유엔약약법죄사무소(United Nations Office on Drugs and Crime:UNODC), 세계은행, 세계관세기구(WCO).
5. EASAMLLG MOU에 서명한 회원국: 보츠와나, 케냐, 말라위, 모리셔스, 모잠비크, 나미비아, 나이지리아, 남아프리카공화국, 스페인, 술라와, 탄자니아, 우간다. Members who have not signed the EASAMLLG MOU are: 레소토, 잠비아, 잠바브웨. 움직인 기구: 영연방 사무국(Commonwealth Secretariat), FATF 사무국, 유엔국제자금세탁방지프로그램(UN Global Programme Against Money Laundering), 인터폴, 세계관세기구(WCO), 아프리카 개발은행(ADB), SADC 사무국, COMesa 사무국, EAC 사무국, 동아프리카 개발은행, 동남아프리카 개발은행(Eastern and Southern African Development Bank), 영국, 미국, 국제통화기금(IMF), 세계은행. http://www.easamllg.org.
세탁방지 기준 이행에 중요한 수단이 된다.

이기에 추가로 3개의 다른 FSRBs가 설립이 점토 중이거나 설립이 활발히 진행 중이다. 10) 3개의 새로운 지역은 다음과 같다.

- 중동과 북아프리카(The Middle East and North Africa: MENA)
- 중서부 아프리카(Central and Western Africa: GIABA)
- 유라시아

FATF로서 위의 기구들을 승인하기 전에 상호평가절차뿐 아니라 회원가입과 기타 운영상의 문제들은 해결되어야 할 필요가 있다.

B. Wolfsberg Group of Banks

Wolfsberg Group는 12개의 국제은행연합체로 주로 국제 프라이빗뱅킹 이슈를 대변한다. 12) 이 그룹이 결성된 장소인 스위스의 Chateau Wolfsberg를 따서 이름이 지어진 Wolfsberg Group은 프라이빗뱅킹에 대한 4개의 원칙을 세웠다.

1. 프라이빗뱅킹을 위한 자금세탁방지원칙(Anti-Money Laundering Principles for Private Banking)

이 원칙은 고객자산사와 금융기관의 프라이빗뱅킹 부서를 다룰 때 적절한 자금 세탁방지 지침에 대한 그룹의 관점을 대변한다. 이 원칙은 모든 계좌의 실소유자 입증, 특히 거래나 협의거래와 같은 추가 고객확인이 요구되는 상황을 포함하여 고객확인을 논의한다.

11. Ibid.; 예비회의는 다음 국가의 대표들이 참여했음: 알제리, 바레인, 이집트, 요르단, 쿠웨이트, 레바논, 모로코, 오만, 카타르, 사우디아라비아, 시리아, 튀니지, 아랍에미리트, 예멘.
이 11개의 원칙은 다음을 포함한다.

1. 고객 승인(Client acceptance): 일반 지침
2. 고객 승인(Client acceptance): 추가 고객확인/주의가 요구되는 상황
3. 고객 파일 업데이트
4. 특이거래나 혐의거래 식별 시에 업무절차
5. 모니터링
6. 관리 책임
7. 보고
8. 교육, 훈련 및 정보
9. 기록보존 요구사항
10. 예외 및 특이사항
11. 자금세탁방지 조칙13)

2. 테러자금조달예제에 관한 성명서(Statement on the Suppression of the Financing of Terrorism)

Wolfsberg 테러자금조달예제에 관한 성명서는 금융기관이 테러자금조달 방지에 공헌도를 높이려는 목적으로 할 수 있는 역할을 기술하고 있다.14) 이 성명서는 금융기관이 테러자금조달방지, 적발 및 정보공유를 통해 그것의 적절 시에 해당기관을 지원할 필요가 있음을 강조한다.

이 성명서는 “고객알기” 방침과 절차가 알려지거나 의심스러운 테러리스트의 명단 검색으로 강화되어야 한다고 규정한다. 또한 은행은 의심스러운 거래나 특이 거래를 볼 때마다 추가로 고객확인을 하여 정부를 돕는데 있어 적극적인 역할을 수행해야 한다. 추가 고객확인은 고객이 테러자금조달에 이 용된 것으로 해당기관에 의해 식별된 부문이나 활동에 연관된 경우 특히 중요하다.15) 이 성명서는 국제 협력 제고와 FATF 특별결재사항의 체택의 필요성을 지속적으로 지지한다.16)

15. Id., 원칙 4 및 5.
3. 환거래를 위한 자금세탁방지원칙(Anti-Money Laundering Principles for Correspondent Banking)

Wolfsberg Group는 국제적으로 환거래의 체결과 유지를 관리하는 14개의 원칙을 제정했다. 이 원칙들은 국제은행이 “위장은행”과 거래하는 것을 금지한다. 또한 이 원칙들은 은행이 환거래 고객과 관련해서 체택해야 하는 적절한 고객확인 수준을 확정하기 위해 고안된 환거래에 대한 위험기반 접근방식을 이용한다.

Wolfsberg 원칙들은 미래의 위험을 평가할 때 환거래은행이 고객 은행의 다음 사항을 고려하도록 요구한다.

- 은행주소
- 소유권 및 경영구조
- 사업 포트폴리오
- 고객기반(Client base)

이 위험 프로파일(profile)은 환거래 시스템을 제공할 시에 고객알기 절차 적용에 은행을 지원하도록 의도된 것이다. 이 원칙들은 또한 특이거래 또는 혼의거래의 식별과 사후조치를 규정하고 있다.

환거래에 관한 원칙은 다음과 같은 주제를 다루고 있다.

1. 시문
2. 환거래
3. 책임과 감독
4. 위험기반 고객확인
5. 고객확인기준
6. 강화된 고객확인
7. 위장은행
8. 중앙은행과 초국가적 기구

18. Id., 원칙 7.
19. Id., 원칙 5.
9. 지점, 자회사 및 계열사
10. 고객기반에 적용
11. 고객 과일 업데이트
12. 협의재 모니터링 및 보고
13. 자금세탁방지 프로그램과 통합
14. 국제동기부(International Registry) 관련 권고사항

4. 모니터링, 스크리닝 및 검색 절차

이 원칙들에서 통합이 위험기반 프로파일(profile) 접근방식을 이용하여 적절한 모니터링, 스크리닝 및 검색 절차\(^{21}\)을 개발하기 위해 처리되어야 하는 문제를 파악한다. 금융기관의 특정 부분에서 수행된 업무에 따라 개별 업무 영역에 대한 위험 프로파일과 금융기관 전체에 대한 위험 프로파일이 다를 수 있다.(예: 소매, 프라이빗뱅킹, 환거래, 증권중개인). 이 원칙에서는 또한 모니터링, 스크리닝 또는 검색 절차가 이 명백히 법안적인 행위로는 구별되는 특성을 가지는 고객과 거래를 식별하는데 국한되는 것을 인식하고 있다.

금융기관은 이 원칙 하에서 거래의 특이한 활동 및 패턴의 식별을 규정하는 적절한 절차를 수립해야 한다. 모든 경우에 특이 거래와 패턴이 의심스러울 필요가 있는지, 금융기관은 여러 사례 중에서 특히 자금세탁 가능성을 판단하여 특정 활동, 패턴 그리고 거래가 상격상 의심스러운지 여부를 분석하고 판단하는 능력을 갖추어야 한다.\(^{22}\)

이 원칙에서는 거래 활동들을 모니터링 하는데 있어 위험기반 접근방식의 이용을 권장한다.\(^{23}\) 또 외환이나 게제조치가 있는 경우에는 언제나 거래를 실제로 이행하기 전에 그 거래에 대한 점검이 포함되는 실시간 스크리닝 또는 필터링 절차의 이용을 권장한다.\(^{24}\) 기관의 위험기반 접근방식에 따라 과거사료 검색이 권장된다.

\(^{20}\) Id., 서문 색인(Introduction Index)
\(^{21}\) http://www.wolfsberg-principles.com/monitoring.html
\(^{22}\) Id., 원칙 3.
\(^{23}\) Id., 원칙 4.
\(^{24}\) Id., 원칙 4.1.
특이한 잠재 혐의거래에 대한 대부분의 지속적인 모니터링은 거래 모니터링 (transaction monitoring)으로 수행되어야 한다. 자금세탁 가능성에 대한 위험기반 거래 모니터링에서는 완결된 거래의 위험을 비교하기 위해서 자금세탁의 잠재 위험을 식별하고 위험의 등급을 매기는 수단을 제공하는 위험모델개발이 요구된다. 적절한 거래모니터링 절차에서는 그 거래가 특이한지 또는 의심스러운지 여부를 판단하기 위해 식별된 위험(거래의 지리적 위치, 제공된 상품과 서비스의 유형, 거래에 연루된 고객의 유형)에 대한 거래 정보를 자금세탁의 각기 다른 유형과 기타 불법 활동과 비교해야 한다.

C. 영연방사무국(The Commonwealth Secretariat)

영연방사무국(The Commonwealth Secretariat)은 국제적인 이슈에 대한 이해와 세계평화의 조장과 같은 다양한 주제에 대한 사람들의 공동 이해를 위해 협의하고 협조하는 53개의 독립국가로 이루어진 자발적인 연합체이다. 모잠비크를 제외한 모든 회원국은 적절한 혹은 간접적으로 영국의 지배를 경험했거나 또 다른 영연방 국가와 행정적으로 연관된 적이 있다.

영연방사무국(The Commonwealth Secretariat) 자금세탁방지와 테러자금조달대응과 관련하여 회원국들이 40개 권고사항과 9개 특별권고사항을 이행할 수 있도록 지원을 제공한다. 영연방사무국(The Commonwealth Secretariat)은 국내의 기구와 협력하고, 회원국들이 FATF 권고사항의 이행 시에 지원한다. FATF, CFATA, APG, 그리고 ESAAMLG의 움직이이다.

영연방사무국(The Commonwealth Secretariat)은 “금융부문의 자금세탁방지 및 테러자금조달 대응방안에 관한 안내서”.
D. 미주기구(美洲機構: Organization of American States) - CICAD

미주기구(OAS)는 시반구의 안보와 외교를 위한 지역기구이다. 전 미주의 35개국이 OAS 헌장을 비준했다. 미주기구는 지역 내에서 증가하는 마약밀매에 대응하기 위해 1986년 미주마약남용관리위원회(Inter-American Drug Abuse Control Commission :CICAD)를 설립했다. 시반구의 국가 수장들은 1994년에 들어서 지역 내의 자금세탁방지 노력을 포함하도록 CICAD의 역할을 승인했다. CICAD는 자금 세탁 뿐 아니라 마약밀매와 미약복용, 원료물질과 무기밀매의 확산에 대응하기 위한 종합적인 지역 전략과 기준이 되는 규정을 개발했다.29)

27. 매뉴얼은 영연방 사무국(Commonwealth Secretariat)에서 직접적으로만 제공함. 현재 온라인에서는 이용 불가함
2편: 효과적인 AML/CFT 구조의 구성요소

5장: 법률제도 관련 요구사항
6장: 예방조치
7장: FIU
8장: 국제협력
9장: 태러자금조달방지
제5장: 법률제도 관련 요구사항

A. 자금세탁의 범죄화
B. 테러와 테러자금조달의 범죄화
C. 압수, 몰수 및 권리의 상실
D. 포함되는(covered) 단체 및 개인의 유형
E. 감독 및 규제 – 신뢰성 관련 기준
F. FATF 권고사항 이행과 양립하는 법률
G. 해당기관 간의 협력
H. 수사
제5장 법률제도 관련 요구사항

A. 자금세탁의 범죄화
   1. 범죄의 정의
   2. 전제범죄의 범위
   3. 국제협력을 위한 국가 간 고려사항
   4. 주관적 요소(state of mind) – 지식 또는 의도
   5. 범인의 책임
   6. 전제범죄를 범한 자의 책임
   7. 변호사 수명료

B. 테러와 테러자금조달의 범죄화

C. 압수, 몰수 및 권리의 상실
   1. 범죄수익의 직간접적인 몰수
   2. 몰수된 재산의 집행
   3. 제3자의 책임
   4. 몰수의 국제적 양상

D. 포함되는(covered) 단체 및 개인의 유형
   1. 금융기관
   2. 지정된 비금융적업군
   3. 기타 잠재적으로 다루어질 개인과 단체

E. 감독 및 귀책 – 신뢰성 관련 기준
   1. 금융기관
   2. 비금융적업군

F. FATF 권고사항 이행과 양립하는 법률

G. 해당기관 간의 협력

H. 수사

각 국가에서 자금세탁방지제도가 국제기준을 충족하도록 하기 위해 취할 필요가 있는 조치는 다양하다. 국제기준체계를 준수할 국가와 달라 타국의 법률제도와 동일한 범죄를 채택할 입장이 아니라는 것을 인식하고 있다. 테러자금조달에 관한 요구사항은 제9장에서 논의될 것이므로 본 장에서는 주로 자금세탁방지와 관련된 8개 법률제도 관련 요구사항에 대해 논의하고자 한다.

이 8개의 요구사항은 본 안내서에서 논의의 편의성을 위해 법률제도 관련 요구사항으로 분류된다. 그러나 요구사항 중의 일부는 다른 범주에서도 쉽게 논의될 수 있다. 예를 들어 “감독 및 귀책 – 신뢰성 관련 기준”은 제6장 “예방조치”에서 논의될 수 있다. 요구사항 각각은 분류되는 범위와 판계없이 자금세탁에 대한 한 국가의 법률제도에 필요한 것이다. 각 국가는 이러한 요구사항 아래 국제기준 외에 고유의 문화적 상황, 법적 지침 및 현행과 일치하는 법률을 채택할 수 있다.
이 8개 요구사항은 다음과 같다.

- 비엔나협약과 판례협약에 따라 자금세탁의 범죄화
- 테러와 테러자금조달의 범죄화
- 억수 몰수, 권리의 상실, 범죄수익에 관한 법
- AML 법에서 다루어지는 단체와 개인의 혐의
- 금융기관의 신뢰성 관련 기준
- FATF 권고사항 이행과 부합하는 법
- 해당기관 간의 협력
- 수사

AML 관련 법률제도 요구사항과 본 안내서의 기타 국제기준들은 FATF에서 발행한 40개 권고사항에 근거를 두고 있다. 국가들을 이 요구사항에 대한 추가 설명과 평가방법에 대해 AML/CFT 방법론을 참조할 수 있다. 40개 권고사항은 권고사항으로 표현되어 있으나 단순한 목표이나 권고 이상이다. 이것은 국제기준을 이행하고 있는 것으로 간주되던 FATF 회원국 뿐 아니라 모든 국가가 준수해야 할 행동강령이다. 따라서 각각의 FATF 권고사항은 법조문을 만들 때 주의 깊게 검토되어야 한다.

A. 자금세탁의 범죄화

AML 제도 구축이나 개선은 국내에서도 자금세탁을 범죄로 만드는 것에서 출발한다. 자금세탁의 범죄화는 3개의 중요한 목표에 도움이 된다. 첫째 AML 관련 예방 조치의 이행을 강제한다. 둘째 결백한 것으로 보이는 행위를 명백한 범죄행위와 결부, 즉 불법수익을 처리하는 일 행위를 범죄로 만든다. 셋째 범죄화로 이와 같은 중요한 법집행과 관련하여 더 많은 국제협력의 기반을 구축한다. 범죄의 성질과 자금세탁범죄의 국제적 영향으로 인해 한 국가의 해당기관들은 강력한 국제협력 수단, 특히 사법공조체계에 의지하게 되어 보다 효과적으로 국제자금세탁행위를 추적, 범죄行长, 및 기소할 수 있다.

제5장 법률제도 관련 요구사항

1. 범죄의 정의


비엔나협약이 마약밀매라는 범주로 한정되어 있고, “자금세탁”이라는 용어를 사용하지는 않지만 비엔나협약에서 명시된 3가지 범죄는 자금세탁범죄의 기본을 이룬다. 그 범주는 다음과 같다.

i. 당해 재산이 마약밀매죄에서 유래한 것임을 알면서 그 불법출처를 은닉하거나 가정할 목적으로 또는 관련자의 범죄책임을 면하게 하는 것으로 혐의한 목적으로 행한 재산의 전환 또는 이체\(^{34}\)

ii. 당해 재산이 마약밀매죄에서 유래한 것임을 알면서 그 재산의 실제 상격, 출처, 소재, 처분, 이전, 권리 또는 소유권의 은닉 또는 가장\(^{35}\)

iii. 당해 재산이 마약밀매죄에서 유래한 것임을 알면서 그 재산의 취득, 소유 또는 사용\(^{36}\)

비엔나협약에 따르면 앞의 두 개의 범주는 국내법에 반드시 통합되어 적용되어야 한다. 세 번째 범죄는 의무는 아니나 각국의 헌법과 범죄도의 기본개념에 따른다.\(^{37}\)

비엔나 혐의의 자금세탁범죄 정의는 가장 널리 인정되고 있고, 자금세탁과 관련된 최근의 모든 국제 혐의에서 이용되고 있다.\(^{38}\) 비엔나협약의 정의를 이용해서 펠레모협약은 자금세탁의 정의를 다음과 같이 확대한다.

33) \textit{The Forty Recommendations}, Rec. 1.
34) \textit{Vienna Convention}, 제3조\((1)(b)\text{와 (c)}\).
35) \textit{Id.}, articles 3\((1)(b)\text{와 (c)}
36) \textit{Id.}, articles 3\((3)(c)\text{와 (c)}\)
37) \textit{Id.}
38) 제3장 UN, 비엔나협약 참조
a. 자금세탁이 고의로 범해진 경우
   i. 당해 재산이 범죄에서 유래한 것임을 알면서 그 불법출처를 은닉하거나 가정할 목적으로 또는 관련자의 범죄책임을 면하게 하는 것으로 협조할 목적으로 행한 재산의 전환 또는 이체
   ii. 당해 재산이 범죄에서 유래한 것임을 알면서 그 재산의 성격, 출처, 소재, 처분, 이전, 권리 또는 소유권의 은닉 또는 가정

b. 각 국가의 법제도의 기본개념에 따라
   i. 수수 시점에 당해 재산이 범죄수익임을 알면서 그 재산의 취득, 소유 또는 사용
   ii. 본 조항 상의 범죄에 기 dap, 연합 또는 공모, 시도와 교사 및 방조, 조정 및 사문제공 39)


39) 팔레모협약 제6조(1)항.
UN Model Legislation, 그리고 유엔의 자금세탁과 범죄수익 기준 법안(2000)(유엔의 기준범죄법안: UN Model Crime Bill)。

2. 전제범죄의 범위

a. 전제범죄로 포함되어야 하는 가장 넓은 범위의 범죄들

자금세탁의 전제범죄는 세탁 시에 자금세탁범죄로 이르게 하는 수익을 창출하는 기본 범죄 활동이다. 특정 범죄 활동을 자금세탁의 전제범죄로 지정하는 것은 국제기준이행에 필요하다. 국제기준이 발전할 때 따라 보다 넓은 범위의 범죄가 자금세탁의 전제범죄로 지정되는 사례가 증가하고 있다.


최근 40개 권고사항에 나오는 전제범죄의 범위는 이전의 것보다 훨씬 더 범위가 넓다. 접문의 권고사항 1은 자금세탁의 전제범죄로써 가장 넓은 범위의 범죄를 포함시키기 위해 국가들은 자금세탁범죄를 모든 중대범죄에 적용해야 한다는 폐쇄협약과 1996년 판 40개 권고사항의 조항을 인용한다. 전제범죄를 기술하는 여러 방법을 제시한 후, 권고사항 1에서는 (최소한) 국가는 “각각의 지정

46) 졅레협약 제2조(h); 유럽의회, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime)(1990) 제1조(e).
47) 비엔나협약 제3조.
48) 졅레협약 제2조(a).
50) Id.
한 범위의 범죄 중의 범죄들(a range of offenses within each of the designated categories of offenses)”을 반드시 포함해야 한다고 명시한다.31) 지정된 범죄 범위는 20개이다.

- 조직범죄단체 및 공갈에 가담
- 테러자금조달을 포함한 테러
- 인신매매 및 인도자 밀입국
- 아동성착취 포함 성착취
- 마약 및 황성신동물질 불법매매
- 불법무기매매
- 상품 및 기타 불법 불법매매
- 부패 및 뇌물
- 사기
- 화폐위조
- 상품위조 및 표절
- 환경범죄
- 살인, 성매
- 남자, 감금 및 인질
- 강도 또는 절도
- 밀수
- 강탈
- 위조
- 저작권 침해
- 내부자인력 및 추가조직32)

전체범죄 기술과 관련하여 2가지의 중요한 점이 있다. 첫째 요구사항은 지정된 범위의 범죄 중에서 “일련의 범죄들”을 포함하는 것이다. 예를 들면 한 국가는 “강도 또는 절도” 항목에서 단지 “자동차 절도”만을 전체범죄로 지정하고 기타 물품의 절도에서 벌어진 수익을 배제한다면 이 권고사항을 이행하지 않는 것이다. 둘째 국가들은 위의 리스트에서 범죄를 정의하고, 전체범죄로 만다는 범죄의 특정 요소의 실질을 규정하는 방법에 대해 제한권이 주어진다.

31) Id., Rec. 1.
32) 40개 권고사항의 용어집에 있는 “지정된 범죄 범위”의 정의 참조
필수 요구사항은 위의 리스트 상의 행위를 통해서 수익을 창출하는 것을 범죄화하는 것이다. 또한 위의 리스트에서 이는가는 용어가 형법에서 정확하게 기술될 필요는 없다. 예를 들어 국가들 중에는 “사기”로 지정된 특정 범죄가 없으나 “절도”와 같은 다른 범죄에서 사기성 행위를 범죄화하는 경우도 있다. 사기성 행위로 인한 범죄 수익의 세탁에 대해 유죄판결을 받는 것이 가능한 것을 감안하면 그 국가는 그 행위를 기술하거나 분류하는 방법이라는 측면에서 제한권을 가지는 셈이다.

이 제한권의 한 가지 예의사항은 테러자금조달이다. FATF에서는 9개 특별권고 사항에서 특히 테러자금조달, 테러행위 및 테러조직이 자금세탁의 전제범죄로 지정되어야 한다고 요구한다. 오로지 교사 및 방조, 미수 또는 공모 관련 범에 근거해 이러한 행위들만 범죄로 규정하는 것은 허용되지 않는다.

b. 전제범죄 기술 방법

FATF는 자금세탁 전제범죄가 되어야 하는 범죄행위의 유형 또는 범위를 기술하지만 개별 국가는 범죄화를 하는 법적 방식을 결정할 권한이 있다. 국가는 다음을 참조하여 법적 방식을 결정할 수 있다:

▶ 모든 범죄
▶ 중대범죄의 범위 또는 전제범죄에 해당되는 처벌과 관련된 기준금액(기준금액 접근방식)
▶ 전제범죄의 리스트, 또는
▶ 이 모든 접근방식의 결합

국가가 기준금액 접근방식을 적용하는 경우 전제범죄는 최소한 국내법 하에서 “중대범죄”로 지정된 모든 범죄 또는 최대형이 1년 이상 침해로 처벌되는 범죄(최소한 처벌을 하는 국가에서도 6개월 이상)를 포함해야 한다. 중대범죄 범죄의 예로는 “기소대상범죄”(즉결심판대상범죄에 대비되는 개념), “죄”, “경범죄에 대비되는 개념”, “범죄”(위법행위(deeds)에 대비되는 개념)가 있다. 전제범죄 지정에 기준금액 접근방식을 이용하는 국가들은 추가되는 최소 2개의 요구사항을 따라야 한다.

3. 국제협력에 관한 법국가적 고려사항

위에서 적정된 바와 같이 FATF 권고사항은 자금세탁의 전제범죄가 되어야 하는 최소한의 범죄 범위를 지정하지만, 이 범위를 넘어가기를 장려한다.54) 범위 확장과 범죄화의 방식은 각 국의 사례에 달리있다. 그러나 한 국가의 확장 범위와 범죄화의 방식은 국제협력과 타국 당국과의 정보교환 능력을 보여주는 것이다.

전제범죄는 국내에서 발생한 경우는 물론이고, 다른 나라에서 발생한 것까지 확대되어야 하는데 권고사항 1에서는 그 행위가 다른 국가에서 범죄로 식별되고 국내에서 발생했어도 범죄가 되는 경우에 해당한다고 명시하고 있다.55) 이것은 소위 "쌍방가범성(dual criminality)"인데 다른 국가에서의 행위가 그 국가와 국내에서 전제범죄이어야 한다는 것이다. 그러나 이것은 최소한의 기준이다. 권고사항 1에서는 또한 국가들이 자금세탁의 유일한 기소 조건이 다른 국가에서 행해진 행위가 그 나라의 전제범죄여부와는 상관없이 만일 국내에서 발생한 경우 전제범죄가 될 경우에는 기소할 수 있도록 규정한다.56) 이러한 접근방식은 그 행위가 범죄진 출국에서는 전제범죄가 아니였지만 수익이 세탁된 국가에서는 범죄였던 행위에 의해 범죄수익이 발생한 경우에 기소를 가능하게 한다.

FATF가 국가에게 반드시 이 접근방식을 채택하도록 권고하지는 않지만 쌍방가범성이 부적합 시에는 사법공조를 제공하도록 권고한다.57)

FATF는 또한 쌍방가범성이 사법공조나 범죄인 인도에 요구되는 경우 그 요구 사항은 양국이 기본 행위를 범죄화하고 있으면 범죄가 각기 다른 국가에서 동일한

55) Id.
57) Id. Rec. 37.
4. 주관적 요소 - 인식 및 의도

비엔나협약에 따르면 범죄자의 고의성 - 자금세탁범죄를 행할 시에 범죄자의 의도 또는 목적 - 은 수익이 전체범죄의 산물임을 "아는" 것을 의미한다.58) 그러나 범죄자가 당해 재산이 범죄행위의 수익이었거나 범죄행위에서 취득되었다는 것을 알 수 있었을 경우 책임의 범위가 "부주의로 인한 자금세탁(negligent money laundering)"으로까지 확대될 수 있다.

국가들은 자금세탁범죄와 관련된 "심리상태"를 판단할 시에 응산이 다양하다.59) 한 국가의 범죄에서 재산의 불법출처에 대한 실질적인 지식 또는 불법출처에 대한 단순한 의심이 자금세탁의 유죄판결에 필수적인 심리상태 또는 정신적 요소가 되는지를 결정할 수 있다. 이 범죄에서 또한 "알았어야 했다"는 유죄 기준을 받아들일 수도 있다. 이 정의가 자금세탁 과실의 한 형태가 된다.60) 이 일반적인 의도 관련 요구사항에 추가하여 범죄는 재산의 "불법출처를 은닉하거나 가리키는 의도 또는 "관련자의 행위에 대한 법적 책임을 면제하" 협조하려는 특별한 의도(목적)를 명시할 수 있다.61)

유엔 기준 법률(UN Model Legislation)에 따르면 재산이 범죄행위에서 유래했다는 실제 지식 또는 "그렇게 믿을만한 사유가 있는 것"은 소위 자금세탁의 주관적 요소가 된다.62) 그러나 기준범죄법안(Model Bill)에서는 당해 재산의 출처, 성질, 소재, 취득, 이전 또는 소유권의 은닉 또는 가장과 같은 구체적인 의도가 특정한 자금세탁범죄에 적용될 수 있는 것으로 기술하고 있다. 또한 특정 자금세탁범죄가 성립되어 위해서는 관련자의 행위에 대한 법적 책임을 면제하려 하여 협조하려는 구체적인 개인의 의도를 명명하는 것이 요구할 수도 있다.63)

58) 비엔나협약 제3조(b)(i).
60) Id. Article 1.1.1.1
61) Id., at subparagraph (a).
62) UN 기준범죄법안 섹션 17(a).
“주관적 요소”에 대한 폭넓은 정의는 OAS 기준 법규(OAS Model Regulations)에서 제택되었다. 이 기준 법규에서는 3가지의 주관적 요소를 다루고 있다: (i) 피의자는 당해 자산이 협약에 규정된 범죄행위의 수익임을 알고 있었다; (ii) 피의자는 당해 자산이 범죄 활동의 수익에 취득되었음을 알았어야 했다; (iii) 피의자는 의도적으로 범죄수익의 상실을 무시했다. 이 세 번째 법규에서 피의자는 범죄수익의 출처를 “몰랐거나” 또는 “알았어야 했지만” 당해 자산의 출처를 의심하고, 그 의심을 검증하거나 해소하기 위한 추가 조사를 하지 않기로 선택했다. 이러한 점에서 피의자는 범죄수익의 성질을 모르는 채로 있기로 의도했거나 조사나 문의로 범죄에 대해 “알 수 있었음에도” “고의로 알고 하지 않았다.” 유죄라는 관점에 봤을 때 이 주관적 요소 기준은 과실과 의도에 대한 특정 지식기준의 범위 사이에 속한다. OAS 기준 법규(OAS Model Regulations)에서는 추가로 이 3가지의 유죄가 되는 주관적 요소가 객관적이고 사실 정황에서 유추될 수 있다고 규정하고 있다.56)

마지막으로 표면적으로는 정상적인 것으로 보이는 활동에 참가하고 있는 개인의 심리상태를 중명하는 것은 매우 어려울 수 있다. 따라서 비엔나협약, 팔레모협약, 40개 권고사항과 다수의 기타 법규에서는 국가의 법으로 객관적인 사실 정황에서 요구되는 심리상태의 유추가 허용되어야 한다고 명시하고 있다.57) 그 객관적인 사실 정황이 상황과 맞는 경우 심리상태와 관련된 요구사항은 충족된다.

5. 범인의 책임

범인이 자금세탁을 하는 경우가 종종 있다. 그러나 범인의 책임이라는 개념은 나라마다 크게 차이가 있다. Common Law를 제택하는 나라들은 범인이 형사책임 법을 따르도록 한다. 대륙법을 제택하는 나라들은 형사법에서 범인이 다루어지지 않을 수도 있다. 따라서 Civil Law를 제택하는 나라의 법이 허용되는 경우 범인의 형사책임을 명시하도록 규정되는 것이 검토되어야 한다.

56) Id., at subparagraph (b).
57) OAS Model Regulations, 제2조.
58) Id., at subparagraph (5).
59) 비엔나협약 제3조(3); 팔레모협약 제6조(2)(f); The Forty Recommendations, Rec. 2; 유럽밖회, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) 1990 조호제(2)(c).
FATF는 직원뿐 아니라 법인 자체도 법률제도의 일반원칙 하에서 가능하다면 언제라도 형사책임 대상이 되도록 권고한다.68) 법률제도 또는 법률에서 법인이 형사책임 대상이 아닌 경우 행정 제재조치가 충분히 이를 대신할 수 있다.

유엔 기준법(UN Model Legislation)은 법인의 형사책임에 대해 명시하지 않는 다. 그러나 법인에 기타 제재조치 적용69) 및 법인의 대리인이나 대표가 법인을 위해 또는 법인의 이익을 위해 자금세탁범죄를 범한 모든 경우에 기타 제재조치의 적용을 명시하고 있다. 유엔기준법 상의 제재조치에는 벌금, 특징사업중지, 폐쇄 또는 철산, 그리고 결정의 공표(publication of rulings)가 있다.70) 유엔기준법에서 는 위한 제재조치를 형사제도로 분류하지 않고, 이 제재조치가 그 행위에 대한 법인의 대리인이나 직원의 개인적인 책임의 적용을 제한하지 않아야 한다.71)

형사책임은 OAS 기준 범규에서 자연인과 동일한 근거로 법인에게까지 확장된다. 한 조항에서는 특히 “person”的 규정을 위해 “권리 취득이나 계약체결이 가능한 법인, 협력회사, 신탁 또는 부동산, 합작회사, 협회, 기업연합, 합작기업 또는 기타 협병되지 않은 조직을 포함한 자연인 또는 법인”을 의미하는 것으로 규정하고 있다.72) UN 기준범죄법안(UN Model Crime Bill)에서 “person”이라는 용어는 자연인과 법인 돈 다를 포함하는 것으로 정의되고 있다.73) UN 기준범죄법안(UN Model Crime Bill)에서 “person”을 OSA의 정의보다 좁은 의미로 규정하고 있기는 하나 이전히 법인의 형사책임원칙을 인정하고 있다.

6. 자금세탁 전재범죄를 범한 자의 책임

자금세탁 책임이 불법적으로 취득한 수익을 세탁한 자뿐 아니라 전재범죄를 저지른 자에게 확장되는지 여부가 중요하다. 일부 국가에서는 전재범죄를 범한 자가 자금세탁활동에 가담하지 않은 경우 범죄수익세탁에 대한 책임을 묻지 않는다. 이 접근방식의 기본적인 이론적 설명은 범죄자가 범죄 활동의 법적 책임으로부터 피하는 행위에 대해 처벌하는 것은 일반부패를, 즉 단일 범죄에 대한 다중 처벌에 해당할 수 있다는 것이다.

68) The Forty Recommendations, Rec. 2; OAS 기준법 제15조.
69) UN 기준법 4.2.3.
70) Id.
71) Id.
72) OAS 기준법 제1조(6).
73) Section 2(1).
다른 국가에서는 범죄행위(the conduct)와 법적 책임 최외에 따른 위험이 전체
범죄행위는 구별된다. 그것을 근거로 전체범죄를 저지른 자에게 불법수익세탁에 대한
책임을 지낸다. 이 접근방식에는 실질적인 이유가 있다. 전체범죄를 저지른 자를
자금세탁 책임에서 면제해주는 것은 범죄수익을 처리할 때 그들은 책임에서 면제
되는 반면 그들의 행위로 제3자를 불리하게 할 수 있다. 이것은 전체범죄가 국가
에서 행해져 제3자를 자금세탁행위로 기소하는 국가의 관할권을 넘어서는 경우 발
생할 수 있다.

전제적으로 이 분야의 일반적인 국제기준에서는 자금세탁에 적극적인 참여여부
와는 관계없이 범죄자의 범죄 활동수익의 세탁에 대해 그에게 책임을 묻는 것을
허용하는 넓은 의미의 자금세탁에 대해 규정하고 있다.74) 그러나 이 기준은 역사
국가마다 편차를 허용한다.

7. 변호사 수임료

변호사들은 이제는 AML/CFT 제도에 포함되는 지정된 비금융전문직에 속한다.75)
이 분야의 다른 전제범죄의 기초를 마련하는데 있어 특별한 주의가 요구된다.

법에서 자금세탁의 전제범죄는 매우 넓게 정의되어 있어 전체적으로 범죄 활동
에 있어서 수익의 사용과 관련된 모든 거래가 포함된다. 이와 같은 넓은 범위를
검안하면 이 법률은 변호사 수임료 수수를 범죄화하는 효과를
낼 수 있다. 이것은 정당한 절차에 대해 유해한 문제를 야기한다.

형사재판에서 피의자의 정당한 변호에 대한 권리가 공정한 재판에 대한 권리의
한 측면으로 이미 규정되어 있는 것을 고려하면 국가들은 자금세탁범죄의 범위를
정하는데 있어 주의를 기울여야 한다.

국가들은 또한 변호사의 업무가 재판에서 피고인을 변호하는 것뿐만 한정되거나
변호와 연관되어서만 이루어진다면 단순히 변호에 대해서는 전제적인 형사책임에
서 변호사를 면제해주는 조항을 고려하고자 할 수 있다.76)

74) 유엔 4조 2조(4); 유럽의회, 범죄수익의 세탁, 수익, 억류 및 물수에 관한 협약(Convention on
75) 기준범죄법안 법률 17: OAS 기준법 제2조.
76) 5장의 지정된 비금융전문직 참조
제5장 범죄의 벌재와 관련 요구사항

피고인의 공정한 재판을 받을 권리에도 불구하고, 변호사들은 또한 금융제도를 보호하고, 업무의 신뢰성에 관한 의무를 지닌다. 만약 변호사가 그의 수입료가 범죄 활동 유래한 것을 알고 있다면 변호사(attorney)는 업무의 신뢰성 기준을 준수하고, 특히 재판에서 피고인 변호 사외 고객에게 다른 서비스를 제공하는 경우 세탁된 자금을 무역해고 받아서는 안된다.

B. 테러와 테러자금조달의 범죄화

다른 범죄자와 마찬가지로, 테러자금조달자는 자금의 출처가 합법적이라도 하더라도 자신의 활동을 지원하는데 필요한 자금을 은닉하기 위해 국내 및 국제 금융제도를 이용할 수 있다. 모든 측면에서 테러와 테러자금조달을 범죄화하는 것은 테러조직의 자금이 제도권으로 유입되는 것을 방지하여 테러조직의 세력을 약화시키는 실질적인 방법이다. 또한 국가의 테러자금이 국내에 있어 몰수될 수 있도록 법으로 적발할 수 있도록 할 필요가 있다. 이것은 또한 테러 시도를 좌절시킨다.

FATF는 9개 특별권고사항에서 국가들이 테러자금조달, 테러행위 및 테러조직을 범죄화하고, 자금세탁의 전체범죄로 지정하도록 촉구한다.77)

위의 "전체범죄 범위"에서 지적된 바와 같이 FATF는 지정된 범죄의 범위 중의 하나가 테러자금조달을 포함한 테러임을 규정한다.78) 따라서 40개 권고사항과 9개 특별권고사항을 취합하여 테러, 테러행위, 테러조직 및 테러자금조달 각각은 국가의 자금세탁법에서 전체범죄로 관리되어야 할 것이다.

C. 압수, 몰수 및 권리의 상실(Secizure, Confiscation, and Forfeiture)

국제적으로 발생하는 범죄와 테러자금조달에 대한 최근의 접근방식은 테러리스트들이 범죄 활동 수익을 내지 못하고, 자금에 접근하는 것을 막는 것이다. 이와

76) 유럽의회, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime) 설명서 보고서(Explanatory Report), para. 33. 이 기준법과 규정은 이 점에 대해서는 아무런 유효이 없음. UN 기준법: UN 기준범죄법안; OAS 기준법 참조.
같은 목적을 효과적인 몰수법이 없이는 달성될 수 없으므로 당국이 범죄자와 테러리스트들에게서 불법적으로 취득한 수익을 영구적으로 박탈할 수도 있다.\(^79\)

1. 범죄수익의 적간접적인 몰수

FATF는 비엔나협약과 폴레모협약에 따라 국가들이 범죄수익몰수에 대한 폭넓은 해석을 허용하는 법을 채택하도록 권고한다.\(^80\) 과거에는 대부분의 법제도에서 몰수는 범죄에서 유래한 수익과는 반대로 주로 살인무기와 같은 범죄에 이용된 수단, 또는 마약매매 시의 마약과 같은 범죄의 대상에 한정되었다. 비엔나협약과 폴레모협약에서 “범죄수익”이라는 용어는 “범죄에서 직접 또는 간접적으로 유래한 또는 취득된 모든 종류의 재산”으로 정의한다.\(^81\) 많은 국가들이 지금은 범죄수익의 대체물 그리고 자금이 국제금융제도권 내외로 이체될 수 있는 용이성이라는 측면에서 몰수 가능한 재산에 대해 위와 같은 보다 넓은 정의를 받아들였다.

FATF는 국가들이 세탁된 재산, 세탁 및 전체범죄의 수익, 세탁에 이용되었거나 이용이 의도된 수단 그리고 상응하는 가치의 재산의 몰수를 허용하는 법을 채택하도록 권고한다.\(^82\) 이와 같은 넓은 정의는 구체적으로 명시된 재산만이 몰수대상이 되는 경우 몰수명령 발령 전 또는 명령의 집행 전에 범죄자들이 재산을 다른 형태로 전환할 가능성이 높기 때문에 유용하다. 범죄자들은 또한 당국의 힘이 미치지 않는 곳까지 재산을 이체하거나 불법적인 출처의 재산과 혼화한 가능성이 높다. 몰수에 대한 전통적인 이해가 몰수명령을 쓸모없게 만들 수도 있는 이렇게 다양한 상황에 대처하기 위해서 국가들은 “가치 몰수(value confiscation)” 접근방식 채택을 고려해야 하는데 이 접근방식으로 정부는 불법적으로 취득한 수익의 가치에 상응하는 범법자의 재산을 몰수할 수 있는 권한이 주어진다.\(^83\)

2. 몰수된 재산의 집행

몰수명령의 효과적인 집행은 관련당국이 몰수 대상이 될 수 있는 재산을 식별,

---

79) 비엔나협약 제1조(2), 유럽수호, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime)(1990) 제1조(2).
80) The Forty Recommendations, Rec. 3.
81) 비엔나협약 제1조(3); 폴레모협약 제2조(3).
82) The Forty Recommendations, Rec. 3.
83) 비엔나협약 제5조; 유럽수호, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime)(1990) 제2조.
추적 및 평가하는데 필요한 권한을 보유하도록 요구한다.84) 다음에는 관련당국이 상업 및 금융기관의 공개를 요구하거나 압수할 수 있는 권한을 보유하도록 요구한다.85) FATF는 특히 은행보험법이나 기타 보안법령이 제정되어 홀수명령 집행을 위한 공개나 압수에 징계가 생기지 않도록 권고한다.86)

오늘날 자물은 컴퓨터의 자료를 누르는 것으로 국외 송금이 가능해졌다. 따라서 당국들은 예방조치를 취할 수 있는 권한도 주어져야 한다. 예를 들면 홀수대상이 될 수 있는 자료를 동결하고 압수할 수 있어야 한다. 이 권한은 자금세탁방지법을 위한 효과적인 법집행제도에 필요한 조건이다.87) (자산의 동결, 압수 및 홀수에 관한 상세한 논의는 제9장, 테러자산의 동결과 홀수 참조. 그 논의는 AML 관련 자산에도 동일하게 적용된다)

3. 제3자의 책임

홀수에 관한 국제법이 제3자가 보유한 재산의 홀수를 차단하지 않는 반면 FATF와 여러 국제협정에서는 제3자가 재산 홀수 차단은 국가가 선의의 제3자의 권리를 보호하기 위한 조치를 취하도록 요구하여 가능하다.88) 계약을 체결하고, 그 계약이 홀수를 집행하는 국가의 권한을 침해할 수 있다는 것을 알거나 또는 알고 있어야 하는 제3자는 선의의 제3자가 아니다. 한 국가의 법은 이러한 상황에서 이와 같은 계약의 유효성에 대한 문제에 대응해야 한다.89)

OAS 기준 법규(OAS Model Regulations)에 따르면 관련 당국은 법적절차(소송)에 대해 통보하도록 요구한다.90) 이러한 통보를 받은 제3자는 홀수대상인 재산에 대
해 권리를 주장할 수 있도록 허용되어야 한다. 기존 법규에 따르면 법인이나 기타 해 당기관은 청구가 (1) 재산에 대한 적절한 법적 권리 중지를 가지고 있는 경우, (2) 전세범죄에 가담, 연합 또는 기타 방법으로 관련되지 않은 경우, (3) 불법적 목적에 재산이 이용된 것임을 알지 못했고, 그것의 이용에 자발적으로 동의하지 않은 경우, (4) 몰수절차를 최적할 수 있도록 만들어진 권리를 취하지 않은 경우, 그리고 (5) 재산의 불법 사용을 막으려는 합리적인 노력을 한 경우 청구자(claimant)에게 재산을 반환해야 한다.

유엔범죄기준법안(UN Model Crime Bill)에서는 선의의 제3자의 관해 문제를 처리할 때 (1) 제3자가 전세범죄에 연관되었다고 법원이 판단하는 경우, (2) 충분히 고려하지 않고 그 재산을 취득한 것으로 법원이 판단하는 경우 또는 (3) 재산의 불법출처를 알면서 취득한 것으로 법원이 판단하는 경우 법인이 판단하는 경우 법인이 재산에 대한 제3 자의 청구를 거부할 수 있다고 명시하고 있다.91) 비교하자면 UN기준법안(UN Model Legislation)은 좀 더 엄격한 기준을 적용하는데 이것은 재산에 대한 청구를 거부하는 근거로 전세범죄에 연루를 요구하지 않는다.92)

4. 몰수의 국제적 양상

국내용으로 효과적인 몰수제도를 구축하는 것은 수없이 많은 국제자금세탁 활동의 중심에서 수익성을 제거하려는 첫 번째 단계일 뿐이다. 자금세탁체계의 성공에 매우 중요한 두 번째 단계는 국경 간 몰수명령을 집행할 공조체계를 구축하는 것이다. 국가들은 자금추적, 확인, 동결 및 압수와 같은 조치를 이용해 해당 기관이 다른 국가의 몰수요청을 이행하도록 할 수 있다.

국제협력은 하는 등의 하나는 국가들의 자산품힘 협정 구축이다. 몰수된 자산 처분에서 일반적인 원칙은 자산 처분이 몰수명령이 이행된 국가의 국내법과 규정에 속해야 한다는 것이다.93) 그러나 국제법체계에서는 국가들이 수사와 몰수 과정에서 협력했던 나라들 간에 몰수된 재산의 공유에 대해 명시하고 있는 사법공조체계를 구축하도록 권고한다.94) 국제법체계는 또한 범죄추적에 현장하고 있는 정부 간 가구에 몰수된 자금의 일부를 할당하도록 권고한다.95)

91) UN 범죄기준법안 족선 36. 이것은 관습법을 제거하는 국가를 위한 기준법
92) UN기준법 4.2.9 절조. 이것은 관습법을 제거하는 국가를 위한 기준법
93) 범죄협약 제5조(a); 유럽의회, 범죄수익의 세탁, 수색, 압수 및 몰수에 관한 협약(Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime)(1990) 제15조, 페라모협약 제14조(1).
94) 범죄협약 제5조(b); 페라모협약 제14조(3)(b); OAS 기준 법규 제7조(d).
95) 범죄협약 제5조(b)(i); 페라모협약(2000) 제14조(3)(a); OOA 기준규정 제7조(e).
D. 포함된(covered) 단체와 개인의 유형

FATF 권고사항에서는 금융기관과 비금융 전문적 자금세탁과 테러자금조달을 방지하기 위한 많은 의무를 부과한다. 이 권고사항에서는 또한 이와 같은 예방 조치를 적합한 시에 예외사항을 명시하고 있다. 따라서 국가가 결정해야 할 중요한 사항은 어느 단체와 개인이 어느 요구사항에 적용되어야 하는가이다. 이에 따라 예방조치의 일부가 "지정된 비금융전문적"에 한정되어 적용되는 반면 모든 예방조치는 "금융기관"에 적용된다.

1. 금융기관

자금세탁자들과 테러자금조달자들이 금융기관을 이용해야 한다는 것은 사명하다. 금융기관은 그들에게 국내외적으로 다른 금융기관들 간에 자금을 이전할 수 있는 수단을 제공한다. 금융기관은 또한 자금세탁과 테러자금조달 과정에 이용된 의사를 완전하고 자산을 지불하는 수단을 제공한다. 금융기관의 유형과 업무역량은 금융기관마다 매우 다르다. FATF 권고사항에 따르면 "금융기관"이라는 용어는 "개인을 위해 다음의 활동 또는 업무 중 하나 또는 그 이상을 사업으로 수행하는 개인 또는 단체"로 규정된다.

- 대중에게서 예금과 기타 상환 가능한 자금 수령(프라이빗 뱅킹 포함)
- 대출(고객 대출, 모기지 대출, 상환청구권을 가지고 있거나 가지지 않은 팩토링(factoring) 포함); 그리고 상업거래 융자(위약금 포함)
- 금융리스(Financial leasing)(고객 상품의 금융리스 계약)
- 자금 또는 가치 이전(공식적·비공식적 방법(대체송금활동 등) 포함)
- 지급수단 발행 및 관리(예: 신용카드 및 직불카드, 수표, 여행자수표, 우편환 및 은행 어음, 전자화폐)
- 금융보증 및 재정적 의무 이행 약속
- 다음의 거래
  a. 단기금융상품(수표, 환여융, CD 과생상품 등)
  b. 외환

96) The Forty Recommendations, 권고사항 5-25 참조
97) Id.
98) 특별권고사항 VI 그리고 VII에 대한 해설서 참조
c. 환율, 이자율 지수상품(exchange, interest rate index instrument)
d. 양도성 증권
e. 상품선물거래
   ▶ 주식발행과 관련된 금융서비스 제공에 참여
   ▶ 개별 및 집합(collective) 포트폴리오 관리
   ▶ 타인을 대신해 현금 또는 유동성 증권(liquid securities) 보관 및 관리
   ▶ 투자이외에 타인을 대신해 자금 또는 금전 투자, 관리
   ▶ 생명보험과 기타 투자 관련 보험의 인수 및 투자(placement)(이것은 중개인과
     보로개와 같은 보험인수와 보험증권에 적용된다) 그리고
   ▶ 환전(99)

이것은 제도적이거나 고정된 정의라기보다는 기능적인 정의이다. 정의의 기준은
업무의 명칭이나 그 업무가 지정되는 방식이 아닌 단체나 개인이 고객을 위해 위
의 활동이나 업무를 수행하는가이다. 예를 들면 대중에게서 예금을 받거나 대출을
해주는 개인이나 사업체는 은행이라고 불리는 것과는 관계없이 해당된다. 많은 경
우 법이나 규정에서는 위의 업무를 인가받은 금융기관에서하도록 제한할 것이고,
이런 상황에서 AML/CFT 규정을 인가받은 금융기관에 적용하는 국가는 그 기준
을 충족하게 되는 것이다. 반면 그 업무가 법적으로 허가를 받지 않은 단체에 의
해 수행되는 경우 AML/CFT 규정은 이 단체에도 적용되어야 할 것이다.

이 요구사항에는 두 개의 조건이 있다. 첫째 위에 언급된 금융활동은 간행적으
로 또는 명확히 한정된 범위에서 수행되어 자금세탁위험이 매우 적은 경우 국가는
자금세탁 요구사항의 전 항목 또는 실제로 한 가지도 적용하지 않는 것으로 결정
할 수 있다.100 이와 같은 경우에 해당하는 예로는 손님에게 간행적으로 매우 한정
된 외환환전서비스를 제공하는 호텔이나 긴급 상황에서 해외 고객에게 전신송금을
할 수 있는 여행사가 있다.

둘 번째 조건은 “압력하게 한정되고 충분한 이유가 있는 상황”과 “자금세탁 위
험이 낮다고 증명됨” 때에 국가는 위에 언급된 금융활동에 40개 권고사항 일부 또
는 전부를 적용하지 않기로 결정할 수 있다.101) FATF는 어떤 상황인지에 대해 명
확한 지침을 제공하지 않는다. 다만 국가들은 위험기반 접근방식을 채택하도록 권

99) The Forty Recommendations, 금융기관
100) Id.
101) Id.
고되는데 이 방법은 고위험 분야에서 조치를 확대하거나 엄격하게 완전히 고치는 AML/CFT 위험에 근거해 조치를 강소할 수 있게 한다. 금융활동은 일반적으로 자금세탁위험이 낮다는 연구가 이루어진 후에 배제되거나 한정된 규율에 따르나한다. 위에 언급된 금융활동 전부는 AML 요구사항 전체를 적용해야 한다는 것이 상황 가정의 출발점이다.

2. 지정된 비금융전문직

FATF 권고사항은 2003년 최초로 40개 권고사항의 범위에 지정된 비금융전문직을 포함하도록 개정되었다. 비금융전문직에 적합 가능한 요구사항은 더욱 제한적이고, 금융기관보다는 보다 제한된 환경에서 적용된다. 어느 요구사항이 어느 비금융전문직에 적합되는지에 관한 세부사항은 제6장에서 다루어지겠으나, 국가들은 AML/CFT 조항의 범위에 다음과 같은 단체와 개인을 포함하도록 요구한다.

- 카지노(인터넷 카지노 포함)
- 부동산 중개인
- 귀금속 금리
- 개업할거나 공동으로 경영하거나 또는 회사에 고용된 변호사, 공증인, 기타 독립적인 법률전문직, 그리고 회계사. 기타 유형의 사업체의 고용인인 “내부”적이나 정부기관에 종사하는 직을 임기는 것은 아니다. 이들은 이미 자금세탁과 관련된 조치 대상일 수도 있다.
- 신탁 또는 법인설립업체는 권고사항이 아닌 다른 곳에서는 다루어야하지 않은 모든 개인이나 사업체를 일컫는다. 이업체는 제3자에게 다음과 같은 서비스를 제공한다.
  a. 법인설립대행
  b. 회사의 이사 또는 충무부정(secretary), 합자회사의 파트너, 또는 기타 법인과 관련하여 유사한 직위 대행(또는 타인이 대행을 하도록 주선)
  c. 회사, 합자회사 또는 기타 법인이나 법률계약을 위해 사업장 주소나 숙박시설, 시설 또는 우편주소가 있는 등록된 사무실 제공
  d. 명시신탁(express trust)의 수탁자 대행(또는 타인이 대행을 하도록 주선), 또는
e. 타인을 위해 명의주주 대행(또는 타인이 대행을 하도록 주선)

102) The Forty Recommendations, 용어집, 지정된 비금융전문직
3. 기타 잠재적으로 포함될 개인과 단체

FATF는 독립적이거나 포괄적인 권고사항에서 마지막으로 국가들은 자금세탁 혐의이나 테러자금조달 혐의가 있는 위에 열거된 직업군 외에 사업체와 직업군에 권고 사항 적용을 검토하도록 명시하고 있다. 이것은 각 국이 어느 사업체 또는 직업을 포함할 것인지의 검토하고, 직업에 적합한 대응이 무엇인지 결정할 사항이다. 그 예로는 고가품과 사치품(골동품, 자동차, 보트 등), 전달포, 경매소의 달러와 투자 자문들이 있다. 이들 중 하나 또는 전부를 다루는 요구사항은 있으나, 위험 및 그에 대한 적절한 대응을 검토하는 요구사항은 있다.

E. 감독 및 규제 – 신뢰성(integrity) 관련 기준

금융기관, 특정한 사업체와 특정한 개인의 관이 없이 자금이 세탁되거나 테러에 사용될 수 있다. 범죄자가 금융기관을 통해하거나 금융기관에서 경영진의 경우 자금세탁을 방지하고 적발하는 것이 매우 어렵다. 이와 유사하게 특정 개인들이 자금세탁에 관여한 경우 국가가 그것을 방지하고 적발하는 것이 더욱 어렵게 된다. 신뢰성과 인가 요구사항은 그러한 단체와 개인이 자금세탁과 테러자금조달에 가담하는 것을 막는데 도움이 된다.

1. 금융기관

a. 핵심원칙 작용대상 기관(Core Principles Institutions)

이러한 기관 즉, 은행, 보험사, 증권사는 바젤위원회, IAIS, 국제증권감독위원회 (IOSC)에서 발행한 기준에 명시된 종합적인 감독의 대상이다. 그 조항에는 다음에 관한 요구사항이 포함된다.

▶ 사업 허가 및 인가
▶ 신뢰성, 전문지식 및 경험과 관련하여 이사 및 경영진에 대한 평가(직접적 판단)
▶ 전과나 규제관련 적발사항이 있는 이사와 경영진의 참여 금지
▶ 전과가 있는 이사와 경영진에 의한 소유 또는 통제 금지

103) Id., Rec. 20.
104) 제4장 참조
이러한 요구사항은 신중히 검토되고, AML/CFT 정책에 적응되어야 하고, 감독
에선 이행 여부를 결정을 위해 기록과 정보의 생산을 강제한 권한이 포함된다.105)

b. 기타 금융기관

기타 금융기관은 핵심원칙 적용대상 기관과 동일한 수준으로 엄격한 요구사항
대상이 아니(이는 주로 핵심원칙 적용 대상 기관과 동일한 수준의 건전성
(prudential) 문제가 발생하지 않기 때문이다). 예를 들면 이사와 경영진은 그들의
신뢰성, 전문지식 및 경험과 관련하여 “적합성”에 대해 평가받지 않는다.
AML/CFT를 위해 기타 금융기관에 대한 최소한의 요구사항은 다음과 같다.

- 허가나 인가를 받아야 한다.
- 기타 금융기관의 사업 분야에서 자금세탁과 테러자금조달의 위험에 따라
AML을 위해 감독 대상이 되어야 한다.106)

이것은 “기타 금융기관” 전체와 관련하여 허가 또는 등록 요구사항을 부과하지만
각국이 기타 금융기관의 AML/CFT 조치 이행에 대한 감독 범위에 대해 재량을
허용한다. 어떤 경우에는 감독이 해당 규정을 이행하지 않은 기관에 대한 법집행조
치에 한정되는 반면 이행에 대한 어떠한 예방 조사나 감독이 없는 경우도 있다.

그러나 FATF는 자금세탁 시 환전상에 대해서 허가나 등록 외에도 이행을 모니
터링하고 보정하는 “효과적인 제도”의 존재를 요구한다.107) 실제로 어떤 것이 효과
적인 제도인지에 대해서 권고사항에서 추가로 기술하지는 않으나 비이행 기관에
대한 법집행조치 이상의 것을 요구하고 있다는 것이 합의되어 있다.

2. 지정된 금융전문직

비금융전문직은 카지노와 그 외 비금융전문직이라는 2개의 범위로 나뉜다.
카지노는 다음을 포함하는 엄격한 요구사항이 적용된다.

- 허가(인가)

106) Id.
107) Id.
법정절차가 카지노를 소유, 통제 또는 경영하는 것을 방지하는 조치
AML/CFT 요구사항의 이행 감독

그 외 비금융전문계에 대해서는 위험 민감 방식(risk-sensitive approach)에 따라
이행을 모니터링하고 보장하는 효과적인 제도를 수립하는 것이 요구사항이다. 모
니터링은 정부기관이나 자율규제기관에서 수행할 수 있다. 기타 금융기관과는 달리
(위 참조) 인간나 동물제도가 없다.

F. FATF 권고사항 이행과 부합하는 법률

법률제도의 중요한 측면은 내부적으로 일관되고 각각이 조화롭게 작용되는 법과
구정을 갖추는 것이다. 따라서 방침에 예외를 만들고 근거가 없는 한 하나의
법이 다른 법과 충돌하지 않고, 이 두 법이 모순 없이 협조하는 것으로 해석되는
것이 중요하다.

충돌이 있을 수 있는 한 분야는 비밀보호법이다. 국가들은 종종 금융정보의 비
밀이 공개되는 것으로부터 보호하는 일반법을 보유하고 있다. 이 일반법은 특정
요구사항과 충돌하기도 하는데 예를 들면 금융기관이 의심스러운 거래를 보고하는
것이다.108)

FATF는 각 국가가 AML/CFT 요구사항을 이행하기 위해 금융기관 비밀보호법이
FATF 권고사항 이행을 금지하지 않도록 보장해야 한다고 규정한다.109)

G. 해당기관 간의 협력

각 국가는 정책임자, FIU, 범죄실태기관(당당되는 경우 관세 포함), 금융기관 감
독기관 및 기타 해당기관이 서로 협력할 수 있도록 효과적인 절차가 수립되어 있
도록 규정한 필요가 있다.110) 국내외와 집행시스템에서 적절한 경우 이 요구사항은

109) Id. Rec. 4.
110) Id. Rec. 31.
자금세탁과 테러자금조달 척결을 위한 방침과 활동의 개발과 실행을 조율하는 것까지 확대된다.

원칙적으로 이 권고사항은 한 국가의 법과 절차가 AML/CFT 노력에 참여하는 기관 간에 조율 촉진 외에도 여러 해당기관간의 협력 촉진으로 간주되어야 함을 의미한다. 가장 중요한 것은 한 국가의 법과 절차가 그러한 협력 노력을 금지하거나 재현하는 것으로 간주되지 않아야 한다는 것이다.

H. 수사

각국가는 정정된 범죄행기관이 자금세탁과 테러자금조달 수사를 담당하도록 보장해야 한다.111) FATF는 자금세탁과 테러자금조달 척결에 수사를 최대한 활용하려는 시도로 국가들이 장복수사, 전문화된 자산 수사 그리고 타국과의 협력 수사와 같은 특수한 수사기법과 절차를 허가, 지원 및 개발하도록 권장한다.112)

자금세탁과 테러자금조달 척결에 참여하는 모든 해당기관과 함께 수사와 관련된 노력은 신뢰성 기준을 충족하는 직원을 포함하여 적절한 재정, 인력 및 기술 자원으로 지원되어야 한다.113)

마지막으로 한 국가의 AML/CFT 제도의 효과성은 유용한 정보에 달려있다. 따라서 각 국가는 수사와 AML/CFT 제도의 다른 측면의 효과성과 효율성에 대한 통계를 보유해야 한다.114)

111) Id. Rec. 27.
112) Id.
113) Id. Rec. 30.
114) Id. Rec. 32.
제6장 : 예방조치

A. 고객신원확인과 고객확인제도
B. 기록유지 요구사항
C. STR
D. CTR
E. 보고 및 공개 요구사항과 비밀보호법과의 균형 맞추기
F. 내부통제
G. 규제 및 감독
H. 법인 및 법적계약
제6장 예방조치

<table>
<thead>
<tr>
<th>A. 고객신원확인과 고객확인제도</th>
<th>C. STR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 고객신원확인과 고객확인제도의 범위</td>
<td>1. 의심스러운 거래: 관련 사항</td>
</tr>
<tr>
<td>2. 고객의 범위</td>
<td>2. 보고 관련 “개인정보보호” 조항</td>
</tr>
<tr>
<td>3. 고객 승인과 신원확인 절차</td>
<td>3. 보고 의무의 범위</td>
</tr>
<tr>
<td>4. 자위협 및 고위험 계좌의 관리</td>
<td>4. 조세범죄(Fiscal Crimes)</td>
</tr>
<tr>
<td>5. 고객확인의 확대가 요구되는 상황</td>
<td>5. 보험부문</td>
</tr>
<tr>
<td>6. Vendors와 기타 그룹으로 고객 확인제도 확대</td>
<td>6. 증권부문</td>
</tr>
<tr>
<td>7. 보험부문에 대한 조치</td>
<td>7. 지정된 비금융전문직</td>
</tr>
<tr>
<td>8. 증권부문에 대한 조치</td>
<td></td>
</tr>
<tr>
<td>9. 지정된 비금융전문직에 대한 조치</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. 기록유지 요구사항</th>
<th>D. CTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 금융기관</td>
<td>1. 다수의 고객거래</td>
</tr>
<tr>
<td>2. 보험부문</td>
<td>2. 국가 간 이동</td>
</tr>
<tr>
<td>3. 증권부문</td>
<td>3. 현대의 자금관리기법</td>
</tr>
<tr>
<td>4. 지정된 비금융전문직</td>
<td></td>
</tr>
</tbody>
</table>

| E. 보고 및 공개 요구사항과 비밀 보호법과의 균형 맞추기 |

<table>
<thead>
<tr>
<th>F. 내부통제</th>
</tr>
</thead>
<tbody>
<tr>
<td>G. 규제 및 감독</td>
</tr>
<tr>
<td>H. 법인 및 법적계약</td>
</tr>
</tbody>
</table>

사금세탁자들과 테러자금조달자들은 다양한 유형의 금융기관과 비금융전문직이 그들의 범죄 활동을 돕도록 이용한다. 실제로 금융기관과 특정 비금융전문직의 이용하는 것은 범죄자들이 범죄를 저지르는데 있어 매우 중요한데 그것은 금융기관과 특정 비금융전문직이 국내외적으로 타 금융기관에 자금을 전송, 환전 및 범죄수익을 다른 종류의 금융상품과 기타 자산으로 전환하는 수단을 제공하기 때문이다.

FATF는 40개 연합국에서 115) 한 국가가 사금세탁방지 분야에서 체택해야 하는 다수의 예방책을 규정했다. 이러한 예방책은 모든 금융기관에 적용가능하고, 좀 더

제한적으므로 지정된 비금융전문적에 적응가능하다. 또한 9개 특별권고사항116에 따른 
대리자급조건 척결에도 동등하게 적응가능하다.

전 40개 권고사항과 마찬가지로 주로 권고사항 5-25까지인 예방적 권고사항이 
아니라 AML/CFT 관련 국제기준을 이행하고 있는 것으로 간주되려면 국가가 준 
수해야 할 행동강령이다. 그러나 이 행동강령은 국가의 고유한 경제상황, 법률제도 
및 허위이고 일치하는 요구사항을 체택하도록 허용할 만큼 탄력적이다. 국가들은 또 
한 요구사항에 대한 추가 설명을 보려면 40개 권고사항과 9개 특별권고사항의 이 
행정기법을 참조하면 된다.117)

A. 고객신원확인 및 고객확인제도

국가들은 바젤위원회118와 FATF119에서 규정한 국제기준에 따라 금융기관이 
석절한 고객신원확인과 고객확인제도 절차를 수립하도록 보장해야 한다. 이러한 
절차들은 금융기관의 개인 및 법인 고객에게 동일하게 적용된다. 이러한 규칙이나 
절차는 금융기관이 고객과 고객의 금융활동에 대한 석절한 지식을 보유하도록 보 
장해준다. 고객신원확인 요구사항은 또한 “고객알기(KYC: know your customer)” 
규칙120으로 알려져 있는데 이 용어는 바젤위원회에서 사용하고 있다.121)

고객알기 방침은 금융기관이 자금세탁과 테러자금조달을 직발, 억제 및 방지하 
도록 도와줄 뿐 아니라 금융기관, 준법 고객 및 전반적인 금융시스템에 실질적인 
해택을 준다. 특히 고객알기방침은:

118) 효율적인 운행감독 및 고객확인제도를 위한 바젤핵심원칙( Basel Core Principles for Effective Banking 
본 안내서의 별첨 IV에, 특별권고사항은 별첨 V에 발췌되어 있음.
120) 바젤위원회, 고객알기 방침, Principle 15에서는 “운행 감독기관은 금융부문에서 높은 
효리 및 직업 기준”을 정하고, 그 외에도 아무도 법칙자에 의해 운영이 이용되는 것을 방지하는 역할을 
KYC 규칙을 포함한 적절한 방침, 임무 관행 및 절차를 보유해야 한다”고 명시한다.
121) 바젤의 운행의 고객확인제도에서는 “환전 개개의 감독기관은 운행이 적절한 통제 및 절차를 수립하여 고객 
을 알게 되는 것의 중요성을 점점 더 인식하고 있다. 현재 및 기존의 고객에 대한 적절한 고객확인은 이러한 
1. 고객신원확인과 고객확인제도의 범위

금융기관이 이용하는 고객신원확인과 고객확인 절차는 소재국의 법과 상충되지 않는 경우 국내외의 지점과 자회사에도 반드시 적용되어야 한다.123) 소재국의 범위 이행을 금지하는 경우 본국의 해당기관은 이러한 절차가 소재국의 기관에 의해 적용될 수 없음을 통보받아야 한다. 소재국의 감독기관은 지방자치단체의 범과 규정을 변경하려고 노력해야 한다.124) 본국과 소재국 사이에 두 개의 다른 수준의 규제 기준이 존재하는 경우 소재국에 법적 제약이 부재할 시 두 개의 기준 중에서 더 높고 보다 종합적인 것이 적용되어야 한다.125)

2. 고객의 범위

바젤위원회는 고객을 다음과 같이 정의한다.

- 금융기관에 계좌를 유지하거나 누군가(예: 설소유자)를 대신해 계좌를 유지하는 개인이나 단체
- 전문적인 중개인(예: 대리인, 최계사, 변호사)에 의해 수행되는 거래의 수취인
- 운행에 막대한 위험을 준 수 있는, 금융거래와 관련된 개인이나 단체126)

중요한 고객신원확인의 한 측면은 고객이 자신을 위한 거래를 하는지 아니면 금융 기관에서 보관하는 문서에서 식별되지 않는 실제 계좌주가 있는지 여부를 확인하는 것이다. 고객이 타인이 다른 단체를 대행하고 있다고 의심할만한 사유가 있을 시에는 적절한 고객확인조치가 마련되어야 한다.

122) 바젤의 운영의 고객확인제도(Basel Customer Due Diligence for Banks)(제9조).
123) The Forty Recommendations, Rec. 22.
124) Id.
125) 바젤의 운영의 고객확인제도(Basel Customer Due Diligence for Banks)(제66조).
126) Id. (제21조).
실소유주는 계층적 지배구조를 가진 법인이나 회사의 경우 또한 확인하기가 어렵다. 계층적 지배구조는 하나의 회사가 하나 또는 그 이상의 다른 법인을 소유하거나 지배하는 것이다. 또 다른 법인이 다수의 법인 각각을 소유하고, 궤극적으론 하나의 모회사가 소유하거나 지배하는 경우도 있다. 회사나 법인이 관련된 경우 실제 모회사나 지배하는 회사의 신원을 결정하는데 있어 적절한 고객확인 조치가 이용되어야 한다.

3. 고객 승인과 신원확인 절차

금융기관은 고객과 고객을 대행하는 자에 대한 명확한 고객 승인 및 신원절차를 개발하고 시행해야 한다.127) 이러한 절차에는 고위험고객 프로필의 개발이 포함되어야 한다. 그러한 프로필에는 인적사항, 출신국, 공적이나 유명인사 여부, 연결계좌(linked accounts), 그리고 사업의 유형과 성질과 같은 기준이 되는 위험 지표가 포함될 수 있다.128) 금융기관은 고객 승인 방침을 마련할 시에 범죄 활동과 관련된 위험 회피와 새 고객을 받아들이라는 의지 사이에 적절한 균형을 맞추는데 특별히 주의를 기울여야 한다. 일반적인 규칙으로써 승인기준의 엄격한 적용은 미래 고객의 위험 프로필과 상응해야 한다. 어느 고객의 프로필이 자금세탁활동의 고위험을 부과하는지에 대한 결정은 경영진만이 내리도록 하는 것이 강력히 권고된다.129)

금융기관은 고유의 고객승인방침을 마련하여 사회적으로 취약한 계층이 배제되지 않도록 해야 한다. 이러한 고객승인방침은 어떤 방식으로도 일반 대중이 금융서비스를 이용하는 것을 제한하지 않아야 한다.130) 이것은 특히 수표, 신용카드나 체크카드, 전자 및 기타 지불수단의 이용을 포함하여 보다 폭넓은 금융상품을 향해 가고 있고 현금 기반 경제에서 이동하고 있는 국가들에게 특별히 중요하다.

계좌는 새 고객의 신원이 충분히 검증된 후에만 개설되어야 한다.131) 어떠한 고객에게도 의명이나 가명으로 계좌를 개설하거나 유지하는 것이 허용되지 않아야 한다.132) 이렇게 금지하는 것은 변호계좌가 공식문서를 이용한 고객신원확인 절차

---

127) Id. ( 제20조).
128) Id.
129) Id.
130) Id.
131) Id. ( 제22조). The Forty Recommendations, Rec. 5.
를 요구하지 않는 경우 변호계좌(a numbered account) 변호로만 설립하는 은행계좌가 아니라 코드로 이용되는 경우 여기에도 적용된다. 변호계좌는 동일한 고객 신원확인 절차 및 합법적인 문서가(기록보존과 함께) 이용되는 경우에만 허용된다. 이러한 점에서 금융기관은 고객의 공식적인 신원확인 문서를 검증하고 검증해야 한다. 미래 또는 현재 고객의 신원을 검증하는 최고의 문서는 복제가 가장 높은 것이다. 이러한 관점에서 국가들은 여권, 운전면허증, 신원문서 또는 세금증명서와 같은 해당기관이 발행한 “공식적인” 문서의 이용을 요구해야 한다.

내리인이 수취인을 대변하는 경우에도(예: 신탁, 명의인, 수탁계좌, 회사, 그리고 기타 중개인이 금융기관은 누구를 대신하여 계좌가 개설되는지 또는 누구를 위해 거래가 되는지에 관해 개인이나 단체의 신원과 상황을 검증하는 합당한 조치를 취할 필요가 있다. 금융기관은 다음과 같은 정보를 미래 고객으로부터 수집하여 이와 같은 단체의 적법성을 검증할 필요가 있다.

- 고객의 단체의 성명과 법적 유형
- 주소
- 이사의 이름
- 단체를 구속하는 권한을 규제하는 조항
- 조직을 대행하는 내리인
- 계좌번호(해당되는 경우)

송금과 같은 자금이체의 경우 금융기관은 정확하고 유의미한 송금자 정보(이름, 주소 및 계좌번호)를 포함하고, 자금 이체 지역 체인(chain)을 이 정보와 함께 전달해야 한다.

고객의 신원은 그가 지정된 기준금액을 초과한 일회성 고객이거나 고객의 실제 신원이 의심되는 경우에 고객 확인절차를 통해서 확인되어야 한다. 이것은 일회성 범인 고객에게도 적용된다.

133) id.
134) 바축의 은행의 고객확인제도(제23조).
135) The Forty Recommendations, Rec. 5.
136) id., Rec. 5.
137) Special Recommendations, Spec. Rec. VII.
138) 바축의 은행의 고객확인제도 제53조; 그리고 FATF, The Forty Recommendations, Rec. 11.
학교신원확인은 일반규칙으로 금융기관이 모든 관련 고객 정보를 최신으로 기록으로 유지하도록 요구하는 지속적인 과정이다. 기록은 규모가 큰 거래, 고객 문서 기준의 변경, 계좌의 자료 변경, 현재 기록이 불충분하다는 인지가 있는 경우에 업데이트 되어야 한다.139) 한 국가의 금융기관 감독기구는 금융기관 이 용의 고객승인 및 신원확인 절차를 개발하는데 있어 지원하도록 강력히 권고된다.

4. 저위험 및 고위험 계좌와 거래

위에서 기술된 고객확인제도 조치는 고객과 거래의 유형에 따른 위험에 따라 적용되어야 한다. 이 일반 원칙은 FATF 권고사항과 고객확인제도에 관한 바젤위원회 논문의 핵심이다. 위험이 더 높은 고객군에 대해서는 강화된 조치가 취해져야 하고, 그 사례의 일부는 아래에서 기술한다. 위험이 더 낮은 고객군에 대해서 국가는 금융기관이 축소되거나 간소화된 조치를 적용하도록 허용할 수도 있다. FATF와 바젤위치는 그러한 고객과 거래의 유형을 식별했으나 이것이 전부는 아니며 국가의 재량에 달려있다. 이렇게 더 낮은 위험을 가진 고객으로는 금융기관, 공기업과 국영기업이 있다. 이와 같은 거래에는 공동관리계좌(pooled accounts), 연금제도 그리고 소액 보험이 있다.140)

고객들은 언제나 식별되어야 하고, 기본적인 절차의 일부가 신원 검증에 적용되어야 한다는 거래가 있다. 축소되거나 간소화된 조치는 사업관계와 거래의 목적과 성질에 대해 수집된 정보의 양과 그 절차를 검증하는 범위까지 적용될 수 있다.142)

이런 위험이 요인인가에 대한 특정 문제는 새 고객의 신원 검증이 요구사항이 되기 전에 이미 계좌를 보유한 고객의 신원확인과 관계가 있다. 바젤위원회나 FATF는 종합적인 프로그램이 기존 고객의 신원 검증이나 기타 고객확인조치 수행을 위해 마련되는 것을 요구하지 않는다.143) 그러나 금융기관이 중요성과 위험에 따라 기존 고객의 신원 검증과 기존 고객에 대한 추가 고객확인을 수행하도록 요구된다.

139) 바젤의 은행의 고객확인제도(제24조).
140) *The Forty Recommendations*, 권고사항 5의 학설서, paragraph 9의 참조.
141) *The Forty Recommendations*, 권고사항 5의 학설서, paragraph 10의 참조.
142) *The Forty Recommendations*, 권고사항 5의 학설서, paragraph 9의 참조.
143) *The Forty Recommendations*, 권고사항 5의 학설서, paragraph 8의 참조.
5. 고객확인의 확대가 요구되는 상황

특정한 경우 40개 권고사항에서는 금융기관에 의한 일반적인 과정에서 수행된 고객확인 외에도 강화된 고객확인조치가 수행되어야 한다고 규정한다. 아래는 추가적인 고객확인절차가 요구되는 사례를 논의한 것이다.

a 봉사적 주요인물

FATF는 봉사적 주요인물을 다음과 같이 정의한다.

외국에서 주요 공직에 있거나 있었던 적이 있는 개인으로 예를 들면, 국가의 수장 또는 정부의 수장, 고위직 정치인, 고위직 국가공무원, 사업부 고위직 또는 군 고위직, 국영기업의 간부, 주요 정당 간부. 정치적 주요인물의 가족이나 가까운 지인들과의 사업관계는 정치적 주요인들이 갖는 평판에 대한 위험과 유사한 위험을 내포한다. 이 정의는 앞의 범위에 중간급 또는 더 낮은 하위급 관료들을 포함하지 않는다.144)

이 정의는 단지 “외국”의 공직에 있는 고객들만을 포함한다. 따라서 “국내” 정치적 주요인물에 적용되지 않는다. FATF는 국가들에게 국내 정치적 주요인물에게 추가 고객확인절차를 확대하도록 권고하는 수준이지만 외국 정치적 주요인물에게는 추가 고객확인절차를 적용할 것을 요구한다.145)

추가적인 고객확인조치는 다음과으로 구성된다.

- 정치적 주요인물 식별
- 계좌 개설 시에 경영진 급의 승인
- 재산과 자금의 원천 확인
- 강화된 지속적인 모니터링

용어의 정의를 감안할 때 금융기관에게 있어 고객이 정치적 주요인물인지를 실제로 알아내는 것은 종종 가장 어려운 도전이 되기도 한다. 공식적인 조치 중에

144) The Forty Recommendations. 용어집. 정치적 주요인물(Politically Exposed Persons)
정치적 주요 인물의 명단을 발행하는 조직이 없지만 여러 상업 단체들은 그와 같은 명단을 보유하고 정기적으로 업데이트 한다.

b. 국경 간 환거래 관계

국경 간 환거래 관계는 금융기관에게 잠재적으로 고위험 계좌의 또 다른 원천이 된다. 환거래는 느슨한 제도를 가진 국가에서 적절한 고객확인절차를 거치지 않고 국제금융시스템에 접근할 수 있는 한 방법이 될 수 있다. 은행은 외국기관과 환거래 관계를 시작하기 전에 다음을 해야 한다.

- 수취은행의 업무 성질, 평판과 감독기관의 자질에 대해 확인
- 수취은행의 AML/CFT 규율 평가
- 환거래에 대해 경영진의 속임 취득
- 각각의 업무를 문서화
- “당좌예금계좌(payable-through-accounts)”가 사업관계의 일부로 이용되는 경우 수취은행이 고객의 신원을 검증하고, 지속적인 고객확인을 수행하도록 보장146)

FATF에서 “비협조국가”로 분류한 국가에 소재한 기관과의 환거래는 피해야 한다147) “위장은행(shell banks) (실질적인 형제가 없고 제도적 금융구조가 기업되지 않은 국가에서 범인적으로 만들어진 은행)”과는 거래하지 않아야 한다148)

c. 비대면 고객

기술의 발전으로 반드시 금융기관을 방문하지 않고, 고객들이 금융서비스를 받는 데 전화와 인터넷을 이용함에 따라 “비대면” 고객과의 사업관계가 증가하고 있다. 국제기준제정기구가 경제에 도움을 주고 고객에게 더 많은 선택권과 서비스를 제공하는 기술 개발을 방해하려는 의도는 없다. 금융기관과 기타 유사 서비스를 제공하는 기관은 AML/CFT 위험이 비대면 고객과 관련하여 다소 다르며, 이들을 처리하는 적절한 조치를 취할 필요가 있음을 인식해야 한다149)

146) The Fort Recommendation, Rec. 7.
147) FATF의 “비협조국가” 리스트는 http://www.fatf-gafi.org/NCTT_en.htm. 참조
149) Id., Rec.8.
FATF가 비례한 고객의 계좌 증가되는 위험에 대한 문제를 제기하지만 그 증가된 위험에 대응하기 위해 어떤 조치가 취하지 않는데 대한 지침을 제공하지는 않는다. 따라서 적절한 방침과 절차를 수립하는 것은 각 국가에 달려있다.

d. 중개인

일부 국가의 금융기관은 중개인이나 제3자가 "소개한" 고객을 보유하고 있고, 이러한 고객에 대해서는 고객확인절차를 수행하지 않았을 것이다. 이러한 상황에서 금융기관은 3가지로 해야 한다. 첫째, 중개인이 고객확인 요구사항을 이행해야 하는 주체가 되고, 그 고객확인 요구사항 이행여부는 감독 대상이 되어야 한다. 둘째, 중개인이 고객의 신원과 기타 고객확인문서에 대한 충분한 정보를 수집하도록 해야 한다. 셋째, 중개인이 요청이 있을 시에 지체 없이 그 정보를 제출할 수 있도록 해야 한다.

중개인은 국내 또는 국제기관일 수 있다. 중개인이 국제기관인 경우 금융기관은 위의 요구사항이 충족되도록 특히 주의한 필요가 있다. 중개인이 허용되는 일부 국가에서는 중개인이 AML 규율 대상인 개인이나 기관이 AML 규율의 이행에 책임을 맡고 있는 규제기관에 의해 감독되고, FATF 기준을 이행하는 국가에 소재하도록 요구한다.

e. 기타 고위험 업체

FATF는 또한 특별한 주의를 요구하는 2가지 다른 범주의 거래에 주목한다. 첫째, 복잡하고 특이한 고객 거래와 명백한 경제적 목적이나 가시적인 법적 목적에 없는 특이한 패턴의 거래가 있다. 이러한 거래의 배경과 목적은 가능한 많이 조사되고, 조사결과는 기록되어야 한다. 금융기관이 배경과 목적을 찾을 수 없는 경우 그리고/또는 그 업체가 의심스럽다면 그 업체와의 거래를 거부 그리고/또는 형의 거래 보고를 고려해야 한다.

둘째, FATF 권고사항의 비이행 국가로 식별되어 특별한 주의가 요구되는 국가가 있다. 이러한 국가와의 거래가 금지되어 있지는 않으나 금융기관은 그 국가에 특별한 주의를 기울여야 하고, 국가의 목적에 의심되는 경우 추가로 조사하여 그
결과를 기록해야 한다. 금융기관이 그 거래가 성실거래임을 납득할 수 없을 경우 그 국가와의 거래를 거부 허용하려고 또는 협의거래보고를 고려해야 한다.

6. 벤더와 기타 그룹으로 고객확인제도 확대

많은 기업의 금융영구 구조는 점점 더 복잡해지고, 국제무역의 발전과 연관성이 증가하고 있다. 결과적으로 많은 금융기관은 금융기관의 직원과 수취은행 외에도 벤더, 금융업자, 업체 대행사에 고객확인을 더 많이 수행하는 것이 필요하다고 느꼈다. 각 국가의 금융기관 감독기관은 확인의 관계가 더 높은 위험으로 간주될 때 특히 고객확인의 경향을 통합하는 방침의 이행을 고려할 수 있다.

7. 보험부문에 대한 조치

IAIS는 고객신원확인과 고객확인에 대한 자체의 지침을 보유하고 있다. 보험 업계는 위에서 논의된 40개 권고사항의 관련 연구사항에 추가해 이 지침을 준수해야 한다. IAIS 지침에서는 보험회사가 다음을 하도록 권고한다.

- 보험 적용과 관련한 모든 당사자가 실제로 존재하는지에 대해 “합리적으로 만족할 만큼” 확인. 다시의 대상자에 대해서는 (예: 집단 생명보험과 언급) 주요 주주 또는 이사와 같은 한정된 집단에 대해 고객확인을 하는 것으로 충분하다.
- 모든 피보험자와 그들과 보험계약자와의 관계 격증 - 피보험자와 보험계약자가 아닌 자들은 관계의 성격에 대해 질문을 받아야 한다.
- 가명 및 차명계와 금지
- 보험청구액, 수수료 및 보험계약자가 아닌 자(예: 협사회사, 회사)에게 주어지는 기타 금융적 격증
- 보험계약자의 재정 흐름이나 거래 패턴이 크고, 예상치 못하거나 설명이 불가한 방식으로 변경되는 경우 고객확인 증가
- 이전 가능한 양로보험(second-hand endowed policies)의 판매와 구입 그리고 일산전속(单一-linked) 보험의 이용과 관련하여 고객확인 증가
- 위험 수준에 따라 정당한 비율로 선의의 재보험 단체에 지불을 보장하는 방법으로 지속적으로 재보험 또는 재재보험 모니터링과 있다.

152) Id., Rec. 21.
8. 증권부문에 대한 조치

IOSCO는 증권회사, 브로커 또는 집합투자회사에 대한 독립된 고객신원확인이나 고객확인 요구사항을 수립하지 않았다. IOSCO가 구체적인 요구사항을 수립하지는 않았으나 40개 권고사항의 고객신원확인 요구사항(방법론에서 보다 충분히 기술됨154)은 증권부문에도 적용된다.

9. 지정된 비금융전문직에 대한 조치

기록보존과 관련한 요구사항 외에도 고객확인에 대한 요구사항은 금융기관보다는 보다 완전한 방식으로 지정된 비금융전문직에 적용된다. 다음의 논의는 고객확인절차가 비금융전문직에 적용되는 경우에 관한 것이다.

a. 카지노

금융기관에 대한 고객확인은 카지노 고객이 3천 달러/유로나 이를 초과하는 금융거래를 할 때 적용된다. 이와 같은 거래의 예에는 카지노 첩 구매 또는 카지노 칩의 현금화, 게임개설, 전신송금 및 환전이 포함된다. 이것은 모든 도박 거래가 5 년 동안 모니터링 되거나 기록되어야 함을 뜻하는 않는다.155)

b. 부동산 중개인

부동산의 매도 및 매수와 관련된 고객의 거래는 고객확인절차를 요구한다. 그로나 신원확인과 기타 고객확인은 거래가 발생하고 그것이 부동산 중개인의 고객인사와 관련한 경우에 실행될 필요가 있다.156) 많은 국가에서 고객은 구매자라기보다는 판매자일 것이다.

c. 귀금속 달러

1만5천 달러/유로나 그 이상의 현금거래는 고객확인 요구사항에서 다루어져야 한다.157)

154) http://www.fatf-gafi.org/pdf/Meth-2004_en.PDF.
155) The Forty Recommendations, Rec. 12, paragraph a. 해당 권고사항은 Recs. 5, 6, 그리고 8-11임.
156) Id., Rec. 12, paragraph b.
d. 변호사, 공증인, 기타 독립적인 법조인 및 화재사

고객신원확인과 고객확인 요구사항은 다음의 활동과 관련하여 고객을 위해 준비되거나 수행되는 거래에 적용된다.

- 부동산의 구매 및 판매
- 고객의 자금, 증권 또는 기타 자산의 관리
- 은행, 저축계좌 또는 증권계좌의 관리
- 회사의 설립, 운영 또는 관리에 대한 기부금 조성
- 변인이나 법률계약의 설립, 운영 또는 관리, 회사 매입 및 매각

핵심 구문은 “거래를 준비하거나 수행하는” 이다. 이것은 거래 방법에 대한 단순 조건 제공이 포함되지 않는다는 뜻이다. 고객신원확인과 고객확인(및 기록보존)은 전문적이 거래의 수행에 관련되고 난 후에 요구된다. 여기서 거래의 수행에는 거래의 실행뿐 아니라 거래를 준비하는 예비 작업도 포함된다. 이것은 고객이 임체적인 자금세탁 또는 테러자금조달 거래에 관여할 수 있도록 허용하는 서비스를 제공함으로써 변호사와 화재사가 금융제도라는 관문의 “문지기(gatekeeper)” 역할을 하는 상황으로 볼 수 있다.

e. 신각 및 법인설립전문회사

고객확인절차는 다음의 활동과 관련하여 고객을 준비되거나 수행되는 거래에 적용가능하다.

- 법인설립실태 대행
- 회사의 이사 또는 총무부정(secretary), 협회회의의 파트너, 또는 기타 법인과 관련하여 유사한 직위 대행(또는 타인이 대행을 하도록 주선)
- 회사, 협회회의 또는 기타 법인이나 법률계약을 위해 사업장 주소나 숙박 시설, 사신 또는 유관주소가 있는 등록된 사무실 제공
- 명시신각(express trust)의 수탁자 대행(또는 타인이 대행을 하도록 주선), 또는
- 타인을 위해 명의주주 대행(또는 타인이 대행을 하도록 주선)

157) Id. Rec. 12, paragraph c.
158) Id. Rec. 12, paragraph d.
159) Id., Rec. 12, paragraph e.
일부 국가에서는 위의 거래를 변호사가 수행한다. 위에 명시된 변호사에 대한
기준과 일관되기 위한 관련 사항은 역시 “준비와 수행”인데 여기에는 단순 조언
제공이 제외되나 특정 거래의 수행을 위한 예비 작업이 포함된다.

B. 기록보존 요구사항

1. 금융기관

금융기관은 고객신원과 거래기록을 계좌 해지 후 최소한 5년간 보존해야 한
다.160) 또한 규제기관에서 요구하는 경우 5년 이상 기록을 보존하도록 요구될 수도
있다. 기록의 내용은 요구 시에 해당기관으로 제출되어야 하고, 범죄행위 기소가
될 경우 충분히 상세해야 한다.161)

기록 보존은 자금세탁과 테러자금조달의 방지와 적발에 중요하다. 잠재적인 고
객이 기록이 보존된다는 사실을 알고 있다면 그가 불법적인 목적으로 금융기관 이
용을 시도할 가능성이 낮다. 기록 보존은 또한 관련자의 적발과 해당기관이 관련
자를 추적하는 것을 도와줄 금융자료를 제공해준다.

다음의 정보는 고객의 거래를 기록할 시에 포함되어야 한다.

- 고객 그리고/또는 수취인의 성명
- 주소
- 거래 일자 및 성질
- 거래 동화의 종류와 금액
- 계좌 유형과 계좌 개수 식별
- 금융기관에서 일반적으로 기록하는 기타 관련 정보162)

161) Id.
162) Id.
2. 보험부문

IAIS는 고유의 기록보존 요구사항이 있다. 보험사들은 40개 금고사항의 관련 지침에 이점을 반드시 준수해야 한다. 또한 고객의 거래를 기록할 시에 다음의 정보를 반드시 취득해야 한다.

- 거래가 완결된 소재지
- 고객의 주민지
- 고객의 요구 분석
- 지급 방법 관련 세부사항
- 보험회사에서 지급하는 수당에 관한 설명(benefits description)
- 고객 신원 검증에 이용되는 문서 사본
- 만기동안 계약과 관련된 사후관련 기록
- 만기 처리와 청구 결산의 세부사항(“결제문서(discharge documentation)” 포함)\(^{163}\)

금융기관 감독기구는 보험사의 모든 대리인(representatives)이 해당 보험법에 따라 관할기구에서 허가를 받도록 점검해야 한다.\(^{164}\) 대리인(Representatives)은 회사를 위해 문서를 보존할 수 있으나 기록의 신뢰성은 상품제공자인 보험사에 달려 있다.\(^{165}\) 이러한 경우 보험사와 대리인(representative) 간의 명확한 책임 구분이 요구된다.\(^{166}\)

3. 중권부문

IOSCO는 자체의 기록보존 요구사항을 수립했고, 중권사는 위에서 논의된 40개 금고사항의 일반 요구사항 외에도 이것을 준수해야 한다. IOSCO는 금융법에 관련 중앙기관이나 기타 해당기관이 중개인이 자신의 규제 이행을 증명하는데 필요한 경우 기록을 보존하도록 보장하는 것을 요구한다.\(^{167}\) 이러한 기록은 관독이 가능하고, 이해가 되며 종합적이어야 하고, 집합투자자산과 거래가 포함된 모든 거래가 포함되어야 한다.\(^{168}\)

\(^{163}\) IAIS 자금세탁방지지침서(Anti-Money Laundering Guidance Notes) 참조
\(^{164}\) ibid.
\(^{165}\) ibid.
\(^{166}\) ibid.
4. 지정된 비금융전문직

지정된 비금융전문직에 대한 기록보존 요구사항은 고객신원확인과 고객확인 요구사항에 적용되는 것과 같은 상황에서 적용된다.169) 위의 섹션 A.9 고객확인 및 신원확인, 지정된 비금융전문직에 대한 조치를 참조하시오.

C. 혐의거래보고(STR)

금융기관이 자금이 범죄 활동의 수익이거나 태러자금조달과 관련된 것으로 의심하거나 의심할만한 합당한 사유가 있는 경우 FIU에 혐의를 보고해야 한다.170) 더구나 은행은 감독기관에 의심스러운 거래와 중대한 사기 사건을 보고하도록 요구되어야 하고, 감독기관은 해당기관이 주의를 기울이도록 할 필요가 있다.171) 금융기관은 STR을 제출할 때 어떠한 경우에도 고객의 행동이 해당기관에 혐의 보고된다는 것을 통보하지 않아야 한다.172) 통보를 한 시점에서는 기록 생산을 포함한 정부당국의 지침을 완전히 이행해야 한다.173)

1. 의심스러운 거래: 관련 사항

의심스러운 거래는 가장 명백하게는 정상적인 계좌 거래 활동과는 동떨어진 거래를 포함하여 여러 가지의 특징이 있다. 명백한 결제, 상업적 또는 법적 목적의 없는 거래의 특이한 패턴 외에도 복잡하거나 특이한 고객거래는 혐의가 있고, 따라서 금융기관과 필요한 경우 해당기관에 의한 추가 조사가 이루어진다.174) 금융기관은 의심스러운 거래를 스캔링할 때 도움이 되도록 특정 범주의 계좌를 모니터링 하는 위험에 민감한 제한거준(risk-sensitive limits)을 수립해야 한다. 의심스러운 활동(예: 잔고와는 맞지 않는 고수익률)의 구체적인 예는 개별 금융기관에 유용하고, 감독기관이 어떠한 형태로든 금융기관에 제공해야 한다.175)

168) Id.
171) 바젤협의원칙 Principle 15, Description 31.
173) Id., Recs.10 그리고 28.
174) Id., Recs.11.
175) Id., Recs. 25; 바젤 은행고객확인제도 (제53조) 참조.
금융기관과 직원들은 항상 의심스러운 거래를 경계해야 한다. 다음의 경우들이 의심스러운 거래를 나타내기는 하나 총망라된 것은 아니다.

### 일반적인 징후
- 계좌로 입금된 직후 인출
- 합당한 사유 없이 갑작지 휴면계좌가 활성화된 경우
- 고객의 자산이 고객이나 그의 사업과 관련된 정보와 불일치하는 경우
- 고객이 허위 또는 조작된 정보를 제공하거나 요구되는 정보에 대해 은행과 의사소통하는 것을 거부하는 경우
- 거래가 불법적인 목적을 암시하거나 경제적으로 비논리적이거나 식별되지 않는 경우

### 고객현금거래와 관련된 징후
- 고객이나 그의 사업과 관련된 정보와 불일치하는 빈번한 현금 입금
- 동일한 국가나 외국에 소재한 타 은행에 개설된 계좌로 현금 입금 직후 수표 발행이나 자금이체
- 고객의 사업과 명백한 관련 없이 빈번한 현금 인출
- 고객지폐를 소액으로 빈번하게 바꾸거나 또는 다른 통화로 빈번하게 환전
- 여행자 수표를 포함하여 고객의 수표를 현금화
- 금융기관에서 신원확인이나 보고가 요구되는 기준 바로 아래의 금액으로 빈번하게 현금 거래

### 예금계좌 거래와 관련된 징후
- 계좌 해지 후 동일한 이름으로 또는 고객의 가족 명의로 새 계좌들을 개설
- 국외에서 송금된 자금으로 또는 현금입금 직후에 주식 구매
- 비논리적인 거래 구조(너무 많은 수의 계좌, 그 계좌들 간의 빈번한 송금, 등)
- 명백한 사유 없이 담보 승인(저당, 채권)
- 수취인을 표시하지 않고 타 은행으로 송금
- 타당한 설명 없이 비물 대출의 예상치 못한 상환
- 고객이나 그의 사업과 관련된 정보와 불일치하는 고객의 수표 입금
2. 보고 관련 “개인정보보호(Safe Harbor)” 조항

“개인정보보호(Safe Harbor)” 법은 금융기관이 모든 의심스러운 거래를 보고하도록 권고하는 것에 도움이 된다. 이 법은 선의로 해당기관에 혐의거래를 보고할 시에 금융기관과 그 직원들을 민행사상의 책임으로부터 보호한다. 이러한 법률 조항은 그 혐의거래가 선의로 보고된 경우(즉, 불성실하거나 악의가 없음) 금융기관과 직원 또는 대리인(representatives)을 기밀보호장이나 비밀보호법의 위반 혐의로 인한 소송에서 보호해야 한다.176)

3. 보고 의무의 범위

STR은 특정 거래가 자금세탁이나 테러자금조달과 관련되어 수사가 이루어져야 한다는 점을 해당기관에 경고하는 하나의 방식이다. 대부분의 경우 보고기관은 그 거래가 범죄수익을 대변한다는 증거가 없고, 어떤 범죄가 연루되었는지 알 가능성 이 희박하다. 금융기관은 단지 그 거래가 특이하고 정상적인 거래 유형과 일치하지 않는다는 점을 인지하는 것이다. 대부분의 경우 금융기관은 자금의 출처나 거래의 목적을 알지 못하고, 비밀정보누출의 위험 없이 고객을 조사할 수 없다. 이러한 상황에서 금융기관은 혐의거래보고서를 제출하고, 추가 조사는 해당기관에게 맡겨야 한다.

보고기관이 대부분은 거래의 기본 상황에 대해 모르기 때문에 혐의거래보고제도는 자금이 범죄와 관련되었을 것이라는 “의심”에 대해 보고하는 요구사항을 그 근거로 해야 한다. 보고기관이 거래를 조사하거나 자금이 범죄 활동과 관련되어 있다는 실질적인 증거를 보유하는 것이 요구되지 않는다.

4. 조세범죄(Fiscal Crimes)

일부 국가에서는 탈세와 같은 조세범죄를 자금세탁의 전제범죄로 분류하지 않는다. 따라서 탈세에서 유래한 수익의 세탁이 반드시 자금세탁범죄가 되지 않는다. 그러나 금융기관은 여전히 의심스러운 거래를 보고하고, 자금세탁 관련 여부는 해당기관이 결정하도록 해야 한다. 그렇지 않다면 고객이 자금세탁 전제범죄와 관련

5. 보험부문

IAIS는 자체의 협의정조보고 지침을 수립했다. 보험업체는 위에 명시된 40개 권고사항의 요구사항 외에도 이것을 준수해야 한다. 보험사들은 FIU나 기타 중앙 기관에 의심스러운 활동을 보고해야 한다. 다음은 추가 조사가 이루어져야 할 부분별 협의정조 사례이다.

- 보험의 특이하거나 불리한 조기 상환
- 일정적인 거래나 금융활동(징수금액 지급 또는 특이한 증권액에게 거액의 커버신 지급)에서 증권사 활용
- 특이한 지급방식
- 사금세탁이나 테러자금조달과 관련하여 느슨한 규제제도를 가진 국가가 관련된 거래

6. 증권부문

IOSCO는 증권회사, 브로커, 또는 집합투자업체에 대한 독립된 협의활동 보고 요구조건을 수립하지 않았다. IOSCO가 이 분야에서 독립적이거나 추가 요구조건을 수립하지 않았다 하더라도 40개 권고사항의 협의정조보고 요구사항은 증권부문에 적용된다.

7. 지정된 비금융전문직

40개 권고사항의 2003년 개정판에 따라 지정된 비금융전문직은 이제 협의정조 보고를 하도록 요구되지만 고객 신원확인과 고객확인의 의무 보다는 한정적이다.

177) IAIS 자금세탁방지지침서 참조
178) Id.
179) The Forty Recommendations, Rec. 16.
변호사, 공증인, 기타 독립적인 법조인 및 회계사는 그들이 고객을 위해 또는 고객을 대신하여 금융거래를 할 때에만 STR을 제출하도록 요구된다. 이것은 다음의 두 가지 측면에서 고객신원확인과 고객확인 의무보다는 좁은 것이다.

- 보고의무는 모든 거래가 아닌 단지 “금융거래”만을 포함한다.
- 비금융전문직이 고객을 위해 금융거래를 할 때에만 보고의무가 있다.\(^{180}\)

법적으로 면책이 되는 상황에서는 보고 의무가 없다. 개별 국가들은 언제 보고 의무가 생기는지 결정하지만 면책에는 주로 고객의 업정 지위를 규정하거나 소송에서 고객을 대변할 시에 취득된 정보가 포함된다. 국가들은 비금융전문직은 자율 규제기구가 FIU와 협력하는 경우 FIU보다는 각자의 자율규제기구(Self-regulatory organization: SRO)에 보고하도록 규정할 수 있다.\(^{181}\)

귀금속 덩어리들은 15,000 달러/유로 기준금액이거나 이를 초과한 고객과의 현금 거래 시에만 STR을 제출하도록 요구된다.\(^{182}\)

신탁 및 법인설립전문회사는 고객을 대신한 거래일 경우에만 STR을 제출하도록 요구된다.\(^{183}\) 따라서 금융거래뿐 아니라 의심스러운 모든 거래가 보고되어야 한다. 그러나 보고는 신탁 및 법인설립전문회사가 실제로 그 거래를 수행하는 경우로 제한된다. 단순히 조언 제공이나 거래 준비는 보고 대상이 아니다.

D. 고객현금거래보고(CTR)

국가들은 기준 금액을 초과하는 모든 현금거래를 보고하도록 요구하는 것이 혜택을 검토해야 한다.\(^{184}\) 그러나 국가가 이러한 요구사항을 갖추는 것이 강제적이지 않다. 고객현금거래보고는 막대한 자원이 들고, 보안과 관련성이 있어 국가들이 이 문제를 고려할 때 심사숙고해야 할 필요가 있다. 각 국가는 고유한 상황에 따라 자체의 보고 기준금액을 정한다. 예를 들면 미국은 금융기관이 지정된 기관에

---

180) *Id*, Rec. 16, paragraph a.
181) *Id*, 권고사항 16의 허셜서
182) *Id*, Rec. 16, paragraph b.
183) *Id*, Rec. 16, paragraph c.
1만 달러를 초과한 동화 또는 무기명증권이 포함된 모든 거래를 기록하고 보고하도록 요구한다.185)

다른 국가들도 유사한 수준에서 보고를 요구한다. 이러한 기준금액은 해당 국가의 감독기관의 권한 하에 법령이나 규정에 따라 정해진다. 국가의 상황에 따라 요구사항은 카지노, 골동품, 내지 자동차 달리, 변호사, 회계사와 같은 비금융전문직 또는 고객 현금이 치달리는 상황에서 적용된다.

해당기관은 한 국가의 기준금액 지정에 매우 주의를 기울여야 한다. 기준금액은 위험의 낮은 거래를 건너뛸 만큼 높지만 적절적으로 금융범죄와 관련될 수 있는 거래를 식별하기에 충분히 낮아야한다. 또한 보고가 제도에 부담이 되고, 보고 이행의 목적을 위해서도 특히 생산적이지 않은 경우 거래의 보고의무 면제를 추가할 수도 있다.

이기에 덧붙여 특정 단체들은 자금세탁과 관련하여 낮은 위험을 보임 수 있고, 면제 대상이 될 수 있다. 이러한 단체에는 부패가 없는 것으로 간주되는 정부, 특정 금융기관 또는 금융회사 그리고 사업 성격상 빈번한 고객현금거래를 하는 고객이 포함된다. 이러한 면제 대상은 그 행사가 일반규칙과 특정 단체에 대해서 적절한지 여부를 판단하기 위해 정기적으로 검토되어야 한다.

1. 다수의 고액현금거래(Multiple Cash Transactions)

현금거래보고 의무사항도 “돈세탁(smurfing)”으로 불리는 같은 날 이루어진 다수의 거래에 적용된다. 통합 거래금액이 지정된 보고기준금액을 초과하면 금융기관은 관련된 전체 거래를 보고할 필요가 있다.186) 이 보안조치는 여러 개소가 연루된 다수의 개별 거래나 국가의 보고기준금액 이하로 발생하는 경우에 자금세탁과 테러자금조달 노력에 중요한 부분이다. 범죄자와 테러리스트는 소프트웨어 프로그램(software programs)에 의한 적법을 피하려는 자신들의 대응책에 의존한다. 이 것이 관련당국이 범죄자와 테러리스트의 금융활동 적법에 예방 분석을 이용하는 것이 절대적으로 중요한 이유이다.

185) U.S. 은행문인법(1970) 참조
186) 바철 은행고객확인제도 (제16조).
물론 보고기준금액을 넘거나 다중 거래 시험(test)을 충족하지 못하는 거래 역시 협의거래로 보고될 수 있다. 예를 들면 국가가 1만 달러 보고기준금액을 지정하고 있는 경우 9,900 달러의 단일 거래는 보고 요구사항을 피하기 위해 고객이 분산거래를 하기 때문에 의심스러운 것으로 간주될 수 있다.

2. 국경 간 이동

자금세탁자들은 자금세탁의 한 방법으로 현금, 무기명 유가증권 그리고 고가품의 국경 간 이전에 관여한다. 국가들이 이와 같은 국경 간 이전이 자금세탁이나 테러 자금조달에 이용되는 경우를 적발하기 위해 메커니즘을 수립하는 것이 중요하다.

당국은 통화, 기타 무기명 증권 및 고가품(귀금속)의 국경 간 이동에 대해 최소한의 보고 기준을 수립하는 것을 고려해야 한다. 이러한 것들의 특이하거나 의심스러운 국경 이동, 출처와 목적지가 그 나라의 관세 정이나 기타 해당기간에 보고 되어야 한다.187)

3. 현대의 자금관리기법

금융기관과 정부 공무원의 모니터링 역량은 현금과 현금 송금 방식에서 수표, 지불카드, 직접입금, 유가증권의 장부기입과 같은 방식으로의 전환에 도움을 주었고, 이러한 거래들은 의심스러운 점이 있을 시에 시류로 유용한 혼란을 남기고, 해당기관이 조사를 할 수 있게 한다. 수수의 성공여부는 정확하고 완결된 기록 보존에 달려 있다. 이러한 이유로 현대의 자금관리 및 지불 이체 방식이 난리 권장되는 것이다.188)

E. 보고 및 공개 요구사항과 비밀보호법과의 균형 맞추기

정보, 예를 들면 협의거래와 고액거래의 보고 또는 금융기관의 해당기관에게 기록 공개하는 것은 불가피하게 국가의 은행보안법이나 비밀보호법에서 기밀로 취급되는 정보가 포함된다.

188) Id., Recs. 20 그리고 28.
AML/CFT 목적으로 그러한 정보의 보고나 공개를 요구할 시에는 국가는 비밀보호법에서 예외를 두거나 아니면 한정된 목적으로 보고와 공개를 허가할 필요가 있다. FATF는 금융기관의 비밀보호법이 그것의 권고사항 이행을 금지하지 않도록 수립되어야 한다고 규정한다. 189) 동시에 국가는 자금세탁 기관과 같은 공공정책의 필요성이 금융정보의 비밀을 보호할 필요보다 중요한 경우를 제외하고는 기밀이 지켜질 수 있도록 보장하는 보호조치를 수립할 필요가 있다. 국가는 전반적인 제도에서 기밀보장과 비밀보호를 보장하여 보고와 공개가 억제되는 것으로부터 보호한다. 그렇게 함으로써 국가는 보고기관과 요구사항 대상인 자들의 최대한의 협력과 적절한 보고 및 공개를 독려한다.

F. 내부통제

국가는 AML/CFT 법에서 다루어지는 모든 금융기관이 자금세탁과 테러자금조달에 이용되는 것을 방지하는 내부방침과 절차를 수립하고 유지하도록 요구한다. 190) 내부방침과 절차는 다른 기관과 다른 종류의 기관 사이에 다양한 것이나 그 기관의 업무의 규모, 범위 및 성질 모두가 고려되어야 한다.

내부절차에는 직원이 AML/CFT와 관련한 사항을 통보받아 업데이트하는 지속적인 교육이 포함된다. 직원 교육은 고객신원확인, 고객확인 그리고 보고 요구사항에 중점을 두고 (1) 자금세탁과 테러자금조달의 상황과 과정을 기술, (2) AML/CFT 법과 규제 요구사항 설명, 그리고 (3) 협의대계와 관련한 보고 의무사항에 대한 기관의 방침과 시스템을 설명할 필요가 있다.

또한 구직자들은 자금세탁 그리고 테러자금조달에 금융기관을 이용하려는 의도가 있을 수 있으므로 구직자들을 선별해야 한다. 191)

경영진 급에서 AML/CFT 준법감시인의 지정은 각 금융기관에 권고된다. 192) 준법감시인은 자신의 기관의 준법 노력에 적절한 경영진의 주의가 할당되도록 돕는다.

189) Id., Recs. 4 그리고 28.
190) Id., Recs. 15.
191) Id.
192) Id., 금고사정 15의 확설서
감사 기능 또한 수립이 필요한 내부방침과 절차이다. 감사기능은 전반적인 준법 기능의 적절성을 시험하고 보장하기 위해 준법관리기능과는 독립되어야 한다. 193)

G. 규제 및 감독 - 신뢰성 관련 기준

이전의 논의는 금융기관과 지정된 비금융전문직을 관리하는 국가기관에 의해 적용되어야 하는 AML/CFT 예방조치를 다루고 있다. 국가기관이 법으로 그러한 요구사항을 부과하는 것은 충분하지 않다. 국가들은 또한 실질적으로 이행되도록 하는 조치를 취할 필요가 있다. 국제기준의 수많은 요소와 마찬가지로 규제와 감독의 범위는 당해 기관에 대한 자금세탁과 테러자금조달의 위험에 근거해야 한다. 기준 제정기관들이 수립한 제재는 다음에 관한 각기 다른 유형의 규제와 감독을 예견한다.

- 핵심원칙 대상 기관
- 기타 금융기관, 그리고
- 지정된 비금융전문직

40개 권고사항의 신뢰성 기준과 관련한 규제와 감독 권고사항은 제5장 감독 및 규제 - 신뢰성 관련 기준에서 상세히 논의된다.

H. 법인 및 법적계약

각국은 자금세탁자들과 테러자금조달자들이 불법적으로 회사와 기타 형태의 법인을 이용하는 것을 방지하는 적절한 조치를 취해야 한다. 194) 이러한 조치에는 실 소유자와 법인 동체에 관한 정확하고 시의적절한 정보가 포함된다. 이 정보는 신속하게 해당기관에서 이용할 수 있어야 한다. 또한 무기명조직이 허용되는 국가에서는 무기명증권이 자금세탁이나 테러자금조달 목적에 이용되지 않도록 적절한 조치가 취해져야 한다. 195)

193) Id.
194) Id., Recs. 33.
195) Id.
국가는 또한 신탁 및 유사한 법적계약이 자금세탁이나 테러자금조달 관련자들에 의해 악용되지 않도록 적절한 조치를 취해야 한다. 196) 이러한 예방조치에는 신탁 및 유사한 법적계약의 체결자(settler), 수탁자 및 수익자에 대한 세무정보 열람이 포함되어야 한다. 197)

196) *Id.* Recs. 34.
197) *Id.*
제7장: FIU

A. FIU의 정의
B. 핵심 기능
C. FIU의 유형
D. 추가 기능
E. FIU 설립
F. 비밀보호 장치
G. 정보와 피드백
제7장 FIU

<table>
<thead>
<tr>
<th>A. FIU의 정의</th>
<th>E. FIU 설립</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. 핵심 기능</td>
<td>1. 적당한 모델 선택</td>
</tr>
<tr>
<td>1. 보고된 정보의 중앙저장과</td>
<td>2. 역량관련 고려사항(capacity considerations)</td>
</tr>
<tr>
<td>2. 분석</td>
<td>3. 인적 자원 관련 고려사항</td>
</tr>
<tr>
<td>3. 정보 제공</td>
<td></td>
</tr>
<tr>
<td>C. FIU의 유형</td>
<td>F. 비밀보호 정책</td>
</tr>
<tr>
<td>1. 행정</td>
<td>1. 주요 방향내의 징벌 비밀보호 대 효율성</td>
</tr>
<tr>
<td>2. 법집행</td>
<td>2. 기밀보장 원칙</td>
</tr>
<tr>
<td>3. 사법</td>
<td>3. 특정성의 원칙(specialty principle)</td>
</tr>
<tr>
<td>4. 아이비리드</td>
<td>4. 독립성과 책임성</td>
</tr>
<tr>
<td>D. 추가 기능</td>
<td>G. 정보와 피드백</td>
</tr>
<tr>
<td>1. 감독 또는 규제책임</td>
<td></td>
</tr>
<tr>
<td>2. 수사</td>
<td></td>
</tr>
<tr>
<td>3. 자신의 집행 및 정보확정</td>
<td></td>
</tr>
<tr>
<td>4. 교육</td>
<td></td>
</tr>
<tr>
<td>5. 리서치</td>
<td></td>
</tr>
</tbody>
</table>

자금세탁방지와 테러자금조달 대응에 관련된 이들은 금융수사를 위해 특정한 종류의 금융정보를 볼 수 있어야 한다. 이에 따라 FIU는 그 과정에서 중요한 역할을 담당하고 있다.198)

자금세탁자들은 불법수익의 성질, 출처, 소재, 처분 및 이동을 은닉하거나 가정하려는 시도로 불법수익을 조작하여 공용적으로는 제도권 금융으로 통합하려 한다.199) 테러자금조달자들은 테러지원을 위해 자금 출처를 은닉하고 자금의 불법 사

198) FIU에 관한 종합적인 논의는 IMF와 세계은행에서 발간한 FIU, 개요(2004), (FIUs Overview) 참조. www.amicft.org.(임기전용)
용을 가중하기도 한다. 금융수가 특정 정보의 보고와 기록보존을 요구하고, 국내외적으로 해당기관 간에 정보공유를 촉진하는 국가의 종합적인 제도로 크게 도움을 받는다. 금융수자의 주요 목적은 자금 식별, 추적 및 문서화, 법집행조치 대상인 자산의 식별 및 소재파악, 그리고 범죄 기소 지원이다.

금융수사는 범죄자가 남긴 금융 관련 살비를 발견하는 것이다. 이 과정의 일부로써 수사관들은 금융기관의 계좌기록, 부동산기록, 담보권과 관련된 문서, 법인 등기, 증가 및 류추얼펀드 계좌, 보험계약과 기타 광범위한 금융 및 사업 관련 기록을 분석한다. 불법적인 금융 활동은 즉각 보다 복잡하고 정교해져 이전의 수사관들이 새롭고 전문적인 금융정보 수단을 취득하도록 요구한다.

자금세탁방지와 테러리즘금조달 척결에 관한 국제기준 제정기구로 인식되는 FATF는 40개 권고사항에 각국이 FIU를 설립해야 한다고 명하고 있다. 또한 국가들이 금융기관과 특정 비금융전문가에게 고객의 신원과 거래에 대한 기록을 보존하고, 의심스러운 거래를 보고하도록 요구하는 조치를 부과하도록 촉구한다. 이와 같은 보고 및 기록보존 요구사항에서 생성된 정보는 국가의 FIU로 보고되고, 거래 재구성, 개별 고객과 특정 사업체 사이에 연관성 확인, 개인의 “주관적 요소” 증명 그리고 마지막으로 범죄자 또는 테러리스트의 자금조달 활동에서 개인의 역할 식별에 이용된다.

정보 보고와 기록보존 요구사항은 많은 양의 금융자료를 생산하게 되는데 이 자료의 대부분은 추가 분석 없이 해당기관이 사용하는 것이 쉽지 않다. 한 국가의 AML/CFT 제도의 구조가 효과적인 경우 이 정보를 처리, 분석 및 제공하는 신뢰할만하고 효율적인 제도를 설립해야 한다. 이러한 제도의 수립 없이 법집행은 범죄자 또는 테러리스트의 금융 거래를 적발하는데 더욱 어려워진다. 금융범죄 가능성을 대한 효과적인 자료 분석의 필요성은 부분적으로 FIU의 확산과 자금세탁과 테러리즘금조달 방지, 적발 및 기소와 관련된 국제적인 노력에서 FIU 역할의 중요성 증대를 설명해 준다.

201) Id., Recs., 10-22.
202) 20046 현재 94개국이 애그룹 회원인 FIU를 설립했음. 전 세계 FIU 에그룹그룹 http://www.egmontgroup.org/ 참조
A. FIU의 정의

FIU 관련 국제기준 세정기구인 에그룹은 1996.11월에 다음과 같은 FIU 정의를 채택했다.

(i) 의심스러운 범죄수익 관련하여 또는 (ii) 자금세탁척결을 위해 국내범이나 규정에서 요구되는 경우 금융정보의 수집(그리고 허가를 받은 요청), 분석 및 해당기관에 제공, 공개를 담당하는 중앙국가기관203)

일례모범적은 "직 회원국은 잠재적인 자금세탁과 관련한 정보의 수집, 분석 및 제공을 위한 국가센터로 FIU의 설립을 검토해야 할 것이다"204라고 명시하며, 이 정의를 채택했다.

이 정의를 확대하여 FATF는 국가에 FIU 설립을 요구하는데 FIU에는 3가지의 필수 기능이 있다. 그것은 자금세탁과 테러자금조달 식발 및 척결을 위해 보고된 정보의 "수집기관" 또는 "저장기관", 분석 및 금융정보 공유205이다. FATF는 또한 모든 국가기관이 국내외 파트너들과 정보교환하고 협력해야 한다는 일반적인 요구 사항을 보유한다.206)

2004년 에그룹은 특히 테러자금조달 척결을 포함하도록 FIU의 정의를 수정했다.207) 최근의 FIU 정의는 다음과 같다.

금융정보의 수집(그리고 허가를 받은 요청), 분석 및 해당기관에 제공, 공개를 담당하는 중앙국가기관:

i. 의심스러운 범죄수익과 잠재적인 테러자금조달과 관련하여

ii. 자금세탁과 테러자금조달 척결을 위해 국내외나 규정에서 요구되는 경우208)

결과적으로 에그룹의 FIU 정의는 40개 권고사항과 일치하게 됐다.

204) 일례모범적 제7조 (1)(b).
205) The Forty Recommendations, Recs. 36, 37 그리고 40.
206) Id., Recs. 26 그리고 31.
208) Id.
B. 핵심 기능

FIU는 나라마다 다르지만 3개의 핵심 기능을 포함한다: 자금세탁과 테러자금조달 척결을 위해 정보를 수령, 분석 및 제공한다. 금융정보의 제공은 국내외적으로 이루어져야 한다.

자금세탁은 종종 국경간의 활동이기 때문에 타국의 FIU와 협력하는 것이 중요하다. 따라서 FIU 관련법과 규정을 포함하여 자금세탁과 관련한 최고의 국내법과 규정조차도 자금세탁과 테러자금조달을 효과적으로 방지하기 위해 효과적인 국제 정보공유절차가 필요하다.

1. 보고된 정보의 중앙지정고

금융기관은 모든 의심스러운 활동과 FIU에 공개가 요구되는 다른 것들(교역현금거래보고)을 보고해야 한다.209 이 “저정기관 기능”의 집중화는(FIU를 공개되는 금융자료 수신자로 지정) 자금세탁방지를 위한 효과적인 국내외 예방구조의 전체 조건이다.210

자료 보고와 요구되는 공개를 위한 집중화된 저정기관 이용은 모든 관련 정보가 한 곳으로 모여 일관된 정보 처리 및 분석의 촉진을 보장한다. 집중화는 또한 정보 수집에 보다 큰 효율성을 보장한다.

2. 분석 기능

FIU는 법이나 국내규제기관에 의해 제출이 요구되는 금융정보를 위한 단순한 데이터베이스 이상이다. FIU는 수집하는 정보를 분석해야 하는데 이는 엄청나게 많은 STRs와 기타 공개되는 금융정보가 종종 정상적인 거래로 보이기 때문이다. 그러나 일상적인 예금, 인출, 자금 이체 또는 관련 구매나 보험 가입이 자금세탁과 테러자금조달의 적발과 기소에는 중요한 정보일 수 있다.

210) FIU 개요 참조, Chapter 3, 거래보고 절차.
FIU는 조사와 분석을 통해서만 범죄 성격을 띄는 금융거래를 식별할 수 있다. 실제로 의심스러운 거래가 단지 특정한 거래와의 구별에는 정보에 근거한 분석이 요구된다. 이러한 분석 없이는 세상에서 가장 정교한 형태의 자료 수집은 소용이 없는 것이다.

이러한 분석 기능은 국가들이 각국의 FIU에 필요한 법적 권한, 적절한 인적자원, 그리고 충분한 기술 역량을 부여하도록 요구한다. 특히 FIU의 분석 기능은 정보에 접근할 수 있는 확대된 권한이 요구된다. 이러한 권한에는 특정 상업 또는 정부 데이터베이스 열람, 보고기관과 기타 출처에 필요 시 추가 정보를 요청할 권한, 그리고 선진화된 정보수집 기법, 국내법에 따른 전화도청과 진복수사와 같은 정치가 포함되어야 한다. 211)

각국은 FIU의 효과적인 분석 기능에 대한 필요성과 비밀보호 관련한 우리 사이에 균형을 맞추어야 한다. 대중에게 공개된 상업 데이터베이스를 이용하는 것은 비밀보호 관련 우리를 제기하지 않으나 중앙정보기관에 추가 정보 요청을 허가하는 것은 우리를 냉각한다. 이것은 FIU 감독과 기타 정보수집 기법들도 동일하게 적용된다. 금융기관의 비밀보호법은 FIU의 기능을 방해하지 않으며 정보를 보호하는 방향으로 마련되어야 한다. 211)

FIU는 3가지의 전문적인 분석 기능을 수행하는데 이는 전술분석(tactical), 운영(추세)분석(operational) 그리고 전략분석(strategic)이다. 212)

a. 전술분석(Tactical Analysis)

전술분석은 사건을 구상하고, 범죄 뒤에 수반되는 사실을 제공하는데 필요한 자료를 수집하는 과정이다. 수령되는 모든 보고서를 전술분석 할 수 있으나 STRs가 가장 직접적으로 유용한 정보를 제공할 것이다.

전술분석에서 보고기관과 기타 기관에서 수령한 자료와 FIU가 보유하고 있는 자료 또는 FIU가 열람 가능한 자료와 비교해보는 것이 포함된다. 이러한 자료에는 성명, 주소, 전화번호, 보고기관에서 전달한 타 보고서 상의 자료가 포함된다. 일부

212) Id., Chapter 3. 보고서 분석
보고기관이 가정 단순한 형태의 전송정보를 생산하면 FIU가 그 보고서에 FIU의 데이터베이스에 보유하고 있는 보고된 고객이나 거래 관련 정보를 추가한다.

FIU의 직원은 STR이 접수되면 추가 분석의 근거를 제공하고자 대상자, 회사, 거래 또는 특정 사건과 관련된 기타 요소에 대한 추가 정보를 찾을 것이다. 추가 정보의 주요 출처는 다음과 같다.

► FIU 자체 데이터
► 대중에게 공개된 출처
► 정부에서 보유한 데이터베이스
► 보고기관과 기타 기관으로부터의 추가 정보
► 다른 FIUs

b. 운영분석(Operational Analysis)

운영분석은 의심스러운 범죄자의 행동에 대해 다른 가설을 세우는데 전송정보를 이용한다. 운영분석은 수사과정을 지원하는 것이다. 이 분석에서는 활동 패턴, 새로운 타깃, 대상자와 공모사간의 관계, 수사 단서, 범죄 프로필을 만들기 위해 FIU가 이용할 수 있는 모든 출처의 정보가 이용된다.

운영분석의 한 기법은 금융 프로파일링이다. 이것은 분석가에게 개인, 개인들 또는 집단이 은닉한 수입에 대한 정보들을 파악하는 방법을 제공한다. 이것은 대상자의 금융 현황과 관련된 증거의 수집, 정리 및 제시를 위한 효과적인 간접적 방법이다. 프로필의 관련성은 타깃이 금융 유통과 수입 간의 차이에 대해 협력적인 출처를 증명하지 못함을 보여준다. 개인의 자산 추적 또한 대상자를 전체범죄와 연결시키는 단서를 제공할 수 있다.

운영분석을 통해 FIU가 접수하는 정보는 운영정보로 발전하고, 추가 조치를 위해 법집행기관이나 검찰에 전달될 수 있다.

213) ibd.  
214) ibd.
c. 전략분석 (Strategic Analysis)

전략분석은 FIU의 미래 업무에 이용될 지식을 개발하는 것이다. 전략분석의 주요 특징은 이것이 개별 사례와 관련되지 않지만 새로운 이슈나 맥락에 관련된 것이다. 전략분석의 범위는 FIU의 권한에 따라 매우 다르다. 그 범위에는 특정 집단의 범죄 패턴 식별이나 국가 차원에서 범죄의 패턴에 대한 통찰을 제공하기 포함될 수 있다.

전략분석은 모든 이용가능한 정보가 수집되어 분석된 후 전개된다. 이것은 운영 분석보다는 철저한 임명위한 자료와 숙련된 분석관이 요구된다. 자료는 보고기관, FIU 자체의 운영정보 및 전출정보, 공개 출처, 법집행 및 기타 정부기관에서 제공한 보고서에서 나온 것이다. 전략분석은 보다 넓은 수준에서 새로운 단체에 보고 요구사항과 기타 AML/CFT 의무를 부과하고, 기존의 보고요구사항을 강화할 필요성을 제안할 수도 있다.215)

3. 국내 정보공유

자금세탁이나 세리아금조달이 의심되는 경우 수사나 조치를 위해 국내의 타 기관과 금융정보와 첨문을 공유할 권한을 보유해야 한다. 또한 자금세탁과 세리아금 조달의 직후, 방지 및 기소에 전담하고 있는 국내의 타 기관과 협력하고 조치를 조정하도록 하기가 주어져야 한다.

해당 기관과의 시의적절한 정보공유는 매우 중요하다. 자금세탁방지를 위한 효과적인 조치는 해당기관이 이용 가능한 정보를 취득하는 것이 달려있다. 대부분의 FIU들에게 정보공유는 주로 보고된 금융정보의 일부 분석 이후에 이루어진다. 다른 FIU의 경우, 특히 엄청난 양의 금융정보를 접수하는 FIU의 경우 금융정보는 법집행기관이 즉각적으로 이용할 수 있다. 이 FIU들은 사후에 필요한 법집행기관의 요청에 따라 보고된 금융정보와 기타 금융정보를 분석한다. 어느 경우에도 핵심은 FIU가 해당기관에 가능한 한 신속하게 금융정보를 제공하여 해당기관이 FIU 에서 제공한 단서를 추적할 수 있는 것이다.216)

215) ibd.
216) ibd, Chapter 3, 보고서 제공.
국내 조정도 중요하다. FIU는 국내 조정에 필수적인 파트너가 되어야 하고, 자금세탁방지에 있어 관련기관을 조정하는데 리드 역할을 할 수 있는 권한이 부여되어야 한다. 관련기관에는 FIU, 금융부문 규제기구 및 감독기구, 경찰, 사법부, 그리고 기타 관련 부처가 있다.\textsuperscript{217}

4. 국제적인 정보공유

자금세탁과 데라자금조달의 많은 부분이 국경간 활동이기 때문에 FIU는 자금 세탁방지 방지를 위한 국제적인 노력에서 유능한 파트너가 되기 위해 전 세계의 FIU와 금융정보를 공유할 수 있어야 한다. FIU의 핵심적인 특징은 외국 상대기관과 효율적으로 신속하게 협력할 수 있는 능력이다. 국제적인 정보공유는 외국 상대기관과의 직접적이고 안전한 의사소통을 통해 이루어져야 한다.\textsuperscript{218}

C. FIU 유형

국가들은 FIU를 설립하거나 그것의 업무 개선 시에 다음의 4가지 기본적인 모델중의 하나를 선택한다.

a. 행정모델\textit{(administrative model)} - 중앙은행이나 재무부와 같은 규제/감독기관에 부속되어 있거나 독립적인 행정기관
b. 법집행 모델\textit{(law enforcement model)} - 일반적 또는 전문화된 것과 관계없이 경찰에 부속된 경우
c. 사법 또는 검찰모델\textit{(judicial or prosecutorial model)} - 사법부나 검찰청에 부속된 경우
d. 하이브리드 모델\textit{(hybrid model)} - 위 3개의 혼합형

첫 번째 FIU가 1990년대 초에 설립되었을 때 이러한 다양함은 주로 국가의 각기 다른 상황과 국제적으로 승인된 모델의 부족한상에 기인한다. 예를 들면 일부 국가에서는 자금세탁과 관련 범죄의 척결 시에 법집행기관을 위한 추가 수단으로써 FIU의 기능이 강조되었고, 이것은 수사 또는 검찰기관에서 FIU를 설립하는 계

\textsuperscript{217} The Forty Recommendations, Rec. 31.
\textsuperscript{218} 제7장 국제협력 절조
가 되었다. 다른 국가들은 금융기관과 경찰 간의 “버퍼(buffer)”에 대한 필요성을 강조했고, 따라서 이들 국가의 FIU는 수사기관이나 경찰기관에서 독립적으로 설립되었다.

그러나 4가지의 분류가 어느 정도는 자연적이고, FIU를 분류하는 다른 방법도 있다는 것이 강조되어야 한다. 아래의 논의는 각 모델에 대한 기술, 장점 및 단점 (전부가 나열된 것은 아니) 그리고 모델을 이용하는 국가의 사례이다.

1. 행정모델(administrative model)

행정 타입 FIU는 주로 법집행기관이나 사법부가 아닌 정부 또는 기관의 일부이거나 감독을 받는다. 행정 모델은 분리된 기관으로 존재하기도 하는데 부 처나 정부의 감독을 받거나 자치모델 받지 않는 경우(독립모델)가 있다. 이러한 체제에 대한 이론적 설립은 금융부문(그리고 보고대상인 비금융전문적)과 금융범죄수사와 기소를 담당하는 법집행기관 사이에 “버퍼”를 만드는 것이다.

행정 타입 FIU 모델의 이점은 다음과 같다.

- FIU는 금융부문 및 보고대상인 기타 부문과 법집행기관 간에 연결기구로 역할. 이것은 공개된 정보를 법집행기관의 주의를 끌게 하는 동시에 보고 기관과 법집행기관 사이에 직접적인 제도적인 연계를 맺는다.
- 금융기관과 타 기관들은 정보의 제공이 자금세탁과 테러자금조달 사건에 한정될 것을 알고, 그 정보 공개가 보고기관의 행정 정보이기보다는 FIU의 자체 분석에 근거할 경우 정보 공개에 보다 확신이 있다.
- FIU는 보고기관에게 “중립적이고, 기술적 및 전문적인 대화의 상대(‘interlocutor’) 이다.
- FIU가 규제기관 내에 설치된 경우 이것은 금융기관에게 일반적인 대화의 형태이다.
- 모든 유행의 FIU와 쉽게 자료를 교환할 수 있다.

219) FIUs Overview, FIU 설명.
단접은 다음과 같다.

- FIU가 법집행기관에 소속되지 않기 때문에 금융정보에 근거하여 협의하게 동결 또는 협의지 체포와 같은 법집행 조치의 적용이 지연될 수 있다.
- FIU는 법집행기관과 사법부가 증거를 취득하기로 보유해야 하는 법적 권한이 없다.
- 행정 타입 FIU는 정부의 직접적인 감독을 더 많이 받는다(완전히 독립적이지 않은 전).

행정 타입 FIU를 보유한 국가에는 안도라, 아르바, 호주, 벨기에, 불고비아, 불가리아, 캐나다, 콜롬비아, 크로아티아, 체코, 프랑스, 이스라엘, 한국, 러시아, 스페인, 이탈리아, 슬로베니아, 스페인, 우크라이나, 미국 및 베네수엘라가 있다.

행정기관을 금융기관 및 기타 보고기관과 법집행기관 사이에 "비피로" 만들므로써 담당은 보고기관의 협력을 보다 쉽게 얻을 수 있다. 보고기관은 법집행기관과 직접적인 제도적 연관성을 가지는 고객과 관계를 맺고 있는 경우가 종종 있다. 행정 타입 FIU는 운행부문에서 선호한다. 이 모델은 같은 이유로 보고기관 명단에 추가된 기관과 적합에 어필할 수 있다.

2. 법집행 모델(law enforcement model)

일부 국가에서는 FIU의 법집행 측면에 대해 강조하여 법집행기관의 일부로 FIU의 설립했는데 이는 그것이 새로운 기관을 구성하고 새로운 법적 그리고 행정 구조를 구성하지 않고 담당되는 법집행 권한을 가진 기구를 설립하는 가장 쉬운 방법이었기 때문이다.

운영적인 면에서 볼 때 이 모델은 금융법적 협약과 같은 기관 법집행기구에 가깝고, 기관 법집행기구의 전문지식과 정보에서 혜택을 볼 것이다. 그 대신 FIU가 절수한 정보는 법집행기관에서 보다 쉽게 열람할 수 있고, 수사에 이용될 수 있어 유용성이
증대된다. 기존의 국내외 범죄정보교환 네트워크를 통해 정보교환이 신속하게 이루어질 수 있다.

범집행기관 유형 FIU의 이점은 다음과 같다.

- 기존의 기반구조에서 설립되므로 새로운 기관을 세울 필요가 없다.
- 최대한의 범죄행으로 금융정보가 공개될 수 있다.
- 자금세탁과 기타 범죄의 정후에 대한 범집행기관의 반응이 신속하다.
- 방대한 국제범죄정보교환 네트워크(인터폴)를 통해 정보가 교환될 수 있다.
- 범죄기록과 정보부(intelligence community)에 상대적으로 쉽게 접근할 수 있다.

단점은 다음과 같다.

- 예방책보다는 수사에 중점을 두는 경향이 있다.
- 범집행기관이 금융기관에 대한 일반적인 대화 상대가 아니다. 따라서 시간이 걸릴 수 있는 상호간에 신뢰가 쌓이는 하여, 범집행기관은 대화에 요구되는 금융 전문지식이 부족한 수 있다.
- 금융기관의 자료에 접속승인을 받는 것은(보고를 거래 외에) 공식적인 수사가 착수되어야 한다.
- 보고기관은 그 정보가 범죄 수사(자금세탁과 테러자금조달만이 아닌)에 이용될 수 있다는 것을 아는 경우 범집행기관에 정보를 공개하는 것을 거절할 수 있다.
- 보고기관은 단지 “의심스러운” 거래에 대해 범집행기관에 정보를 공개하는 것을 거절할 수 있다.

범집행 FIU를 보유한 국가에는 오스트리아, 에스토니아, 독일, 폴란드, 아이슬란드, 아일랜드, 슬로바키아, 스웨덴, 영국이 있다.

또한 범집행 FIU는 분리되고 구체적인 법적 권한 없이 범집행기관의 모든 권한을 갖게 될 것이다. 이러한 권한에는 거래 동결, 자산 압수가 있다(기타 범집행기관의 권한에 적용되는 것과 동일한 정도의 사법부의 감독 아래).
3. 사법 또는 검찰모델(judicial or prosecutorial model)

이 유형의 FIU는 사법부 내에 설립되고 가장 혼란하는 검찰 아래 설립된다. 이
러한 체계는 주로 대법원을 보유한 국가에서 나타난다. 이러한 국가의 검사들은
사법부에 소속되고 수사기관에 대한 권한을 가진다.223)

사법 또는 검찰 유형 FIU는 은행비밀법이 매우 강력하여 금융기관의 협력을 보
장하는 데 사법부나 검찰청과의 직접적인 연계가 요구되는 나라에서 잘 운영된다.

이 유형의 FIU의 이점은 다음과 같다.

▶ 정치적 간섭으로부터의 독립성이 매우 높다.
▶ 정보의 공개는 법적 수사나 기소 권한이 있는 기관에 직접적으로 제공된다.
▶ 사법부의 권한(예: 자금 압수, 계좌 동결, 취조, 구류, 수색)을 즉각적으로
  이용할 수 있다.

단점은 다음과 같다.

▶ "의심"에 따른 정보 공개의 허가를 제외하고는 일반적으로 범죄의 범행
  FIU의 동일한 단점이 이 유형에도 적용된다.
▶ 사법부 또는 검찰청 유형이 아닌 FIU와 정보를 교환하는데 어려움이 있을
  수 있다.224)

이 유형을 보유한 국가에는 키프로스와 독일부르크가 있다.225)

4. 하이브리드 FIU

하이브리드 유형의 FIU는 위에 기술된 3가지 유형이 다른 방식으로 결합된
형태이다. 이 유형은 각기 다른 유형의 이점을 한 기구로 모으려는 시도이다. 일부
FIU는 행정 유형과 범죄의 유형의 특성을 결합하는 반면 다른 FIU는 검찰의 권한과

26) Id.
27) Id.
28) Id.
관세청의 권한을 결합한다. 일부 FIU에서는 지속적으로 모기업의 권한을 행사하는 반면 다양한 규제기관과 범죄기관 출신의 직원이 업무를 한다. “하이브리드” FIU를 설립한 국가에는 덴마크, 저지(Jersey), 건지 섬(Guernsey), 노르웨이가 있다.225)

D. 추가 기능

이용되는 모델의 유형과는 관계없이 핵심기능 외에도 여러 기능이 추가될 수 있다.

1. 감독 또는 규제책임

FIU는 기록보존과 보고 요구사항의 이행과 관련하여 금융기관과 비금융전문직의 감독권한이 부여될 수 있다.227) 이러한 경우 FIU는 또한 보고 또는 기록보존 의무를 이행하지 못하는 단체와 개인에게 제재조치나 처벌(예: 벌금, 허가 중지)을 부과할 권한이 주어질 수 있다. 이 외에도 자금세탁과 테러과금조달 방지에 관한 법의 이행에 요구되는 규정을 공표한 권한이 주어질 수 있다.

국가내의 일부 기관은 이와 같은 이행 문제를 담당할 필요가 있다. 대부분의 국가에서 이 책임은 각 금융부문, 비금융전문직의 감독기관에 속한다. 그러나 FIU가 금융정보를 분석하는 것 외에도 금융정보를 받는 유일한 기관이기 때문에 AML/CFT 의무 이행의 모니터링을 할 수 있는 민경만한 기관이다. 일부 국가는 AML/CFT 이행 관련 책임을 FIU에 주는 쪽으로 선택했다. 특정 국가에서 일부 보고기관과 보고개인들은 FIU의 감독 이외에는 다른 기관의 감독 대상이 아니고, 이로 인해 FIU가 제기되는 이행 문제를 대응하는 가장 적합한 기관이 된다.

이에 추가로 FIU는 자금세탁방지법의 이행과 관련하여 금융부문과 기타 보고부문에 대한 규정을 발행할 권한이 주어질 수 있다. 그러나 FIU에 대한 책임을 부여하는 경우는 기타 감독 권한 사안과 AML/CFT 필요시 간의 권한을 맞추는 문제가 고려되어야 한다. FIU가 핵심기능과 추가 책임을 수행하기 위해서는 적절한 자원과 정부의 지원을 받아야 한다. FIU의 인적 구성이 원활한 경우 추가적인 감독 또는 규제기능이 핵심기능을 겸제할 수 있다.

29) Id
30) Id, 기타 FIU 기능
2. 수사

국가들은 FIU에 자금세탁에 대한 지속적인 수사에서 기타 법집행기관에 수사지원을 제공하는 책임을 부여하기도 한다. 이러한 경우 FIU는 요청 시 수사기관과 정보를 공유하도록 기대된다. 이러한 권한에는 FIU가 금융기관에 추가정보를 요청하거나 잠재적 자산 식별하여 동결, 압수 또는 몰수를 포함하여 수사를 할 수 있도록 만들어주는 추가 권한 행사를 수행한다.

3. 자산의 접행 및 블로킹(Blocking)

국가들은 또한 FIU에 긴급 조치가 요구되는 경우를 효과적으로 대응하기 위한 임시조치를 취할 권한을 부여할 수 있다. FIU는 의심스러운 거래 식별의 필수적인 정부기관이므로 FIU에 몰수 대상이 될 수 있는 자산을 보존하는 임시 권한을 부여하는 것이 당연하다. 임시 조치에는 자산의 법적 처분을 제한하는 기타 조치 외에도 일시적인 자산 동결이 포함될 수 있다.

그러나 임시 권한은 FIU가 자금세탁과 테러자금조달 방지에 관한 법에 따라 몰수 대상이 될 수 있는 자산을 수사하고 식별할 수 있도록 요구한다. 그러나 이 과정에서 FIU가 국내외 상대기관과 정보공유 및 협의거래보고서 접수 및 분석과 같은 핵심기능을 수행하는데 충분한 자원을 보유하도록 특별한 주의를 기울여야 한다.

거래 블로킹 그리고 또는 자산동결에 관한 임시 권한이 허가되는 경우 그 권한은 주로 블로킹이나 동결의 기간이라는 측면에서 제한적이다. 자산 동결이나 압수는 주로 사법부나 FIU 외의 정부기관이 요구된다.228)

4. 교육

FIU의 집중되고 여러분야로 이루어진 전문지식으로 인해 자금세탁과 테러자금조달 대응 조치에서 금융기관의 인력에 조언을 제공하고 교육하는 정부기관으로 역할을 쉽게 할 수 있다.

31) Id
국가는 이 교육기능을 FIU에 추가할 것인지 여부를 결정하는데 있어 자원의 환계를 고려해야 한다. 교육 서비스에 대한 수요가 방대해 질 수 있으므로 이 분야에서 역량, 예산 및 전문지식은 매우 중요한 부분이다.

5. 리서치

FIU는 자금세탁과 테러자금조달에 관한 금융정보의 접수, 분석 및 제공에 관한 경험에 근거하여 정부에 연구 내용을 제공할 수 있는 독특한 지위에 있다. 이것은 FIU가 전략분석과 관련하여 독특한 권한이 주어진 경우 특히 그러하다. FIU의 전략 분석 기능은 독립된 연구를 수행하고 그 결과를 보고하는 것으로 확대될 수 있다.

수많은 기능과 마찬가지로 연구의 추가와 그 범위는 예산, 인력 및 전문지식에 달려있다. 그러한 자원 없이 FIU의 핵심기능은 수행되기 어려울 수 있다.

E. FIU 설립

FIU의 설립이나 기존의 FIU 업무 강화에는 결정되어야 할 사항이 많다.

1. 적절한 모델 선택

FIU 모델 결정은 국가의 문화적/경제적 특징과 법 전제 및 법집행 전통에 대한 실질적인 지식에서 비롯된다. 하나의 모델이 모든 국가에서 효과적이길 수는 없으나 일부 기준은 필수적이다. 아래의 논의는 질문의 형식을 밝혔다.

▶ FIU가 금융업무와 관련한 역량과 전문지식을 보유한 것인지 또는 보유하고 있는가? 아니라면 무엇이 필요할가?
▶ 재인용 또는 기존의 FIU와 금융업 사이의 관계는 어떠한가? 무엇이 그 관계를 강화하겠는가?
▶ 금융기관은 금융정보의 기밀을 보호와 개인의 비밀보호의 잠재적 침해 완화를 충진하는 문화를 보유할 것인가 또는 보유하고 있는가?
▶ 재인용 또는 기존의 FIU에 적용되는 법적 제도가 FIU가 국제적인 행정 협력에 참여하도록 허용하는지, 그리고 의심스러운 거래와 관련하여 신속
2. 역량 관련 고려사항 (capacity considerations)

금융수사는 개별 수사관과 금융정보 수집을 지원하는 기술 기반구조를 말한다. 
한국은 FIU가 그 직원의 분석능력을 최대한 활용할 수 있는 방법에 관한 정책 
결정을 해야 한다. 이러한 점에서 또한 분석능력을 위한 최상의 제도적 환경을 결 
정해야 하는데 여기에는 중앙은행, 재무부, 경찰, 사법부가 있다. FIU를 한 나라의 
기존의 규제, 행정 또는 법집행기관과 완전히 독립된 기관으로 만드는 것은 실각 
한 자원 분배를 낳을 수 있다.

3. 인적 자원 관련 고려사항

채용 방침은 자원, 비율 그리고 제도적 효과성과 관련한 문제와 관계가 있다. 수사 
관련 금융전문지식이 상대적으로 취약한 것은 가능한 한 다양한 인재의 채용을 위해 
금융수사의 여러 가지 성질에 따라 인적 구성이 검토되어야 한다는 것을 의미한다. 

직원의 배경과 채용 조건은 둘 다 중요하다. 한편으로는 재무부 직원, 은행 감독자 
그리고 관세청 관리는 각자의 금융전문지식과 보고기관과 관련된 거래에 대한 
이해력이 있다. 다른 한편으로는 경찰이나 사법부 관리들은 특히 FIU가 법집행 
권한이 주어진 경우 유용한 법집행 경험이 있다.

채용조건 또한 FIU의 업무에서 독립성과 기밀보장 정도에 영향을 준다. FIU 
분석관들에게 요구되는 고도의 분석능력/경험의 부족은 일부 국가가 타기관에서 
파견된 전문가들로 인력을 구성하는 것을 선택한다는 것을 의미한다. 이것이 비용 
이 적게 드는 것이기에는 하나 - 그리고 효과적인 정보공유를 보다 촉진하는 것 - 
정부는 비밀보장과 과천인력으로 조직 구성하는 것이 경제적인 영향을 고려할 필 
요가 있다.
F. 비밀보호 장치

FIU는 법적 그리고 제도적 보안장치에 대한 고립 없는 경계를 요구하는 매우 민감한 정보의 수호자이자 저장기관이다.

1. 주요 방침간의 갈등: 비밀보호 대 효율성

특정 방침간의 갈등은 FIU가 형태를 갖추면서 생긴다. 이 갈등은 주로 AML/CFT 법과 규정의 미심한 목표에서 기인하는데 이 목표들은 비밀보호 관련 이해관계자와 대립한다.229)

사금융통계법제법은 부분적으로는 은행보안법이 감독 및 범죄 행 노력에 만들어내는 장애물에 대한 대응으로써 생겼다. 일부 국가에서는 강력한 은행비밀보호 요구 사항이 범죄 및 규제위반 징벌과 자산 추적이나 물수에 요구되는 금융정보 취득을 위한 수사 노력의 비범하하게 착실시켰다. 이러한 결과는 금융기관 보안법이 FATF의 금고사항을 근거하지 않아야 한다고 규정하는 금고와는 상충되는 것이다.230) 변격로운 절차 또한 외국의 정보 그리고 또는 증거를 수집하려는 수사 노력은 발해한다. 금융의 국제화와 함께 이러한 우리를 더욱 심각하게 한다. AML/CFT 법은 오늘날의 국제화된 경제에서 효과적인 규제 및 범죄 범죄행을 위한 전제조건으로써 국내외적으로 효율적인 정보교환과 증거 수집을 보장하는 시도로 간주될 수 있다.

금융정보의 민감하고 은밀한 성질은 FIU가 중요한 금융증거수집과 정보공용 기능을 위해 필요한 전자상의 보안조치를 마련한 필요가 있음을 의미한다. 효과적인 법집행은 효율적이고 신속한 금융정보에 대한 접근에 달려있다. 그러나 이 법집행 필요성은 금융비밀 관련 우리를 넘어와 오용 소지에 대한 적법한 우리를 제기한다.

사금융통계와 대리사금융결나 범죄와 관련된 금융정보의 저장기관, 처리기관 그리고 정보보호소로서의 역할에서 FIU는 효율성 대 비밀보호라는 논쟁의 최전방에 서

32) 에그문권들의 목록에는 그 전문에서 “금융정보 공개의 민감한 성질을 면두에 두어야 한다”고 규정 한다. 또한 “FIU는 국내외 기관과 비밀보호법이 이러한 원칙에 따라 FIU에 정보보호를 금지 하는 것으로 구성되지 않도록 해야 한다”라고 규정한다” 33) The Forty Recommendations, Rec. 4.
있다. 이러한 갈등은 FIU의 구조, 기능, 권한 및 임무 절차에 대한 국가의 선택에 반영되어 있다. 국가들은 FIU의 권한과 재원에 대한 각각의 선택에 내재된 비밀보호의 비용에 대한 현실적인 평가를 할 필요가 있다.

2. 기밀보장 원칙

FIU에 기밀보장 원칙을 적용하는 것은 금융비밀정보의 오용에 대한 가장 중요한 보호 정치 중의 하나이다. 이 원칙은 FIU가 보고기관과 사법제도 사이에 중개인으로 기능을 수행할 수 있도록 해 줄 것이다.

FIU가 경찰이나 검찰청 같은 타기관에 소속된 경우 FIU는 주로 기밀보장에 관련 일반 의무에 따른다. 그 일반 의무가 부재한 경우 특정한 기밀보장 의무가 FIU의 관리 및 설립 관련 법률조항에 명시되어야 하고, 형사 재판조차 그리고/또는 효과적인 민사 재판조차 리렌치되어야 한다.231) 기밀보장 의무는 또한 일반적으로 적용되는 국내의 비밀보호법에도 규정될 수 있다.

그러나 FIU의 기밀보장 의무는 보고기관에 대한 피드백이 FIU와 금융 중개인 간의 관계와 보고기관이 효율적인 보고 절차를 개발하도록 하는데 중요하기 때문에 피드백 제공을 부담하게 제한하지 않도록 규정되어야 한다.232) 기밀보장 요구사항은 FIU 간의 국제협력을 금하지 않는 방식으로 준비되어야 한다.233)

3. 특정성의 원칙(specialty principle)

기밀보장 의무를 보완하기 위해 FIU는 금융기관과 기타 기관에서 보고할 정보의 이용을 제한하거나 보고기관으로부터 FIU에 요청된 것처럼 "특정성의 원칙 (specialty principle)"을 제택할 수 있다. FIU가 자금세탁과 테러자금조달 척절 이외의 목적으로 제공된 정보 이용이 금지되는 경우 국가들은 보고기관 및 기타 기관과 FIU 사이에 신뢰를 쌓을 수 있다.

특정성의 제한사항(Speciality limitation)은 “자금세탁과 테러자금조달 대응”이라는 것을 의미하는점에 달려있다. 제한사항은 FIU 설립 법에서 기술된 바와 같이 FIU가 관리하는 금융기관이 FIU의 의무 수행에만 이용될 수 있다는 의미로 규정되어야 한다. 이것은 또한 FIU의 정보제공 조건과 관련하여 특정한 법령 또는 규정 조항에서 명시될 수 있다.

특정성의 원칙(Specialty principle)은 충분히 넓은 의미로 작성되어 FIU가 자금세탁 및 테러자금조달 방지법과 규정을 이행하는 것을 금지하지 않아야 한다. 이것은 또한 FIU에 제공된 정보가 기본 전제법적 이해관계 또는 규정을 이행하는데 이용될 경우, FIU는 사용할 수 있음을 의미해야 한다. 이에 추가로 특정성의 원칙(specialty principle)의 FIU간의 국제정보교환에 적용되는 경우 국제협력의 효율성을 억제하거나 순상하지 않는 방식으로 규정되어야 한다.234)

특정성의 원칙(Specialty principle)의 위반은 제관에서 인정되지 않는 증가에 대한 절차상의 법 그리고/또는 기밀보장 위반의 면사 또는 법적 책임에 의해 제재되어야 한다.

4. 독립성과 책임성

국가들은 정치적 영향력으로부터 FIU의 독립성과 분석 대상 거래 또는 제공 대상 정보를 결정할 때 해당기관이나 기타 감독기관으로부터 독립성을 보장해야 한다. 독립성을 보장하는 금융정보의 오용이나 악용에 대한 또 다른 보호조치를 제공할 것이다. 독립성이 절대적인 개념은 아니고, 항상 책임성에 대한 약간의 조치가 있을 것이나 FIU는 오용되거나 기타 정부기관의 부적절한 영향을 받지 않아야 한다. 독립성의 이러한 특성은 FIU의 보고기관 관계에 신뢰감을 주고, 따라서 자금세탁과 테러자금조달 방지와 적발을 촉진한다.

이러한 독립성은 여러 가지 방식으로 보장될 수 있다. 특정한 경우에는 허용되는 한계를 넘어 제도를 이용할 수 있는 기관에 대한 의무 없이 자율 예산과 인력과 같이 독립된 기관으로 FIU를 설립하여 그 독립성을 유지할 수 있다. 그러나 이 독립성은 국외보고, 감사 그리고/또는 사법부 감찰이라는 책임 절차에 의해 달성되어야 한다.

G. 정보와 피드백

FIU가 자금세탁과 테러자금조달 채결을 위해 국가의 해당기관 이외에 보고기관과 개인과 간밀하게 협력하는 것이 중요하다. FIU는 비밀보호 의무와 일관되게 자금세탁과 테러자금조달 경향과 유형에 대한 피드백을 제공해야 한다. 이 피드백은 금융기관과 비금융전문적이 AML/CFT 업무와 통계체계를 개선시키고 특히 협의 거래보고 개선에 도움을 줄 것이다. 보고기관은 협의거래보고서의 유용성에 대해 FIU로부터 피드백을 거의 받지 못하거나 전혀 받지 못한다는 비판을 받받지 않는다. 따라서 보고기관은 보고에 대한 보고기관의 접근방식이 자금세탁과 테러자금조달 채결에 도움이 되는지 여부에 관한 지침이 없다.

FIU가 보고기관에 특정 보고서에 대해 언급할 수 있는 것에는 명백한 제약이 있으나(특히 그 보고서가 지속적으로 조사되고 있는 경우), FIU는 보고서의 질과 유용성에 대해 일반적인 피드백을 제공할 수 있어야 한다. 또한 자료를 수업하여 분석하고 나면 자금세탁의 현황과 경향에 대한 유용한 정보를 생산해야 한다. 이 것은 보고기관과 개인과 공유되어 AML/CFT 제도 설계 시에 유의해야 할 점을 알려야 한다. 특정 사건의 이력에 대한 피드백은 수사 관련 법적 절차가 종결되고 나면 유용했다는 것이 명백되어야 한다.

FATF는 FIU를 포함한 모든 해당기관이 지침을 세우고 피드백을 제공하도록 규정한다.238) 관계 당국들은 AML/CFT 평가에서 이 이슈가 중요한 역할을 할 것으로 기대한다. FIU는 또한 접수되고 제공한 STRs에 대한 종합적인 통계를 보유할 필요가 있을 것이다.239)

---
239) Id, Rec. 32.
제8장 : 국제협력

A. 효과적인 국제협력의 전제조건
B. 자금세탁 대응을 위한 국제협력의 일반원칙
C. FIU간의 국제협력
D. 금융감독자 간의 국제협력
E. 법집행기관과 사법당국 간의 국제협력
F. 세입 관련 범죄에 대한 검토(Considerations for Fiscal Matter Offenses)
제8장 국세협력

<table>
<thead>
<tr>
<th>A. 효과적인 국세협력의 전제조건</th>
<th>D. 금융감독자 간의 국세협력</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 국세협력의 전제조건: 종합적이고 효율적인 국내 역량 개발</td>
<td>1. 은행감독자 간의 협력</td>
</tr>
<tr>
<td>2. 국세협력 비준 및 이행</td>
<td>2. 증권감독자 간의 협력</td>
</tr>
<tr>
<td>3. FATF 권고사항과 기타 부문별 국제기준 이행</td>
<td>3. 보험감독자 간의 협력</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. 자금세탁 대응을 위한 국제협력의 일반원칙</th>
</tr>
</thead>
<tbody>
<tr>
<td>C. FIU간의 국제협력</td>
</tr>
<tr>
<td>1. FIU의 국제협력의 주요 특징</td>
</tr>
<tr>
<td>2. FIU의 국제협력 능력을 좌우하는 것</td>
</tr>
<tr>
<td>3. 각기 다른 기구의 기준간의 관계와 국제협력</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E. 범죄행동기관과 사법당국간의 국제협력</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 기본원칙</td>
</tr>
<tr>
<td>2. 추가 원칙</td>
</tr>
</tbody>
</table>

| F. 세입 관련 범죄에 대한 검토 (Considerations for Fiscal Matter Offenses) |

조직범죄와 기타 규모가 크고 수익성이 매우 높은 범죄 활동이 국경 간에 이루어지는 반도수가 높아지고 있다. 이것은 특히 범죄자들이 범죄수익의 불법 출처와 나아가 그들의 불법적인 활동을 은밀하기 위해 전 세계 자유롭게 자금 이전 시에 공개된 국제금융제도를 이용하는 경우 국경을 초월하여 자금세탁이 반복하게 발생한다. 전 세계의 여러 기관 간에 신속한 정보교환과 효과적인 국제협력은 자금세탁방지 성공의 전제조건이다.

국세협력은 자금세탁방지와 그와 관련된 수사의 모든 단계(즉, 금융정보수집, 수사 및 기소 단계)에서 필요성이 더욱 증대되고 있다. 예를 들어 자금세탁사건에 대한 금융정보 수집 단계에서 FIU는 혐의거래보고서와 제공된 기타 금융정보를 적정하게 분석하기 위해서 외국 상대기관과 정보를 교환할 필요가 있다. 경찰이 자금세탁 사건을 성공적으로 수사하기 위해서도 같은 절차가 필요하다. 경찰이나 자진 없이 외국 상대기관과 신속하게 정보를 교환하는 능력은 모든 FIU, 범죄행동기관 또는 검찰의 중요한 특징이 되어가고 있다.
또한 자금세탁자들은 항상 눈순하고, 비효과적이거나 부패한 자금세탁방지 및\n테러자금조달 대응 제도를 가진 피난처 또는 완전된 국제협력 역량을 지닌 국가를\n찾고 있다는 것을 염두에 두고 절절한 국제협력기반을 수립하는 것이 자국의 금융\n시스템에서 자금세탁을 방지, 적발 및 기소하는데 도움이 될 것이다.

A. 효과적인 국제협력의 전제조건

국가들이 기존의 국제협력 수단을 이용할 수 있기 위해서는 (1)종합적이고 효율적인\n국내 역량 개발, (2) 자금세탁과 테러자금조달 관련 국제협약 비준 및 이행, (3) 기타\n부문별 국제기준뿐 아니라 FATF의 권고사항 준수(40개 권고사항)과 9개 특별권고\n사항)을 포함한 몇몇 전제조건을 충족해야 할 필요가 있다.

1. 국제협력의 전제조건: 종합적이고 효율적인 국내 역량 개발

물론 필요한 모든 기관들을 설립하고, 필요한 권한, 책임, 직원 및 예산을 제공\n하여 이 기관들이 의무를 효율적으로 수행할 수 있게 하는 것은 한 국가가 타국과\n국제적인 수준에서 협력할 수 있게 하는 전제조건이 된다.3)

그 중에서도 국가는 효과적인 AML/CFT 기반을 갖추기 위해서 자금세탁과 테러\n자금조달 척결을 목적으로 협의조례와 기타 형태의 필수보고의 접수와 분석을 맡고\n있는 중앙기관인 FIU뿐 아니라 각 부문의 금융기관을 감독하기 위해 행정감독기관을\n설립해야 한다.

이와 유사하게 사법경찰시스템이라는 측면에서 국가는 제대로 기능을 수행하고\n부패하지 않은 사법/기소시스템과 아울러 자금세탁과 테러자금조달 수사 시에\n전문화된 기술과 훈련을 받은 효과적인 경찰 서비스를 보유해야 한다.

이러한 기관들을 적절히 설립하는 것은 국내 및 국제 수준에서 자금세탁과 테러\n자금조달 척결을 위한 효과적이고 종합적인 기반을 마련하는 셈이다.

3. 40개 권고사항(The Forty Recommendations), Rec. 36.
2. 국제협약 비준 및 이행


국가들은 또한 범죄수익의 세탁, 수색, 압수, 몰수에 관한 유럽회의 협약(Council of Europe’s Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990) (스트라스버그 협약:Strasbourg Convention))과 같은 각국의 지역기구에서 제작한 기타 AML/CFT 협약에도 서명하고 비준해야 한다.8)

국가들은 국내법에서 자금세탁의 범죄화와 국제협력과 관련된 조항을 포함하여 이와 같은 협약의 모든 조항을 완벽히 이행해야 하고, 그 이행으로 협약에서 규정하는 사법공조체계에 참여할 수 있을 것이다.9)

3. FATF 권고사항과 기타 부문별 국제기준 이행

국가들은 조직범죄, 자금세탁방지와 테러자금조달 대응에 관한 기존의 국제기준을 이행해야 한다. 이러한 기준들에는 자금세탁과 테러자금조달에 대해 한 국가의 법과 규정의 모든 측면에 적용되는 FATF 권고사항이 포함된다. 이것은 또한 바젤위원회에서 제작한 효과적인 은행감독을 위한 핵심원칙(Core Principles for Effective Banking Supervision)과 고객확인원칙(Customer Due Diligence Principles)이 포함된다. 기타 기준들은 국제보험감독사연합(International Association of Insurance Supervisors:IAIS), 국제증권감독

7. 40개 권고사항(The Forty Recommendations), Rec. 1, 특별 권고사항(Special Recommendations), Spec. Rec. 1.
8. 40개 권고사항(The Forty Recommendations), Rec. 35.
9. Id., Rec. 36.
B. 자금세탁 대응을 위한 국제협력의 일반원칙

관련 국제기준에 따르면 국가들이 정보교환과 국제협력을 위한 효과적인 통로가 자금세탁이나 테러자금조달 수사의 각 단계에서 존재하도록 다음의 일반원칙들이 이행되어야 한다.

▶ 국가 A의 기관이 국가 B의 기관에서 공식적으로 요청한 정보를 보유하고 있는 경우 요청을 받은 국가 A의 기관은 국가 B의 요청기관에 신속하게 정보를 제공할 수 있어야 한다.

▶ 국가 A의 기관이 국가 B의 기관에 유용하다는 것을 알고 있는 정보를 보유하고 있는 경우, 국가 A의 기관은 국가 B의 기관에 즉각적으로 신속하게 그 정보를 제공할 수 있어야 한다.

▶ 국가 A의 기관이 국가 B의 기관으로부터 정보나 문서를 취득 또는 수사나 조사의 수행 또는 자금세탁 관련 분석, 조사 또는 기소 시에 유용한 특정 조치를 취해주기를 요청받는 경우, 요청을 받은 국가 A의 기관은 요청받은 것을 수행할 수 있어야 한다(물론 요청받은 내용이 국내법에서 엄부수행을 규제하는 규칙에서 허용하는 것인 경우).

외국기관과의 정보교환, 지원과 협조 제공은 부당하게 제한된 조건에 중속되지 않아야 한다. 그러나 요청받은 기관이 그것의 지원에 특정 조건을 걸 수 있다는 것은 실리 적인 요구에 불과하다. 예를 들어 요청받은 기관은 그것의 지원에 다음과 같은 특정

10. Id., Rec. 40.
11. Id., Recs. 36과 40.
조건을 갖 수 있고, 요청기관은:

- 요청받은 기관과 유사한 기능을 수행한다(specialty principle)
- 요청에서 이용될 정보의 목적과 범위를 기술하고, 요청받은 기관에서 해당 정보를 전송하면 그 정보는 그 요청의 범위에 따라 요청기관에서 처리되어야 한다(투명성).
- 요청받은 기관에 적용될 수 있는 기밀조치와 유사한 기밀조치 대상이 된다(기밀조치).
- 자체적으로 요청받은 기관과 정보를 교환할 수 있다(상호주의).

C. FIU간의 국제협력

자금세탁은 국경 간에 이루어지는 활동이므로 자금세탁의 적용은 종종 각국의 FIU 간의 정보공유와 외국 상대기관과 효율적이고 신속하게 협조하는 능력에 의존하기도 한다. 국가들은 또한 FIU의 설립 시에 어떤 모델을 선택하느냐에 따른 결과를 인지하고 있어야 한다.

1. FIU의 국제협력의 주요 특징

FIU의 국제협력 역량은 동일한 의무를 수행하는 기관들 사이에서 상호정보원칙과 상호신뢰의 기반에 달려있다. 각 FIU는 에그룹그룹의 FIU에 대한 정의에 따른 주요 특징을 보유하고, 에그룹 원칙(Egmont Principles)에 따라 운영되어야 한다. 이로 인해 각 FIU가 다른 FIU들 서로 인정하게 할 것이다. 이러한 주요 특징들은 제7장, FIU 부분에 기술되어 있다.

각 FIU는 또한 금융거래정보와 기타 관련된 금융정보를 외국 FIU와 공유할 때 법적으로 허가를 받아야 한다. 특히 타 FIU로부터의 정보제공 요청 시 또는 자발적으로 정보를 교환하고 협력할 수 있어야 한다. 이것은 상호주의 또는 MOU와 같은 공식적인 상호협정을 통해 이루어질 수 있다. 마지막으로 요청받은 FIU는 요청 FIU의 수사와 관련된 정보나 내용분석을 신속하게 하거나 할 수 있도록 허가를 받아야 한다.

2. FIU의 국제협력 능력을 좌우하는 것

FIU의 국제협력 능력은 부당하게 제한적인 조건의 대상이 되지 않아야 한다.
(본 절의 B의 법적제한 참조). 기밀보장 조항을 포함하여 지적한 보호조치가 FIU 간의
정보교환이 국내외적으로 협의된 기밀보호와 자료보호 기본 원칙을 준수하도록
수렴되어야 한다.3) 모든 국가는 최소한 외국 FIU에서 수렴한 정보가 국내에서 취득된
유사한 정보에 적용되는 동일한 기밀보장 조항에 따라 처리되고 보호되도록 해야
한다.4)

3. 각기 다른 기구의 기준간의 관계와 국제협력

FIU는 그의 내부조직구조나 운영구조와는 무관하게 모든 외국 FIU와의 국제
협력이 허가되어야 한다. 이것은 특히 전 세계 존재하는 FIU의 다양한 조직구조라는
측면에서 중요하다. 실제로 금융정보수집기구인 대부분의 FIU는 재무부, 규제/감독
기관, 또는 기타 임시행정조직과 같은 행정기구에 부속되어 있거나 경찰조직에 부속
되어 있다. 어떤 FIU는 감찰에 부속되어 있는 경우도 있다. 대부분의 FIU가 동일한
책무를 공유한다 하더라도 이들 간에 법적/절차상의 차이뿐 아니라 구조상의 차이
점이 있을 수 있다. 따라서 특정 FIU의 최대치의 국제협력 능력을 관리하는 규칙은
이러한 다양성을 고려해야 한다. 다시 말하면 FIU가 그것의 성격이나 조직구조와는
무관하게 모든 외국 FIU와 정보교환을 할 수 있도록 그 규칙들이 충분히 탄력적
이어야 할 필요가 있다는 것이다.5)

한 국가의 FIU에게 (1) 금융정보 공유에 제한이 있는지 여부, (2) 제한이 있다면
공유되어야 하는 정보의 양, (3) 공유되어야 하는 정보의 종류가 문제가 된다.
따라서 정책입안자들은 특정한 FIU 모델을 선택하는 것은 FIU의 국제협력 능력에
적합한지 등의 영향이 있다는 것을 인식해야 한다. 예를 들면 순전히 사법부에 기반을
든 FIU의 설립은 사법적인 FIU가 없는 타국과의 국제협력에 장애가 될 수 있다.
실제로 많은 국가에서 기본 법률 원칙이나 현행에서는 사법당국이 행정기관이나
경찰과 동일한 국제협력이나 정보교환 체널을 이용하는 것을 허용하지 않는다. 몇

13. 40개 권고사항(The Forty Recommendations), Rec. 40.
14. 자금세탁사례를 위한 FIU 간의 정보교환원칙(Principles for Information Exchange Between financial
Intelligence Units for Money Laundering Cases), 목표서 별첨(Annex to Statement of Purpose),
에그몽그룹(The Egmont Group).
15. 40개 권고사항(The Forty Recommendations), Rec. 40.
몇 국가에서는 이러한 법률 원칙에서 사법당국이 사법부의 협력절차에 따라서만
국제협력을 하도록 강제하는 경우도 있는데 이 협력절차는 다수의 제한조건이 있을
수 있는 조약과 원칙에 따라 관리된다. 이러한 조건은 정보수집단계에서 외국 FIU와의
종합적이고 신속한 정보교환을 맺을 수 있다.

D. 금융감독자 간의 국제협력

금융감독자(은행, 보험, 증권)가 AML/CFT 분석 및 조사와 관련하여 외국 상대
기관과 협력하고 또는 요청 시에 협력하도록 허가되어야 한다는 것은 널리 인정
되고 있는 사실이다. 위와 Part B에서 기술된 바와 같이 국제협력 일반 원칙은
이러한 특정 정보교환 채널에 적용된다. 감독과 관련해서 관련 감독자 사이에 각
각의 부문에서 이와 같은 협력이 이루어진다.

1. 은행감독자 간의 협력

바젤위원회는 정보공유와 관련하여 추가 원칙을 발표했는데 이는 모든 은행감독
자에 적용된다. 이 원칙들은 2001년 10월에 바젤위원회에서 발간한 고객확인제도
논문(Customer Due Diligence paper)에서 수립되었다. 특히 은행의 지점 감독자들은
본국의 감독자들이 그 정보를 필요로 하는 경우에 예금, “여신 집중”, 또는 관리
대상 자금 통지와 관련된 통합보고서를 공유할 수 있어야 한다.16

소재국은 외국은행의 본국 감독자들이나 감사자들이 지점 차원에서 외국은행의
사회자들 간에 본국의 “고객알기” 절차와 방침 준수를 검증하기 위한 현장 실사
를 수행하는 것을 허용해야 한다. 이것은 고객 파임과 임의 추출된 계좌에 대한
검토를 요구할 것이다.17

본국 감독자들이나 감사자들은 소재국에서 필요한 범위에서 개별 고객의 계좌에
대한 정보를 열람할 수 있어야 한다. 이것은 감독자들이 실행 중인 위험관리업무를
평가하는 것 뿐 아니라 고객신원확인에 적용되는 고객확인제도의 기준을 적절히

16. 바젤은행감독위원회(Basel Committee on Banking Supervision), 고객확인제도(Customer Due Diligence
17. Id.
평가하는 범위까지를 의미한다. 18)

마지막으로 감독자들은 협력 활동을 통해 취득된 개별 계좌에 관한 정보가 합법
적인 감독 목적에만 제한적으로 이용되고, 그 정보의 수취인에 의해 적절한 방식
으로 보호되도록 보호 장치를 수립해야 한다. 19)

2. 중권감독자 간의 협력

IOSCO는 모든 중권감독자에게 적용되는 추가 원칙을 발표했다. 중권감독자들은
국내외 상대기관과의 공개 및 비공개 정보의 공유에 대한 권한이 있어야 한다. 20)

국경 간 위법행위의 적발과 역제를 용이하게 하고, 허가 및 감독 책임 이행 시에
지원하기 위한 협력체계가 국제수준에서 수립되어야 한다. MOU가 여기에 포함된다. 21)

국제협력은 (1) 허가 소지인, 상장된 회사, 주주, 설소유주 또는 허가 소지인이거나
회사를 관리하는 개인에 대한 공개 또는 비공개 정보 취득(은행, 중개업 또는 기타
기록), (2) 요청된 대상자에 대한 정보를 보유할 수도 있는 자들에게서 자발적인
협조 수신, (3) 강요 하에 정보 취득(문서 생산이나 구두 집단 또는 진술 또는 이
두 가지 다), (4) 국가의 규제 절차에 대한 정보 제공 또는 (5) 법인명령이나 기
타 긴급한 이행명령의 보정 시에 지원할 수 있다. 22)

정보공유체계는 공식 이외의 무관하게 (1) 허가 소지인, 상장된 회사, 주주,
설소유주 또는 허가 소지인이거나 회사를 지배하는 개인에 대한 공개 또는 비공개
정보 취득, (2) 은행, 중개업 또는 기타 기록, (3) 요청된 대상자에 대한 정보를

18. Id.
19. Id.
20. 국제증권관리위원회이(International Organization of Securities Commissions : IOSCO), 핵심원칙
보다 상세한 것은 IOSCO 다자간 MOU (May 2002) 참조.
21. 국제증권감독기구 (IOSCO), 원칙, Sec. 9.4. 참조. IOSCO 원칙 11. 10. 그리고 IOSCO 공개문서
제52호, 집합투자제도의 국경 간 활동과 관련한 국제협력에 관한 논의 논문(Discussion Paper on
International Cooperation in Relation to Cross-Border Activity of Collective Investment
22. 국제증권관리위원회이기구(IOSCO), Principles, Sec. 9.4. “중분히 규제되지 않고, 비협조적인 국가에
의해 증권 및 선물 규제자들에 대해 제기된 문제에 관한 보고(Report on Issues Raised for
Securities and futures Regulators by Under-regulated and Uncooperative Jurisdictions),” 공개문서
제41호, 국제증권관리위원회기구 기술위원회, 1994년 10월
보유할 수도 있는 자들에게서 자발적인 협조, (4) 강요 하에 정보 취득(문서 생산
이나 구두 증언 또는 진술 또는 이 두 가지 다), 그리고 (5) 한 국가의 규제 체계에
대한 정보의 취득 또는 제공 시에 또는 법인명령, 예를 들어 긴급한 이행명령의
취득 시에 지원 제공을 검토해야 한다. 23)

3. 보험감독자 간의 협력

보험감독자들은 특정한 AML 목표를 위해 서로간의 협력을 관리하는 공식적인
규칙이 없다. 이것이 각국에서 허용하는 범위까지 정보를 공유하지 않다는 것을
뜻하는지는 않는다. 어떠한 경우에도 위에 기술된 바와 같이 일반적인 국제협력
원칙은 보험 부문에서 적용되어야 한다.

E. 법집행기관과 사법당국 간의 국제협력

검찰과 사법부 간에 국제협력은 자금세탁활동에 대해 종합적이고 효율적이어야
하는 모든 제도에 있어 중요하다. 수사의 한 시점에서 외국의 협조 없이 자금세탁
기소가 성공하는 사례는 거의 없다. 24)

국제협력은 유엔과 기타 지역 국제기구에서 동의한 모든 관련 협약의 시명과
비준에 달려있다. 실제로 이러한 협약들은 종종 외국 사법당국과의 정보교환과
외국 사법당국을 대신하여 조치에 참여하는데 필요한 법적 기반을 제공하기도 한다.

이 분야에 있어 일반적인 원칙은 위의 Part B에서 기술된 것과 동일하다. 사법적인
국제협력의 효과에 영향을 미치는 대수의 추가 그리고/또는 매우 한정된 원칙이 이 분야에서
수립되었다는 것을 뜻한다. 이러한 원칙들은 FATF 권고사항뿐 아니라 유엔의 다양한
협약에서 비롯된 것이다.

23. IOSCO, 원칙, Sec. 9.3.
24. 40개 권고사항(The Forty Recommendations), Rec. 36.
독립적인 사법당국들 사이에서 국제협력 체계를 협의할 때 헌법 요건의 변경이 존중되고 처리되어야 한다. 또한 특히 영향력 있는 개인이 관련된 경우 AML/CFT 협의자가 사건에서 인도대상이 아닌 범위에 속하는 “징치범죄”로부터 포기하는 것을 허용하지 않도록 주의를 기울여야 한다.

1. 기본원칙

법과 절차는 AML/CFT 범죄 행위에 있어서 특히 강제적인 조치의 이용과 관련하여 사법공조를 정리하고 촉진해야 한다. 여기에는 금융기관과 타인에 의한 기록 생산, 개인과 부지 수색, 제산 추적과 자산 확인, 자산 압류와 AML/CFT 수사, 기소와 외국에서 관련 조치에 이용된 증거 취득이 포함된다.25)

해당법과 절차에는 AML/CFT 수사 또는 소송 시에 요청국이 (1) 금융기관, 기타 단체 또는 자연인으로부터의 정보, 문서 또는 증거(금융기록 포함)의 생산 또는 압수, (2) 금융기관, 기타 단체 및 주소지 수색, (3) 중인 진술 취득, (4) 범죄의 수단뿐 아니라 세탁되었거나 세탁이 의도된 자산, 자금세탁 수익, 테러자금조달에 이용되었거나 이용이 의도된 자산 또는 그에 상응하는 가치의 자산의 추적, 식별, 동결, 압류 및 몰수를 추구하는 경우 효과적인 사법공조가 명시되어야 한다.26)

양자 또는 다자간 사법공조와 같은 국제협력을 지원하기 위한 조약이나 기타 공식적인 제도(그리고 비공식적인 절차)가 수립되어야 한다.27) 제도적인 장치와 기타 장치는 범죄행위가 수사 대상에 관해 외국 상대기관과 정보를 교환하는 것을 허용한다. 이러한 장치는 유효한 협의와 기타 협력 장치에 기반을 두어야 한다. 또한 국가기관은 정보교환 요청의 착수, 출처 및 목적뿐 아니라 그 해결결과도 기록해야 한다.

국가들은 해당 범죄행위기관과 사법당국에 적절한 금융, 인적 및 기술 자원을 제공하여 이들이 적당한 감독 보장, 수사 진행, 지원 요청에 신속하고 충분한 대응을 할 수 있도록 해야 한다.

25. Id, Rec. 40.
26. Id, Rec. 38.
27. Id, Rec. 27.
2. 추가 원칙

가능한 최대의 범위에서 국내법 하의 범죄의 "주관적 의도(mental intent)"에 관한 요청국과 요청받는 국가의 다른 기준들은 사법공조조서에 영향을 미치지 않아야 한다. 개인이 자금세탁과 전체범죄를 범한 경우 및 개인이 자금세탁만을 범한 경우 모두 수사와 소송에서 지원이 제공되어야 한다.28)

당국은 타국의 해당기관과 함께 수사(기밀정보의 통제된 인도 포함)에 협조하여 수행하도록 허가를 받아야 한다. 적절한 보호조치가 수립되어 있으면 확인되어야 한다.29)

적절한 조치는 가능한 경우 몰수가 적간접적으로 범죄행위기관의 협력 조치의 결과일 때 타국과의 몰수된 자산 공유 허가를 포함하여 압수와 몰수를 위한 효과적인 국경 간 협력을 허용해야 한다.30)

마지막으로 절차상으로 자금세탁, 테러자금조달 또는 관련 범죄 혐의로 기소된 개인의 인도의 인도가 가능하지 않은 경우 국내에서 고소된 자의 기소를 허용해야 한다.31)

F. 조세 관련 범죄에 대한 검토(Considerations for Fiscal Matter Offenses)

일반적으로 국가들은 해당기관이 외국 상대기관과 가능한 가장 폭넓은 범위로 국제협력을 하도록 보장해야 한다. 위의 섹션 B에서 지적된 바와 같이 국가들은 그들의 지원에 부당한 제한조건을 두는 것을 잃기야 함에도 불구하고, 몇몇 조건을 줄 권리가 있다. 국가들이 생명가법성(dual criminality)의 부재 시에도 지원을 하도록 권고되지만 사법공조(MLA)나 범죄인 인도(extradition)에 적용될 수 있는 조건은 생명가법성이이다.

몇몇 국가들은 조세포탈과 같은 몇몇 조세 범죄(fiscal offenses)를 자금세탁의 전

28. Id., Rec. 36.
29. Id., Rec. 27.
30. Id., Rec. 38.
31. Id., Rec. 39
제재죄로 범죄화하지 않고, 따라서 다른 국가가 세입 범죄 수익의 세탁과 관련하여 지원을 요청하는 경우 지원을 제공할 수 없을 수 있다. 그러나 세입문제가 요청의 일부이고, 비세입 관련 요소가 있어 이 비세입 관련 요소(non-fiscal component)에 자금세탁의 전체범죄가 포함되는 경우, 요청받는 국가는 지원을 제공해야 한다.
제9장 : 테러자금조달 대응

A. 유엔 관련 협약의 비준 및 이행
B. 테러자금조달과 관련 자금세탁 범죄화
C. 테러 자산의 동결 및 몰수
D. 테러 관련 혐의거래보고
E. 국제협력
F. 대체송금제도(Alternative Remittance Systems)
G. 전신송금(Wire Transfers)
H. 비영리기관(Non-Profit Organizations)
I. 현금반출업(Cash Couriers)
J. 테러자금조달에 관한 자기 평가 질문서(Self-Assessment Questionnaire)
제9장 테러자금조달 대응

<table>
<thead>
<tr>
<th>A. 유엔 관련 협약의 비준 및 이행</th>
<th>F. 대체송금제도(Alternative Remittance Systems)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. 테러자금조달과 관련 자금세탁 범죄</td>
<td>G. 전신송금(Wire Transfers)</td>
</tr>
<tr>
<td>C. 테러 자신의 동결 및 몰수</td>
<td>H. 비영리기관(Non-Profit Organizations)</td>
</tr>
<tr>
<td>D. 테러 관련 협의거래보고</td>
<td>I. 현금반출업(Cash Couriers)</td>
</tr>
<tr>
<td>E. 국제협력</td>
<td>J. 테러자금조달에 관한 자가 평가 절의서 (Self-Assessment Questionnaire)</td>
</tr>
</tbody>
</table>


FATF는 이와 같은 목표를 달성하기 위해 업무를 수정하는 동시에 최초의 테러자금조달에 관한 8개 특별권고사항을 제정했다. 2004년 10월에는 현금반출업(Cash Couriers)에 대한 새로운 특별권고사항 IX를 제정했다. FATF가 이전에 했던 것과 마찬가지로 자금세탁에 관한 40개 권고사항과 특별 권고사항은 단순한 제안이 아니라 테러자금조달 대응의 국제기준을 이행하고 있는 것으로 간주되려면 FATF 회원국이 아닌 모든 국가가 준수해야 할 행동의 원칙이라고 할 수 있다.1) 국가들은 특별권고사항의 평가방법에 대한 정보에 관해 AML/CFT 방법론을 참조할 수 있다.2) 또한 FATF는 모든 국가가 특별권고사항을 체계하고 자가 평가에 참여하도록 권고했다.3) 40개 권고사항과 함께 특별권고사항의 이행에서는 테러자금조달의 적발, 방지 및 역체에 관한 기본적인 것들이 명시되어 있다.

지급세탁방지 및 테러자금조달 대응에 관한 안내서

특별권고사항은 상대적으로 이전에 새로운 개념이다. 따라서 이전의 해석과 이행에 관한 해결이 다소 제한적이다. 처음에 FATF는 특별권고사항의 설명을 돕기 위해 일반지침서(Guidance Notes)를 체택했다.4) 시간이 지나 경험이 축적됨에 따라 특별권고사항의 몇몇 부분에 대한 공식적이고 보다 권위 있는 해설서(Interpretative Notes)를 발간했다.5) 또한 특별권고사항의 몇몇 부분에 대해 우수사례 지침(Best Practices guidance)을 발간하기도 했다.6) 마지막으로 금융기관이 테러자금조달에 이용되는 모니터링에 대해 배우는데 도움이 되는 수단으로써 테러자금조달 적발 시에 금융기관을 위한 지침(Guidance for Financial Institutions in Detecting Terrorist Financing)을 발간했다.7)

A. 유엔 관련 협약의 비준 및 이행

첫 번째 특별권고사항은 두 부분으로 구성된다. 첫째에는 "각 국가는 테러자금 조달억제를 위한 유엔협약(UN Convention for the Suppression of the Financing of Terrorism)(1999)을 비준하고 완전히 이행하는 즉각적인 조치를 취한다"라고 명시되어 있다.9) 이 권고사항 이행 평가자들은 국가가 이 협약의 여러 조항을 이행하기 위해 취한 조치에 특별한 주의를 기울인다.

두 번째 부분에서는 각 국가가 테러자금조달을 다루는 유엔 인보리 결의안, 특히 제1373호를 완전히 이행하도록 요구한다.10) 특별권고사항이 특히 제1373호11)를 언급하고 있는지거나 국가는 테러자금조달과 관련된 모든 결의안에 대응해야 한다. 다르게 그러한 결의안의 분야는 시간이 지나면서 변경될 가능성이 높다. 아래 나열된 결의안은 FATF 40계 권고사항과 8계 특별권고사항 이행 평가를 위한 방법론(Methodology for

Assessing Compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations)에서 현재 중요한 것으로 명시되어 있는 것이다.12)

- S/RES/1333(2000)14)
- S/RES/1363(2001)15)

모든 유엔 협약에서와 마찬가지로 실질적인 이행이 핵심이다. 협약 이행은 국가가 유엔협약 조항과 유엔 안보리 결의안이 유효하게 하기 위해, 즉 국내에서 법적으로 구속력이 있게 하기 위해 모든 적절한 조치와 필요한 조치를 취했다는 것을 의미한다.19) 이렇게 필요한 조치들은 한 국가의 헌법 및 법 구조에 따라 법, 규정, 명령, 혼령 또는 또 다른 해당 법률 및 행정조치에 의해 취해질 수 있다.20)

테러자금조달은 다룰 유엔안보리결의안 중에서 본 권고사항에 특별히 언급된 것은 결의안 제1373호이다.21) 이 결의안은 모든 유엔회원국이 다음을 하도록 요구한다.

- 테러자금조달 행위 범죄화
- 모든 형태의 테러집단 지원 거부
- 테러 행위와 관련된 개인, 조직 또는 단체의 자금 또는 자산 동결을 포함하여 테러리스트에게 피난처나 지원 제공 억제
- 테러리스트에 대한 능동적 또는 수동적인 지원 금지
- 계획된 테러행위에 대한 정보 공유와 범죄 수사 시에 타국과 협력22)

19. FATF, 지침서(Guidance Notes), Paragraph 5.
20. Id.
B. 테러자금조달과 관련된 자금세탁의 범죄화

특별권고사항의 두 번째 부분에는 두 가지의 요소가 담겨 있는데 이는 각 국가가 다음을 해야 한다고 요구한다.

- 테러자금조달, 테러행위 및 데러조직의 범죄화
- 테러를 자금세탁의 전제범죄로 지정

FATF는 각 국가가 특별권고사항 II의 이행방법을 기술한 해설서(Interpretative Note)를 발간했다.24) 이 권고사항은 자금이 불법적 또는 합법적 유래에서 비롯된 것인 지하는 관계없이(권고사항의 두 번째 요소에 따르면 이것은 자금세탁의 전제 범죄가 되어야 하는 경우) 각 국가가 테러자금조달, 테러행위와 데러조직을 범죄화 하도록 요구한다. 법은 테러자금조달이라는 관점에서 구체적이어야 한다. “교사 및 방조(aiding and abetting)” 또는 “시도(attempting)” 또는 “용모(conspiracy)”를 범죄화하는 것으로는 충분하지 않다.25) 이 개념은 몇몇 법제도에서는 항상 명확하지 않다. 따라서 법은 자금이 테러에 이용되어야 한다는 의도를 가지고 자금을 모집하거나 제공하는 자를 포함해야 한다. 자금이 실제로 테러에 이용되었는지를 입증하는 것은 필요치 않다.26)

C. 테러 자산의 동결 및 몰수

세 번째 특별권고사항에 따르면 각 국가는 유엔 결의안에 따라 테러리스트, 테러자금조달자와 데러조직의 자금 또는 자산을 동결하는 조치를 이행해야 한다.27) 또한 국내에서 “테러자금조달, 테러행위 또는 데러조직에 이용된, 이용이 의도된 또는 이용을 위해 합당한 수익인 재산을 압수하고 몰수함” 권한을 해당기관에게 주기 위해 적합한 조치를 취해야 한다.28)

23. (특별 권고사항) Special Recommendations, Spec. Rec. II.
25. Id.
26. Id.
27. (특별 권고사항) Special Recommendations, Spec. Rec. III.
28. Id.
FATF는 특별권고사항 III의 이행에 관한 공식적인 해설서(Interpretive Note)를 발간했다.29) 여기에 추가로 국가들이 이 권고사항의 요구조건을 가장 잘 이행할 수 있는 방법을 이해하는데 도움을 주는 우수사례집을 발간했다.30)

이 권고사항에는 다른 국가에서 각각 다른 의미를 지닐 수 있는 3가지의 기본 개념이 있는데 그것은 동결(freezing), 압수(seizure) 및 몰수(confiscation or forfeiture)이다. “동결”은 국가내의 해당기관이 특정한 자금이나 자산을 막거나 제한하여 그러한 자금이나 자산이 이환되거나 분산되는 것을 방지하는 권한을 가지는 것을 뜻한다.30) 그 “동결된” 자금이나 자산은 소유자의 재산으로 남게 되고, 금융기관의 관리와 기존의 관리통제 하에 있게 된다. 자산 동결의 목적은 소유자의 자산 동체권을 강화하고 하여 금지된 목적에 이용될 수 있도록 하는 것이다.

“압수”는 해당 국가기관이 명시된 자금이나 자산에 대해 동체권한을 가지는 것을 의미한다.32) 압수 상태에서 자산이나 자금은 원래 주인의 재산으로 남게 되지만 자산의 소지, 관리 및 통제는 관련 해당기관으로 넘어간다. “몰수”는 해당기관이 명시된 자금이나 자산의 소유권을 국가로 이전할 권한을 지니는 것을 의미한다.33) 몰수는 주로 자산이나 자금이 범죄 활동에서 유래했거나 법 위반에 이용되었거나 의도되었는 유죄판결이나 사법부의 판결이 있을 사에 발생한다.

테러리스트 자금은 관련 유엔결의의 권한에 따라 추가로 법적인 절차나 사법 절차 없이 행정조치로 동결되어야 한다. 유엔결의의 이행은 회원국에서 법적 구속력이 있는 의무기인에 모든 국가가 즉각적으로 행동하는 것이 가능해야 한다. 지체가 있는 경우 자금이 그 국가에서 이동될 가능성이 높기 때문에 실제로 동결조치가 즉시 이루어지는 것이 매우 중요하다.

유엔 1267 위원회는 알카다, 탈레반, 오사마비안라덴에 대한 여러 유엔결의의 권한에 따라 동결 명령이 내려진 자금을 소유한 개인과 집단의 통합명단을 발간한다.34) 동결명령은 앞의 개인 및 집단과 이들을 위해 행동하는 자와 관련이 있다. 이 명단은 업데이트되고, 통합명단은 유엔 웹사이트에 게재된다.

31. FATF, 특별권고사항 III에 대한 해설서, Paragraph 7a.
32. Id., Paragraph 7b.
33. Id., 지침서 Paragraph 7c.
D. 테러 관련 혐의거래보고

특별권고사항 IV에 따라 “차금이 테러, 테러행위 또는 테러조직과 연관되거나 이용되는 것으로 의심되거나 의심할만한 협력한 사유가 있는” 금융기관은 해당 기관에 혐의를 신속하게 보고해야 한다. 36)

이 요구사항은 40개 권고사항에서 규정된 바와 같이 금융기관과 지급에서야 40개 권고사항에서 규정되는 비금융전문직에 적용된다(제5장 참조). 37) 이 보고 요구사항은 국가의 자금세탁방지 및 테러자금조달 대응 법률의 적용 시에 일관적이어야 한다.

이 권고사항에는 두 가지 상황에서의 보고를 포함한다. 차금이 테러자금조달과 연관되었다는 “의심(suspect)”이 있는 경우와 차금이 테러자금조달과 연관이 있다고 “의심할만한 협력한 사유”가 있는 경우이다. 이 두 가지 경우의 구별은 요구되는 거래보고에 대한 기준을 규정하는 핵심이었다. 38) “의심”이라는 기준은 주관적인 것이고, FATF의 자금세탁방지 권고사항에서 적용되는 것과 동일한 기준이다. 39) “의심할만한 협력한 사유”라는 기준은 자금세탁방지 권고사항과 일관적이기는 하나 단순한 “의심” 기준보다는 넓은 개념이며, 따라서 더 넓은 범위의 상황에서 보고가 요구된다. 국가들은 이 보고 요구사항을 “의심” 또는 “의심할만한 협력한 사유의 존재” 기준에 근거해 만족시킬 수 있다. 40)

35. FATF, 특별권고사항 표에 대한 해설서, Paragraph I.
36. (특별 권고사항) Special Recommendations, Spec. Rec. IV.
37. FATF, 지침서 Paragraph 19.
38. FATF, 지침서 Paragraph 21.
E. 국제협력

특별권고사항 V에서는 각 국가가 사법공조체계나 기타 메커니즘을 통해 “테러 자금조달, 테러행위 및 테러조직과 관련된 범죄, 행정부 집행 및 행정 수사, 문의 및 소송과 연관된 가능한 가장 넓은 범죄죄의 조치”를 또 다른 국가에게 제공해야 한다고 규정한다.41 각 국가는 테러자금조달, 테러행위 또는 테러조직의 혐의를 받는 개인에게 피난처를 제공하지 않고, 가능하다면 그러한 자를 인도할 수 있는 절차를 수립하도록 모든 적절한 조치를 취해야 한다.42

이 권고사항의 첫 번째 부분에서는 사법공조체계나 이것이 외의 수단을 통한 정 보교환을 요구한다. “사법공조”는 증거취득, 형사소송이나 수사와 관련된 문서나 물품의 수색 및 입수, 형사 사건에서 외국인에게 제한, 압수, 물수령 및 집행함 능력을 포함한 모든 범주의 법적 지원을 제공할 권한을 의미한다.43 “사법공조가 아닌 기타” 수단을 통한 정보교환은 MOU, 시신 교환 또는 기타의 방식에 따라 양자 간에 정보를 교환하는 FIU나 기타 정부기관을 통한 교환을 포함한 기타 정책을 의미한다.44

이 권고사항의 두 번째 부분은 “피난처(safe haven)”와 “범죄인 인도”의 개념과 관계가 있다. 이러한 용어들은 유엔 안보리의안 제1373호45에서 이용된 “피난처”46, 그리고 테러자금조달억제에 관한 유엔국제협약47에서 이용된 “범죄인 송환”48이라는 용어와 동일한 의미를 지닌다. 국가들은 범죄인 인도와 관련하여 “정치적 동기의 주장은 테러자금조달에 관련한 것으로 혐의를 받고 있는 개인의 송환을 거절하는 사유로써 인정되지 않는다”라고 보장해야 한다.49 이 개념과 문구는 테러자금조달 억제에 관한 유엔협약에서 온 것이다.50

40. FATF, 지침서 Paragraph 21.
41. (특별 권고사항) Special Recommendations, Spec. Rec. V.
42. Id.
43. FATF, 지침서 Paragraph 24.
44. Id., Paragraph 25.
46. UN 안보리의안 제1373호 (2001), Paragraph 2 (c).
47. Id.
48. (UN)의 테러자금조달억제협약 UN Convention of Suppression of the Financing of Terrorism, 제 11조.
49. FATF, 지침서 Paragraph 26.
50. 협약 제14조
F. 대체송금제도(Alternative Remittance Systems)

특별권고사항 VI에 따라 각 국가는 “사급이나 가치의 이전” 서비스를 제공하는 개인과 법인가 허가를 받았거나 등록이 되어 있고, 대금결제관에 적용되는 동일한 기준, 즉 40개 권고사항을 준수하도록 조치를 취해야 한다.51) 불법적이나 그러한 서비스를 하는 단체들은 행정, 단서 또는 형사재개 대상이 되어야 한다.52) 이와 같은 요구사항은 비공식적인 송금제도를 통한 금전 또는 가치 이체에도 적용되어야 한다.

FATF는 이 권고사항을 이행하는 방법에 대해 국가들에게 공식적인 지침과 일반적인 지침을 제공하기 위해 우수사례집뿐만 아니라 해설서(Interpretive Note)를 발간했다.53)

비운행권 기관에서 제도권을 통해 개인이나 법인을 대신해 자금이 이전되는 공식적인 자금의 송금 또는 이체서비스를 종종 제공하기도 한다. 40개 권고사항 이행을 결정하려는 목적으로 "금융기관"이라는 용어의 정의 내에 포함되는 송금 서비스업자(money transmitters)들은 국가의 AML/CFT 법률 준수해야 하고, 허가를 받았거나 등록되어야 한다.54)

"금전 또는 가치 송금제도"라 함은 비공식적이고 감독을 받지 않는 네트워크나 절차를 통해 한 곳에서 다른 장소로 자금이나 가치가 이체되는 금융서비스의 한 유형을 말한다.55)

많은 국가에서 이러한 비공식적인 제도는 전통적으로 위에서 기술된 바와 같이 비제도권에서 운영되어 왔다. 이러한 비공식적인 제도에는 Black Market Peso Exchange, Hundi 또는 하럴라가 있다.56)

51. (특별 권고사항) Special Recommendations, Spec. Rec. VI.
52. Id.
54. (40개 권고사항) The Forty Recommendations, 용어, 금융기관.
55. FATF, 지침서 paragraph 31, 그리고 해설서 paragraph 4.
특별권고사항 VI의 목표는 국가들이 모든 형태의 금전/가치 송금제도에 대해 AML/CFT 요구사항을 부가하도록 보장하는 것이다. 57 따라서, 한 국가는 비공식적 인 것을 포함하여 최소한 모든 금전 및 가치 송금서비스가 특정한 FATF 및 국제기준을 준수하도록 보장해야 한다. 58) 다르나, 이 권고사항의 원칙적인 요건은 해당기관이 모든 비공식적인 금전/가치 송금서비스 업체에 허가를 내주거나 등록 하고, 이러한 업체가 자금세탁과 테러자금조달을 경계하도록 적절한 프로그램을 보유하는 것을 요구하는 것이다. 59) 이 요구사항은 40개 권고사항과 일치한다. 60)

국제사회는 이 권고사항을 통해 비공식적인 금전/가치 이체제도를 폐지하려는 것은 아니다. 대부분의 경우에 있어 이러한 이체제도는 제도권 금융 이용이 용이 하지 않은 사람들에게 귀중한 서비스를 제공한다. 그러함에도 불구하고 이러한 이체제도가 자금세탁 및 테러리스트에게 자금을 송금하는데 이용된 적이 있었고, 이 권고사항은 그러한 경우에 대해 AML/CFT를 적용하라는 목적이다. 이 권고 사항은 또한 이러한 송금업체의 이행을 요구하지만 이 업체들이 바젤위원회, 국제 보험감독자연합 또는 국제중권감독위원회기구에 소속된 기관으로써 동일한 규제와 감독 요건의 대상은 아니다.

G. 전신송금(Wire Transfers)

특별권고사항 VII에서는 각 국가가 송금서비스업체(money remitters)를 포함하여 금융기관이 자금 송금에 대한 정책적 유효한 송금자정보(이름, 주소, 계좌번호) 및 관련 메시지를 포함하도록 요구하고, 그 정보가 전체 송금과정에서 송금 또는 관련 메시지와 함께 남도록 요구하는 적절한 조치를 취해야 한다. 61) 여기에 추가해 그 금융기관이 전세 송금자 정보를 담고 있지 않은 의심스러운 자금송금에 대해 조사를 강화하고 모니터해야 한다. 62)

이 권고사항의 이행은 다소 복잡한 것으로 판명되었고, FATF는 이의 요구

57. FATF, 지침서 paragraph 29, 해설서 paragraph 2.
58. (40개 권고사항) The Forty Recommendations, Recs. 4-25.
59. Id., Rec. 23.
60. Id.
61. (특별 권고사항) Special Recommendations, Spec. Rec. VII.
62. Id.
사항을 명확하게 하기 위해 다소 긴 해설서를 발표했다. 이 권고사항에 적용되는 우수사례는 없다.

이 권고사항의 목적은 전신송금을 보내는 사람이 누구인지에 대한 정보를 취득하여 불법적인 목적으로 송금된 자금이 송금자와 함께 식별될 수 있게 하는 것이다. 정보 요구사항은 송금이 국외이나 또는 국내에서 이루어지느라에 달라졌다. 국경 간 송금은 이름, 계좌번호(또는 계좌가 없을 경우 고유참조번호, 1회성 송금)와 주소가 수반되어야 한다. 수신송금 번호 또는 생년월일과 출생지는 고객 주소가 노출될 위험이 있는 경우 주소를 대체할 수 있다. 전신송금 시에 이 정보를 제공하는 것은 국제적인 자금세탁이나 테러자금조달 관련 수사가 있는 경우 정부기관의 조회보다는 훨씬 신속하고 쉽게 송금자에 대한 정보를 취득할 수 있게 해 줄 것이다.

송금기관이 수취기관이나 해당기관에서 요청을 받고 3일 이내에 조사에 대한 나머지 정보를 추적할 수 있는 경우 국내송금은 단지 계좌번호만이 수반된다. 국가들은 3천여로/달러까지의 거래에 대해 이와 같은 요구사항을 면제해 줄 수 있다.

수취기관은 유의미한 정보를 보여주지 않는 전신송금을 식별할 수 있어야 한다. 이것은 모든 거래를 조사하라는 요구사항은 아닐고, 수취기관이 그 정보의 정확성을 조사할 수 있도록 할 가능성이 매우 낮다. 자금이체를 의뢰한 송금자는 수취운행의 고객이 아니다. 그러나 수취기관은 전신송금 중 몇몇을 추출하여 조사하는 체계를 수립해야 한다. 수취기관은 정보가 부족한 경우 형의거래보고 제출을 검토해야 한다. 금융기관이 요구하는 송금자 정보를 포함하지 않는 메시지를 보내는 경우 수취기관은 그 송금자와의 거래관계를 재검토해야 한다.

H. 비영리기관(Non-Profit Organizations)

특별권고사항 VIII에 따르면 각 국가는 비영리기관이 테러자금조달 목적으로 이용될 수 있는지를 판단하기 위해 이 기관에 대한 법과 규정의 적절성을 검토해야 한다. 특히 국가는 비영리기관이 다음에 악용되지 않도록 보장해야 한다.

64. Id, paragraph 1.
65. Id, paragraph 8 and 9.
67. Id, paragraph 11-14.
68. (특별 권고사항) Special Recommendations, Spec. Rec. VIII.
제9장 테러자금조달 대응 163

- 합법적인 조직으로 가정한 테러조직에 의한 악용
- 자산동결조치를 피하는 것을 포함하여 테러자금조달의 경로로써 합법적인 단체를 부당하게 이용
- 합법적인 목적의 자금을 테러조직으로 운반하게 전환하는 것을 은닉하거나 덮는 것에 이용(69)

이 권고사항에 대한 해설서는 없으나 비영리기관이 악용되는 것에서 보호하는데 있어 국가들에 돕기 위한 노력의 일환으로 FATF는 “비영리기관의 악용 퇴치”라는 제목의 국제우수사례집을 발간했다.70)

이 권고사항의 목적은 다른 합법적인 단체뿐 아니라 비영리기관(예: 자선단체, 종교단체, 교육단체, 사회 또는 우예단체)이 테러리스트에 의해 악용되는 것을 방지하는 것이다.71) 이러한 점에서 이 권고사항은 다소 일반적인데 이는 비영리기관의 범위에 해당하는 각기 다른 단체들이 다양한 법적 형태를 지니고, 단체의 성격이 국가마다 다르기 때문이다.72)

특정 국가에서는 거의 또는 아예 효력이 없는 엄격한 규칙의 준수를 요구하지 않으려는 노력에서 이 권고사항은 특정한 요구사항보다는 달성되어야 할 일반적인 지침과 목적으로 구성된다. 이 권고사항 하에서 국가들이 관심을 둘고 되어야 할 분야는 다음의 3가지이다.

- 금융투명성 확보. 비영리기관은 투명한 금융거래기록을 보유하고 감사를 받을 수 있고, 자금이 해명될 수 있는 방식으로 운영되어야 한다. 재무제표는 공개되어야 하고, 자금은 제도권 은행에 개설된 계좌에서 사용되어야 한다.
- 프로그램 검증. 비영리기관은 자금 수취인이 누구인지와 수취인이 자금을 어떻게 쓰는지를 알아야 하고, 이것을 모니터링하는 적극적인 조치를 취해야 한다. 이것은 특히 수취인이 외국에 있는 경우 중요하다.
- 행정. 비영리기관의 운영에 관해 보관된 만족할 만한 수준의 기록이 있어야 하고, 명확한 지배구조와 내부 책임이 존재해야 한다.

69. Id.
71. FATF, 지침서 Paragraph 39,
72. Id.
I. 현금반출업(Cash Couriers)

2004년 10월에 채택된 이 권고사항의 목적은 테러리스트와 기타 범죄자들이 금전을 한 국가에서 다른 국가로 운송하여 범죄수익을 세탁하거나 테러활동의 자금을 조달할 수 없도록 보장하는 것이다.73) 국경 간에 현금과 현금에 상응하는 것을 휴대한 개인이나 단체는 종종 “현금반출업”으로 알려진다.

특별권고사항 IX에는 현금반출업의 활동과 관련하여 4가지의 요건이 명시되어 있다. 첫째 각 국가는 금전과 소지인식유가증권(Bearer negotiable instrument : BNI)의 국경 간 운송을 석발하는 시스템을 수립해야 한다.74) 둘째 각 국가는 해당기관에 (i) 테러자금조달이나 자금세탁에 연관된 것으로 의심되는 또는 (ii) 신고나 공개 요구에서 잘못 전달된 금전과 BNI를 지출하거나 제출할 수 있는 법적인 권한을 제공해야 한다. 셋째 각 국가는 금전과 BNI의 국경 간 이송에 관한 위의신고를 하거나 공개를 한 자에 대해 효과적이고, 빠르며 적절하게 처리하는 제재조치를 수립해야 한다고 요구한다. 마지막으로 각 국가는 테러자금조달이나 자금세탁에 연관된 금전과 BNI를 불수할 수 있는 조치를 체택해야 한다.

FATF는 이 권고사항을 채택함과 동시에 이것에 수반되는 공식적인 해설서를 채택했다.75) 해설서에는 한 국가가 이 권고사항의 요건을 이행하는 방법에 대한 종합적인 기술 및 권고사항에서 요구되는 용어에 대한 종합적인 정의가 명시되어 있다. FATF는 또한 “테러리스트와 기타 범죄자들에 의한 국경 간 현금 운송 석발 및 방지”라는 제목의 국제우수사례집을 채택했다.76) 각 국가는 특별권고사항 IX의 요건을 이행하는 방법에 관해 2005년 2월 채택된 우수사례집을 참조할 수 있다. 해설서에 따르면 “소지인식유가증권(BNI)”은 다음을 뜻한다.

▶ 이행사수요와 같은 소지인식 형태의 금전 수단
▶ 가공의 지급 받을 자에게 승인된 소지인식 형태의 유가증권 또는 인도와 동시에 권리가 이양되는 형태의 유가증권
▶ 시명은 되어 있으나 지급 받을 자의 이름이 명기되지 않은 분명한 증권 (수표, 약속채용, 유효환 포함)77)

73. 특별권고사항 IX에 대한 해설서, Paragraph 1.
74. (특별 권고사항) Special Recommendations, Spec. Rec. IX.
75. 특별권고사항 IX에 대한 해설서
본 권고사항의 목적을 위해서는 금, 귀금속이 "소지인식유가증권"이라는 용어의 의미에서 제외되어야 한다는 사실에 주목해야 한다. 이와 같은 풀목에 대한 공개, 신고 또는 기타 형태의 표시는 관세법이나 규정과 같은 국가의 법적 요구에 포함될 수 있으나 본 권고사항을 준수하기 위해 그것들을 포함하는 것이 필요하지는 않다. 이와 같은 "물리적인 국경 간 운송"은 금전이나 소지인식 유가증권을 한 국가에서 다른 국가로 반입·반출하여 물리적으로 운송하는 것을 뜻한다. 여기에는 (i) 자수인에 의한 또는 그 자수인의 점이나 자동차에 실어 (ii) 간데이터 화물로 선적하여 또는 (iii) 자수인이나 법인이 우편으로 하는 물리적 운송이 포함된다.

해설서에 따르면 국가는 두 개의 시스템(신고(declaration) 또는 공개(disclosure) 중의 하나를 이용하여 적발 조치를 수립해서 본 권고사항의 요건을 충족할 수 있다. "신고제도"에 따르면 명시된 기준 금액(최대치가 15,000 유로/달러를 넘지 않음)이나 그 이상의 금전이나 소지인식 유가증권을 물리적으로 국경 간에 운송하는 자는 지정된 해당기관에 이체금액과 기타 관련 정보에 대해 진실한 신고서를 제출하도록 요구된다. 이는 정해진 기준금액은 권고사항의 목표를 충족하기에 충분히 낮게 책정되어야 한다.

"공개제도"에 따르면 금전이나 소지인식 유가증권을 물리적으로 국경 간에 운송하는 자는 요청 시 지정된 해당기관에 이체금액과 기타 관련 정보에 대해 진실하게 공개하도록 요구된다. 이와 같은 절에서 국가는 해당기관이 적법 또는 의심에 따라 혹은 그의 요청을 할 수 있도록 보장해야 한다.

국가가 반입·반출하는 운송에 대해 적발시스템을 갖춰야 할 필요는 있으나 반입·반출 운송에 대해 동일한 유형의 시스템을 이용할 필요는 없다는 것에 주의하는 것이 중요하다.

77. 특별권고사항 IX에 대한 해설서 Paragraph 3.
78. Id., 각주 1.
79. Id.
80. Id., Paragraph 5.
81. Id., Paragraph 9.
82. Id., Paragraph 9a.
83. Id., Paragraph 9b.
84. Id., Paragraphs 9, 10a.
예를 들면 반입되는 운송 건에 대해서는 신고 제도를, 반출되는 운송 건에 대해서는 공개제도를 가질 수 있고, 그 반대로 가능하다.

허위신고나 공개는 다음을 뜻하는 것으로 규정된다.

- 운송된 금전이나 소지인식유가증권의 금액 허위 진술
- 신고 또는 공개 요구 사례 또는 해당기관에서 다른 방법으로 요청을 받은 관련 자료의 허위 제출, 또는
- 요구에 따라 신고하거나 공개하지 못함

허위신고나 허위공개를 발견하는 경우 지정해당기관에게 대상이 되는 금전이나 소지인식유가증권의 출처와 금전과 소지인식유가증권의 사용 용도에 대해 개인에게서 추가정보를 요청하여 취득할 수 있는 법적 권한이 있어야 한다.

어느 제도를 이용하건 신고 그리고/또는 공개 과정을 통해 취득된 정보는 ITU에서 이용할 수 있어야한다. 또한 신고 그리고/또는 공개 과정에서는 40개 전고시항, 특히 35-40까지와 특별전고사항 V에 따라 가능한 가정 점보의 국제협력과 지원이 허용되어야 한다. 이러한 점에서 최대 기준금액을 넘은 것에 대한 신고와 공개가 이루어지는 경우, 허위 신고나 공개가 발견되는 경우, 또는 자금세탁이나 테러자금조달 협의가 있는 경우 신고, 공개 또는 발견된 금전 또는 소지인식 유가증권 금액과 개인의 신원자료를 포함한 관련 정보가 보유되어야 한다.

테러자금조달이나 자금세탁과 실제로 관련된 금전이나 소지인식 유가증권을 물리적으로 운송하는 자와 관련하여 그 금전이나 소지인식 유가증권은 물수를 허용하는 40개 전고사항(전고사항 3)과 특별전고사항 III과 일관된 조치(법적인 조치 포함)의 대상이 되어야 한다. 조치 대상으로 결정되기 전에 (i) 테러자금 조달이나 자금세탁 협의 또는 (ii) 허위 신고 또는 공개가 있는 경우에 해당기관은 테러자금조달의 증거가 존재하는지 여부를 결정할 협력적인 시간을 통해 대상 금전 그리고/또는 소지인식 유가증권을 중지하거나 제한할 법적인 권리를 가지야 한다.

85. Id, Paragraphs 6, 7.
86. Id, Paragraph 10b.
87. Id, Paragraph 10c.
88. Id, Paragraph 10f.
89. Id.
90. (특별 권고사항) Special Recommendation IX 그리고 특별권고사항 IX에 대한 해설서 Paragraph 11.
91. 특별권고사항 IX에 대한 해설서 Paragraph 10e.
마지막으로 국가들은 수령된 정보의 적절한 사용을 보장하는 보안조치에 따라 그리고 국가 사이에 상품과 서비스에 대한 무역대금지불과 자본 이동의 자유를 어떠한 방식으로든 제한하지 않고 특별권고사항 IX를 이행하도록 권고한다.32)

J. 테러자금조달에 관한 자가 평가 질문서(Self-Assessment Questionnaire)

FATF는 특별권고사항과 관련한 해석과 이행 사안을 중점적으로 다루기 위해 테러자금조달에 관한 자가 평가 질문서(Self-Assessment Questionnaire:SAQFT)를 발행했다.33) 이 질문서는 원래 FATF 회원국들만이 이용했다. SAQFT가 처음에 완결되었을 때 FATF는 특별권고사항에 대한 지침서와 SAQFT를 발행했다. SAQFT는 FATF 웹사이트 상에서 이용가능하며 자가 평가 목적으로 어느 나라라도 이용할 수 있다.34)

---
32. 특별권고사항 IX에 대한 해설서 Paragraph 10e.
34. Id.
3편: 국제통화기금과 세계은행의 역할

10장: 국제통화기금과 세계은행의 자금세탁과 테러자금에 대한 이니셔티브
제10장 : 자금세탁과 테러자금조달 척결을 위한 세계은행과 IMF의 이니셔티브

A. 인식제고
B. 공동의 AML/CFT 평가방법 개발
C. 제도적 역량 개발
D. 연구 및 분석
제10장 자금세탁과 테러자금조달 쇠퇴를 위한 세계은행과 IMF의 이니셔티브

<table>
<thead>
<tr>
<th>A. 인식재고</th>
<th>C. 제도적 역량 개발</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 국제마감</td>
<td>1. 교육 컨퍼런스 조직</td>
</tr>
<tr>
<td>2. 국가 지원 전략</td>
<td>2. 개별 국가에 대한 기술 지원</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. 공동의 AML/CFT 평가방법 개발</th>
<th>D. 연구 및 분석</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 12개월 에비(PIot) 프로그램</td>
<td>1. 하와라 분석</td>
</tr>
<tr>
<td>2. 기준 및 법 준수에 관한 보고</td>
<td>2. 대체송금제도 연구</td>
</tr>
<tr>
<td>3. 공동 방법의 수정</td>
<td>3. 세계은행의 AML/CFT 웹사이트</td>
</tr>
<tr>
<td></td>
<td>4. 참고 안내시</td>
</tr>
</tbody>
</table>

세계은행과 IMF의 역할(missions)은 근본적으로 다르다. 그러나 두 기관은 자금 세탁방지와 테러자금조달 쇠퇴에 대하여 동일한 목표가 있다. 또한 그 목표를 이루기 위하여 전 분야에 걸쳐 협력하고 있다.

세계은행의 기본적인 역할은 전 세계의 비용을 퇴치하는 것이다. 세계은행은 국가에 기반구조 개선과 개발도상국의 환경을 위한 대출 외에도 제도적 역량 개발을 위한 대출 및 기술 지원을 제공하여 개발 노력을 돕는다. 세계은행의 임무(mission)에는 공공 및 민간부문에서 자원 재분, 지식 공유, 협력관계 구축이 포함된다.1)

IMF의 역할은 본질적으로 경제적이고, 전 세계의 금융안정성을 감독하는 것이다. IMF의 목표에는 다음과이 포함된다.

- 국제금융 협력 증진

---

국제무역의 확대와 균형 잡힌 성장 촉진
외환안정 조정
다사간 지불시스템 구축 지원

이기에 추가로 IMF는 국가들이 국내 및 국제 경기 호황에 악영향을 주는 조치에 의존하지 않고 국제수지의 불균형을 개선할 수 있도록 대출을 하여 국제금융안정을 촉진한다.2)

2001년 4월 세계은행과 IMF의 이사회는 자금세탁이 주요 금융시장과 소규모 금융 시장에 영향을 미치는 국제적인 문제가 되고 있다는 것을 인식했다.3) 세계은행은 자금세탁이 국내경제 개발 및 안정된 금융기관 구축 단계에 있는 국가에 대한 경제적, 정치적, 사회적으로 파괴적인 영향력을 감안하면 자금세탁이 개발도상국에 막대한 비용을 초래할 수 있다는 것을 인식했다. IMF는 자금세탁이 예측되지 않은 국경 간 자금이체로 인해 자금수요의 예측이 불가능한 변화, 금융기관과 금융시스템의 건전성에 위험 그리고 국제자본흐름과 환율 변동성 증대를 포함하며 폭넓은 거시 경제적 영향을 초래할 수 있다는 것을 인식했다.


에비 프로그램 과정에서 IMF와 세계은행은 33개국에서 평가를 실시했고, FATF와 그리고 FATF 스타일 지역기구(FSRBs)는 추가로 8개국에서 평가를 실시했다. IMF와 세계은행의 이사회는 2004년 3월 에비 프로그램의 결과를 검토했다. 이사회는 에비 프로그램이 성공적이었다고 결론을 내렸고, AML/CFT에 대한 증가하는 국제적 관심과 FATF와 FATF 스타일 지역기구의 협력을 향상했다. 그 시기에 이사회는 FATF와의 협력을 지속하고, 개정된 FATF 권고사항을 기준 및 법규 준수에 관한

보고서(ROSCa) 준비와 그 기준을 평가하는 개정된 방법론에 대한 새로운 기준으로 승인하며, 차후에 이 업무에 추가로 자원을 제공하기 위해 AML/CFT 업무를 영구적인 이사회 활동의 일환으로 만들기로 결정했다. IMF와 세계은행은 FATF와 FSRBs가 이용하는 동일한 방법론으로 약 20년의 평가를 실시한 예정이다.

A. 인식제고

1. 한 국가의 자금세탁방지와 테러자금조달 대응을 위한 제도적인 기반 구축이나 개선의 첫 번째 단계는 지도층의 인식제고, 국가 미래와의 관련성 중명, 타국가와의 경험 공유, 이용 가능한 자원 및 지원에 대해 알리주는 것이다. 이 목표를 향해 세계은행과 IMF는 AML/CFT 관련 지역방침에 대한 국제대화(Regional Policy Global Dialogues on AML/CFT)를 창설했다. 이 대화는 생명형 비디오 콘퍼런스를 이용해서 회원국들에 의해 회원국의 정부 관료들, 세계은행과 IMF의 직원, FATF 스타일 지역기구, 지역개발은행과 기타 국제기구들이 논의하고 정보를 교환할 수 있도록 지역 내에서 개최된다.

- 불법자금호흡에 대한 대응 시에 국가들이 직면하는 어려움과 악
- 상호 사례 공유
- 지역 내 국가들의 특성화 문제점과 악
- 자금세탁과 테러자금조달 척결에 필요한 지원의 종류 이해

국제대화(Global Dialogue Series)에서 대우되는 몇몇 중요한 질문사항은 다음과 같다.

- 세계은행과 IMF는 국가들이 자금세탁과 테러자금조달에 대한 대응을 강화할 도록 어떤 도움을 줄 수 있는가?
- 자금세탁과 테러자금조달은 부패와 연결한 기업지배구조라는 보다 넓은 범주에 어떻게 포함되는가?
- 국가의 대응은 무엇이었는가?
- 규제기관이 직면한 최근의 난관은 무엇인가?
- 자금세탁과 테러자금조달 척결을 위한 효과적인 프로그램 이행 시에 각 국가에게 적절한 제도적 체계는 무엇인가?
- 자금세탁과 테러자금조달 척결에 있어 참가국들이 당면한 미래의 난관은 무엇인가?
참가국의 고위 정책임자들은 위의 질문에 대답하기 위하여 범죄자들의 금융
시스템은, 특히 자금세탁과 테러자금조달의 경제적 비용에 관한 그들의 관심을
제시한다. 기타 논의점은 이와 같은 위협에 적합하여 지속적인 경제개발과 금융
시장 건전성을 위한 질적적 수단이 있었다. 이 다재는 국가들이 고유의 경험과
국제 전문가들의 폭넓은 경험이 따라 각자 배우는 것으로 도움을 준다.

2. 국가 지원 전략

세계은행 금융부문평가 프로그램(Financial Sector Assessment Program
FSAP)의 결과를 국가지원전략(Country Assistance Strategy: CAS)에서 검토되는
보다 넓은 범위의 개발 조치를 통합하고 있는데, 국가지원전략에는 국가의 정부와
협의하여 3년 단위로 세계은행의 FSAP에 대한 우선순위가 규정되어 있다. FSAP의
조사결과에 대한 체계적인 검토 후 2002년 3월부터 30건 이상의 국가지원전략에
AML/CFT 지원이 이미 포함되었다. AML/CFT 제도의 취약성이 중대한 지배구조
및 개발 위협을 초래할 수 있는 국가에서 기술 지원은 우선순위가 된다. 국가지원
전략은 또한 국제기준과 우수사례를 흉추하지 못하는 국가에서 보다 면밀하게
AML/CFT 관련 문제들을 대응하고 있다.

IMF는 AML/CFT 요소를 제4조 감독에 통합 적용했다.4 이사회에 대한 금융제도
안정성 평가(Financial System Stability Assessment: FSSA) 보고에 추가해, AML/CFT
결의서에서 나타난 결과는 2002년 1월 이후 제 4조에 관한 70자례의
논의에서 적용되었다.

B. 공동의 AML/CFT 평가방법 개발

세계은행과 IMF는 2002년에 FATF와 기타 국제기준제정기구, 즉 바젤위원회,
국제증권감독위원회, 국제보화감독자연합, 에코그룹들과 긴밀히 협력하여 하나의
융합적인 AML/CFT 평가방법론을 구축했다. 이 방법론은 2002년 10월 총회에서
FATF가 동의하고 승인했다. 이 방법론은 평가 법집행 이행을 포함하여 FATF의
40개 권고사항과 특별권고사항 각각을 포함하는 120개의 기준으로 구성되어 있다.5

여기에는 HU의 설립을 포함하여 국가의 법적 및 제도적인 AML/CFT 기반이 포함되었다. 또한 관련 유엔안보리의안과 국제협약 및 기타 국제기구기구의 조치가 포함되었다. 금융기관을 위한 예방조치에 대한 상세한 평가도 규정되어 있다.


평가방법론은 국제기구가 금융보문평가프로그램과 OFC 과정에서 한 나라의 국제 금융기준 이행 정도에 대한 전반적인 평가의 일부로서 수행되는 AML/CFT에 대한 평가방법론이 이행할 때 이용될 것이다. 이 평가에서는 AML/CFT에 대한 기준 및 법규 준수에 관한 보고서(ROSCs)가 나올 것입니다. 이것은 세계은행과 IMF의 이사회에 보고될 것이다. 평가방법론은 또한 FATF와 FSRBs가 상호평가를 할 시에도 이용될 것이다. FATF와 FSRBs는 기준 및 법규 준수에 관한 보고서(ROSCs)를 상호평가의 일부로 준비할 것이고 이것은 세계은행과 IMF에서 승인한 것이었다.

FATF, FSRBs, 세계은행과 IMF 각각이 동일한 방법론을 이용하여 평가를 수행하고, 각자의 보고서를 인정하기로 합의하는 과정은 하나이다. 이 기구들은 합의하여 평가 일정에 따라 이 일정은 국제금융기구의 FASP/OFC일정과 FATF/FSRB의 상호평가 일정과도 일치된다. IMF와 세계은행은 대략 연간 20건의 평가를 수행하고, FATF와 FSRBs는 대략 20건의 평가를 수행할 것으로 예상된다. 이 일정은 모든 국가가 대략 5년에 한 번 종합평가를 받을 수 있도록 해야 한다.

C. 제도적 역량 개발

1. 교육 컨퍼런스 조직

세계은행과 IMF는 특정 지역의 AML/CFT와 관련된 공무원을 활용하여 특정
AML/CFT 인건에 대해 교육 컨퍼런스를 개최한다. 예를 들어 2002년 동안 2번째 기술지원컨퍼런스가 개최되었는데, 한반본 우루과이의 리버데로, 다른 한반본 러시아의 모스크바에서였다.

모스크바 컨퍼런스는 제시된 정보의 유형에 관해 설명하는 것이었다. 컨퍼런스는 FIU의 설립에 초점을 맞추었다. 이 컨퍼런스는 운영 중인 FIU의 주석 역할과 운영을 시작한 국가에 중점을 두었다. 이것의 주요 목적은 최근 AML/CFT 이행 기준을 충족한 동유럽 국가 출신의 전문가를 참여시키고, 동유럽 국가 출신의 공무원들이 경험과 우수사례를 발표하도록 하는 것이었다.

이 컨퍼런스는 또한 AML/CFT에 관한 기술적 지원을 제공하는 국가와 기구가 가장 긴급한 요구가 필요한 곳을 이해하도록 돕고, 필요한 나라의 정부 관리들에게 접촉해 자주의 지원이 보다 쉽게 제공되도록 하는데 유용한 도구였다.

이 컨퍼런스는 AML/CFT 사안에 대한 관심의 중요성을 중명하고, 참가국의 공무원이 이해할 수 있는 방식으로 국제기준의 다양한 요구사항들이 발표되었다는 점에서 성공적이었다. 이것은 또한 각 국가에서 조치를 시작하는데 필요한 구체적인 단계를 보여주었다. 이 외에도 정부 관리들은 이웃 국가의 상대기준과 달라 그 분야의 전문가에게 개별적으로 접촉할 수 있게 되어 AML/CFT 이행 시에 조언과 지원을 구하는 것이 더 부담스럽게 되었다.

2004년 5월 남아프리카에서 동남부 아프리카 자금세탁그룹(ESAAMLG)의 14개 회원국이 참여하며 추가 위크숍이 개최되었다. 이 위크숍은 세계은행과 IMF의 참여와 함께 ESAAMLG에서 준비했고, 몇몇 국제기구와 외국의 전문가가 참여했다. 위크숍의 목적은 ESAAMLG의 정책업무자들이 자금세탁과 대리자금조달에 대응하는 국내 전략의 기본적 요소에 대해 알리고, 각 국가에서 주요 AML/CFT 문제를 해결하기 위한 전략을 개발하도록 협력하는 것이다. 참가자들은 회의에서 협력하여 2004년 8월 ESAAMLG 총회에서 최종적으로 결정되어 발표되기 전에 국가에서 추가로 개발된 예정이었던 전략을 만들었다.

2. 개별 국가에 대한 기술 지원

세계은행과 IMF는 AML/CFT 제도를 구축하거나 개선하고자 하는 국가에 다양
한 형태의 기술지원을 제공하고 있다. 2001년 4월 이후로 이러한 기술지원은 증가하였으며, 세계은행과 IMF는 금융부문평가프로그램(FSAPs)의 결과와 독립적인 AML/CFT 검토를 기술지원이 필요한 곳을 결정하고 기술지원의 우선순위를 매기는 수단으로 이용한다.

개발도상국의 경우 AML/CFT 관련 기술지원은 국가의 CAS(국가지원전략)에 포함되는데 여기에는 국가의 정부와 협의하여 3년을 기준으로 하는 세계은행의 지원 프로그램의 우선순위가 명시되어 있다. 특히 AML/CFT 제도의 취약성은 중대한 지배구조 및 개발 위험을 초래할 수 있는 국가에서 기술 지원은 우선순위가 된다.

AML/CFT에 대한 세계은행과 IMF의 기술지원은 다음에 중점을 두고 제공한다.

- 국제우수사례를 중복하는 AML/CFT 법과 규정 제정
- 금융부문 감독기관과 AML/CFT 조치의 집행을 담당하는 기타 유사한 해당기관의 법, 규정, 방침 및 절차의 이행
- 국제우수사례를 중복하는 FIU의 법적기반 구축
- 공공 및 민간 부문에서 AML/CFT 관련 우려에 대응하기 위한 교육 및 인식 프로그램 개발
- 다국적 교육훈련 프로그램에서 타국과 협조 및 컴퓨터 기반 교육자료 개발

세계은행과 IMF의 이사회가 AML/CFT를 이들 기관의 활동의 영구적인 업무로 만드는 2004년 3월 결정에 의한 2년이라는 기간 동안 세계은행과 IMF는 63개 국을 아우르는 85건의 국가별 기술지원 프로젝트와 130개국이 포함된 32건의 지역 프로젝트를 수행했다.

D. 연구 및 분석

1. 하위라 분석

세계은행과 IMF는 흔히 "하위라"로 불리는 비공식적인 자금송금제도(informal

funds transfer systems: IFTs)의 운영 특징을 연구했다. 이 연구에서는 하랄라가 발전해온 역사적, 사회경제적 맥락을 조사한다. 이러한 점에서 하랄라는 상업적 전통적인 운영 수단이 취약하거나 부재했을 당시에 원거리 간에 활발했던 무역에서 그 뿌리를 찾는다.

이 연구는 또한 합법적 그리고 불법적인 목적에 대해 비공식적인 자금송금제도의 운영상의 특징을 분석한다. 이 운영상의 특징은 주로 속도, 낮은 거래비용, 인종적, 문화적 편의성과 익숙함, 다양성과 장점적인 익명성이다. 또한 비공식적인 자금송
금제도는 금융기관이 비효율적이고, 금융정책이 제한적인 국가에서 반영해왔다. 마
지막으로 다른 어느 지하경제활동과 마찬가지로, 비공식적인 자금송금제도는 통화
관리, 환율에 영향을 주는 것, 경제 데이터 왜곡(따라서 통계정보는 정책입안자가
이용 가능함), 수입세와 서비스에 대한 세금 축소와 밀접한 관련이 있다.

이 연구는 이러한 활동에 대한 규제 및 감독 대응의 관련성을 논의한다. FATF
특별취재요구에의 금융기관 VI는 국가가 금융기관과 동일한 AML/CFT 요건에 따라
하랄라와 기타 비공식적인 자금송금제도를 제도권의 일부로 취급하기를 권고한다. 
보다 많은 국가들이 하랄라와같은 단체들이 FATF의 권고사항에 따라 허가를 받거나
등록을 하도록 하고 있다.

2. 대체송금제도(Alternative Remittance System) 연구

2002년 9월 APEC 대무장관들은 APEC 회원국에서 대체송금제도의 이용을 장려
하는 경제, 구조 및 규제 요소를 조사하기 위해 대체송금제도 관련 실무그룹을
구성했다. 이 프로젝트에 대한 지원으로 세계은행은 송금요금의 규모를 측정하는
기반을 마련하고, 공식적인 채널 대 비공식적인 채널에 대한 동기를 분석하며, 
국제 AML/CFT 기준을 준수하는 송금 서비스의 제공 시에 제도권 금융부문의
역할을 조사하는 보고서를 준비했다.

APEC의 대체송금제도에 후속조치의 일환으로 그리고 세계은행의 모든 고객을
위해 대체송금제도라는 중요한 주제를 연구하는데 있어 세계은행의 참여를 확대하려는
노력의 일환으로, 특정 국가에 대한 사례비교연구가 준비되었다. 연구 결과들과 사례

연구의 결론은 의견과 경험 교환을 위해 공유될 것이다. 이것은 지속적인 프로젝트로써 각기 다른 연구의 결과들은 보고되고, 세계은행의 AML/CFT 웹사이트에 게재될 것이다.

3. 세계은행 AML/CFT 웹사이트

세계은행은 특히 AML/CFT 용도로 웹사이트를 운영한다. 이 웹사이트는 자금 세탁과 테러자금조달 척결을 위한 세계은행의 프로그램과 노력들에 대한 최신 정보가 담겨있다. 여기에서 또한 본 안내서와 같은 참고자료와 출판물을 열람할 수 있다. 이 웹사이트의 주소는 www.amlcft.org이다. AML/CFT와 관련하여 세계은행에 연락 하고자 하는 사람은 aml@worldbank.org로 이메일을 보내야 한다.

4. FIU 헌드북

IMF와 세계은행은 2004년 FIU의 설립과 운영의 모든 측면에 관한 헌드북을 출간했다. 이 헌드북의 제목은 "FIU 총람"이다.11)

이 헌드북에서는 다음을 포함하여 FIU와 관련된 주제가 다루어진다.

- FIU 설립의 주요 단계
- 운영을 위한 기본 모델
- 핵심 기능
- 추가 기능
- 국제평가

5. 참고 안내서

AML/CFT에 관한 본 안내서는 자금세탁과 테러자금조달 척결을 위한 세계은행과 IMF의 노력의 산물이다. 정책입안자들이 국가, 특히 이 분야에 한정된 경험이 가진 개발도상국이 이용할 수 있는 AML/CFT 자료를 본 후 모든 문제의 대응에 이용

11. 헌드북은 IMF에서 구매 가능함. 세계은행의 AML/CFT 웹사이트에서 볼 수 있음(임기전용).
될 수 있는 단일한 출처가 없다는 것이 명백해졌다. 따라서 세계은행과 IMF는 본 안내서를 단일하지만 종합적인 출처에서 모든 관련 정보를 이용할 수 있는 수단으로써 만들었다.


안내서는 세계은행의 웹사이트 http://www.amlcft.org에서 볼 수 있고, 다른 언어로도 번역될 예정이다.

영문원판
Reference Guide to
Anti-Money Laundering and
Combating the Financing of Terrorism

Second Edition
and Supplement on
Special Recommendation IX

Paul Allan Schott
Reference Guide to
Anti-Money Laundering and
Combating the Financing of Terrorism

Second Edition
and Supplement on
Special Recommendation IX
Reference Guide to
Anti-Money Laundering and
Combating the Financing of Terrorism

Second Edition
and Supplement on
Special Recommendation IX
Contents

Foreword ix
Acknowledgments xi
Abbreviations and Acronyms xiii
Introduction: How to Use this Reference Guide xv

Part A: The Problem and the International Response

Chapter I: Money Laundering and Terrorist Financing: Definitions and Explanations I-1
B. What Is Terrorist Financing? I-4
C. The Link Between Money Laundering and Terrorist Financing I-5
D. The Magnitude of the Problem I-6
E. The Processes I-7
F. Where Do Money Laundering and Terrorist Financing Occur? I-9
G. Methods and Typologies I-9

Chapter II: Money Laundering Impacts Development II-1
A. The Adverse Implications for Developing Countries II-2
B. The Benefits of an Effective AML/CFT Framework II-7

Chapter III: International Standard Setters III-1
A. The United Nations III-2
C. The Basel Committee on Banking Supervision III-13
D. International Association of Insurance Supervisors III-16
Chapter IV: Regional Bodies and Relevant Groups

A. FATF-Style Regional Bodies
B. Wolfsberg Group of Banks
C. The Commonwealth Secretariat
D. Organization of American States—CICAD

Part B: The Elements of an Effective AML/CFT Framework

Chapter V: Legal System Requirements

A. Criminalization of Money Laundering
B. Criminalization of Terrorism and the Financing of Terrorism
C. Seizure, Confiscation, and Forfeiture
D. Types of Covered Entities and Persons
E. Supervision and Regulation—Integrity Standards
F. Laws Consistent with Implementation of FATF Recommendations
G. Cooperation Among Competent Authorities
H. Investigations

Chapter VI: Preventive Measures

A. Customer Identification and Due Diligence
B. Record Keeping Requirements
C. Suspicious Transaction Reporting
D. Cash Transaction Reporting
E. Balancing Privacy Laws with Reporting and Disclosure Requirements
F. Internal Controls, Compliance and Audit
G. Regulation and Supervision—Integrity Standards
H. Legal Entities and Arrangements

Chapter VII: The Financial Intelligence Unit

A. Definition of a Financial Intelligence Unit
B. Core Functions
C. Types or Models of FIUs
D. Possible Additional Functions
E. Organizing the FIU
## Annexes

I. Websites for Key Organizations, Legal Instruments, and Initiatives  
   [Annex I-1](#)

II. Other Useful Websites and Resources  
    [Annex II-1](#)

III. United Nations Anti-Terrorist Conventions Referred to in the International Convention for the Suppression of the Financing of Terrorism  
     [Annex III-1](#)

IV. The Financial Action Task Force Forty Recommendations on Money Laundering and Interpretative Notes  
    [Annex IV-1](#)

V. The Financial Action Task Force Special Recommendations on Terrorist Financing  
   [Annex V-1](#)

VI. The Financial Action Task Force Interpretative Notes and Guidance Notes for the Special Recommendations on Terrorist Financing and the Self-Assessment Questionnaire  
     [Annex VI-1](#)

VII. Cross-Reference of The Forty Recommendations to Reference Guide  
     [Annex VII-1](#)

VIII. Cross-Reference of the Special Recommendations to Reference Guide  
      [Annex VIII-1](#)

## Diagrams

The Processes of Money Laundering and Financing of Terrorism  
[Annex I-8](#)
Foreword

Efforts to launder money and finance terrorism have been evolving rapidly in recent years in response to heightened countermeasures. The international community has witnessed the use of increasingly sophisticated methods to move illicit funds through financial systems across the globe and has acknowledged the need for improved multilateral cooperation to fight these criminal activities.

The World Bank and International Monetary Fund developed this second edition of the Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism to help countries understand the new international standards. The Reference Guide will hopefully serve as a single, comprehensive source of practical information for countries to fight money laundering and terrorist financing. It discusses the problems caused by these crimes, the specific actions countries need to take to address them and the role international organizations, such as the Bank and the Fund, play in the process.

We offer this new version as a tool for countries to establish and improve their legal and institutional frameworks and their preventive measures according to the new international standards and best practices. This Second Edition of the Reference Guide and Supplement on Special Recommendation IX will also be translated into Arabic, Chinese, French, Portuguese, Russian, and Spanish in order to better serve a broader audience.

We intend to keep the Reference Guide under review as money laundering and terrorist financing trends and techniques, as well as the international response, evolve and to update it as necessary. We welcome your feedback and recommendations on how this resource can be more useful.

Margery Waxman  
Program Director and Senior Adviser  
Financial Market Integrity  
World Bank

R. Barry Johnston  
Assistant Director  
Monetary and Financial Systems Department  
International Monetary Fund

Jean-François Thony  
Assistant General Counsel  
Legal Department  
International Monetary Fund
Acknowledgments

This publication was written by Paul Allan Schott, consultant with the Financial Market Integrity Unit of the Financial Sector of The World Bank. The author is especially grateful to Margery Waxman, Director, Financial Market Integrity, World Bank, for her support, encouragement and patience in producing the first and second edition of this Reference Guide.

The author is grateful to his Bank and Fund colleagues for their willingness to read multiple drafts of the first edition and provide advice and insights based on their work in the development and implementation of the joint Bank/Fund program to combat money laundering and terrorist financing: John Abbott, Maud Julie Bokkerink, Pierre-Laurent Chatain, Alain Damais, Ross Delston, Gabriella Ferencz, Ted Greenberg, Raul Hernandez Coss, Barry Johnston, Nadim Kyriakos-Saad, Samuel Maimbo, John McDowell, Bess Michael, Michael Moore, Pramita Moni Sengupta, Takashi Miyahara, Thomas Rose, Heba Shams, Jean-François Thony, and Cari Votava.

Most importantly, the author wishes to thank Joseph Halligan for his work in updating the Reference Guide to reflect the revision of the FATF 40 Recommendations and the methodology. Finally, the author could not have produced this comprehensive second edition without the work of Bank staff members who helped organize the material carefully, checked all references and made this publication a reality: Oriana Bolvaran, Nicolas de la Riva, Martín Joseffson, Amanda Larson, Annika Lindgren, Maria Orellano, James Quigley, Dafna Tapiero, Emiko Todoroki, and Tracy Tucker.
Abbreviations and Acronyms

AML  anti-money laundering

APG  Asia/Pacific Group on Money Laundering

Bank  World Bank Group

Basel Committee  Basel Committee on Bank Supervision

BCCI  Bank of Credit and Commerce International

CAS  Country Assistance Strategy

CFATF  Caribbean Financial Action Task Force

CFT  combating the financing of terrorism

CTC  United Nations Security Council Counter Terrorism Committee

Egmont Group  The Egmont Group of Financial Intelligence Units

ESAAMLG  Eastern and Southern Africa Anti-Money Laundering Group

FATF  Financial Action Task Force on Money Laundering, Group d'action Financière sur le blanchiment de capital (GAFI)

FSRB  FATF Style Regional Bodies

FIU  Financial Intelligence Unit

The Forty Recommendations  The Forty Recommendations on Money Laundering issued by FATF

Fund  International Monetary Fund

GAFI  Group d’action Financière sue le blanchiment de capital (FATF)

GAFISUD  Financial Action Task Force on Money Laundering in South America
IAIS  International Association of Insurance Supervisors
IFTs  informal funds transfer systems
IMF  International Monetary Fund
IOSCO  International Organization of Securities Commissions
KYC  “know-your-customer”
MONEYVAL  Council of Europe the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
MOU  memorandum of understanding
NCCT  Non-Cooperative Countries and Territories
OAS  Organization of American States
OFC  Offshore Financial Center
PC-R-EV  Now known as MONEYVAL
ROSC  Report on Observance of Standards and Codes
Special Recommendations  Nine Special Recommendations on Terrorist Financing issued by FATF
STR  suspicious transaction reports
TA  Technical Assistance
UN  United Nations
UNSCCTC  United Nations Security Council Counter Terrorism Committee
Wolfsberg Group  Wolfsberg Group of Banks
Introduction: How to Use this Reference Guide

This Second Edition of the Reference Guide is intended to serve as a single, comprehensive source of information for countries that wish to establish or improve their legal and institutional frameworks for anti-money laundering (AML) and combating the financing of terrorism (CFT). These issues have become increasingly important in a global economy where funds can be easily and immediately transferred from one financial institution to another, including transfers to institutions in different countries. The international community is relying upon all countries to establish effective AML/CFT regimes that are capable of successfully preventing, detecting and prosecuting money laundering and terrorist financing in order to fight the devastating economic and social consequences of these criminal activities.

Part A of this Reference Guide describes the problem of money laundering and terrorist financing, their adverse consequences, and the benefits of an effective regime. It also identifies the relevant international standard-setting organizations and discusses their specific efforts and instruments that fight these activities.

Part B describes the various elements that are part of a comprehensive legal and institutional AML and CFT framework for any country. Each of these components has been established by the Financial Action Task on Money Laundering (FATF) and the other international standard setters and each element is essential to a comprehensive and effective regime. This part of the Reference Guide is a step-by-step approach to achieve compliance with international standards, although it does not dictate the specific methods or actions to be adopted. Rather, it raises the issues that must be addressed and discusses the options that a country has to resolve these issues.

Part C describes the role of the World Bank and International Monetary Fund (IMF) in the global effort and the coordination of technical assistance
available to countries in order to help them achieve compliance with international standards.

Each chapter is a self-contained discussion of the topics covered in that chapter (although references are made to related discussions in other chapters) with detailed references to background and original source materials. Annexes I, II and III provide complete citations to reference materials that are used in the Reference Guide or that are otherwise useful to a country in dealing with the many difficult issues associated with AML and CFT. For convenience, Annexes IV and V restate the international standards set by FATF, The Forty Recommendations on Money Laundering (revised in 2003), Glossary and Interpretative Notes and the nine Special Recommendations on Terrorist Financing, respectively. Annex VI is FATF’s Interpretative Notes and Guidance Notes for the Special Recommendations on Terrorist Financing and Self-Assessment Questionnaire for countries on terrorist financing. Finally, Annexes VII and VIII are cross references for the FATF recommendations to discussions in the Reference Guide.

As a country reviews its AML and CFT legal and institutional frameworks, it may wish to use the Comprehensive Methodology on AML/CFT referred to in Chapter X as its own checklist and self-assessment mechanism. This is the same Methodology used by FATF, the FATF-style regional bodies, the Bank and IMF in making assessments of either their own members or of other countries.
Chapter I

Money Laundering and Terrorist Financing: Definitions and Explanations

A. What Is Money Laundering?
B. What is Terrorist Financing?
C. The Link Between Money Laundering and Terrorist Financing
D. The Magnitude of the Problem
E. The Processes
  1. Placements
  2. Layering
  3. Integration
F. Where Do Money Laundering and Terrorist Financing Occur?
G. Methods and Typologies

For most countries, money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques used to launder money and finance terrorism add to the complexity of these issues. Such sophisticated techniques may involve different types of financial institutions; multiple financial transactions; the use of intermediaries, such as financial advisers, accountants, shell corporations and other service providers; transfers to, through, and from different countries; and the use of different financial instruments and other kinds of value-storing assets. Money laundering is, however, a fundamentally simple concept. It is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Basically, money laundering involves the proceeds of criminally derived property rather than the property itself.

The financing of terrorism is also a fundamentally simple concept. It is the financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. Less simple, however, is defining terrorism
itself, because the term may have significant political, religious, and national implications from country to country. Money laundering and terrorist financing often display similar transactional features, mostly having to do with concealment.

Money launderers send illicit funds through legal channels in order to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is the support of terrorism. But the result is the same—reward. When money is laundered, criminals profit from their actions; they are rewarded by concealing the criminal act that generates the illicit proceeds and by disguising the origins of what appears to be legitimate proceeds. Similarly, those who finance terrorism are rewarded by concealing the origins of their funding and disguising the financial support to carry out their terrorist stratagems and attacks.

A. What Is Money Laundering?


- The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;

The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense…or offenses.³

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering (AML) efforts,⁴ defines the term “money laundering” succinctly as “the processing of…criminal proceeds to disguise their illegal origin” in order to “legitimize” the ill-gotten gains of crime.⁵

A money laundering predicate offense is the underlying criminal activity that generated proceeds, which when laundered, results in the offense of money laundering. By its terms, the Vienna Convention limits predicate offenses to drug trafficking offenses. As a consequence, crimes unrelated to drug trafficking, such as, fraud, kidnapping and theft, for example, do not constitute money laundering offenses under the Vienna Convention. Over the years, however, the international community has developed the view that predicate offenses for money laundering should go well beyond drug trafficking. Thus, FATF and other international instruments have expanded the Vienna Convention’s definition of predicate offenses to include other serious crimes.⁶ For example, the Palermo Convention requires all participant countries to apply that convention’s money laundering offenses to “the widest range of predicate offenses.”⁷

In its 40 recommendations for fighting money laundering (The Forty Recommendations), FATF specifically incorporates the technical and legal definitions of money laundering set out in the Vienna and Palermo Conventions and lists 20 designated categories of offences that must be included as predicate offences for money laundering.⁸

---

³. See Vienna Convention, articles 3(b) and (c)(i); and Palermo Convention, article 6(i).
⁴. See Chapter III, B., FATF.
⁶. See discussion at Chapter V, A.,2., The Scope of the Predicate Offenses.
B. What Is Terrorist Financing?

The United Nations (UN) has made numerous efforts, largely in the form of international treaties, to fight terrorism and the mechanisms used to finance it. Even before the September 11th attack on the United States, the UN had in place the International Convention for the Suppression of the Financing of Terrorism (1999), which provides:

1. Any person commits an offense within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
   a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
   b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

2. ...

3. For an act to constitute an offense set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in paragraph 1, subparagraph (a) or (b).9

The difficult issue for some countries is defining terrorism. Not all of the countries that have adopted the convention agree on specifically what actions constitute terrorism. The meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country.

FATF, which is also recognized as the international standard setter for efforts to combat the financing of terrorism (CFT), does not specifically define the term financing of terrorism in its nine Special Recommendations on Terrorist Financing (Special Recommendations) developed following the events of September 11, 2001. Nonetheless, FATF urges countries to ratify and implement the 1999 United Nations International Convention for Suppression of the Financing of Terrorism. Thus, the above definition is the one most countries have adopted for purposes of defining terrorist financing.

**C. The Link Between Money Laundering and Terrorist Financing**

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

For these reasons, FATF has recommended that each country criminalize the financing of terrorism, terrorist acts and terrorist organizations, and designate such offenses as money laundering predicate offenses. Finally, FATF has stated that the nine Special Recommendations combined with The Forty Recommendations on money laundering constitute the basic framework for preventing, detecting and suppressing both money laundering and terrorist financing.

Efforts to combat the financing of terrorism also require countries to consider expanding the scope of their AML framework to include non-profit organizations, particularly charities, to make sure such organizations are not

---

10. See Chapter III, B., FATF.
11. The Special Recommendations are reprinted in Annex V of this Reference Guide.
12. Id., at Spec. Rec. I.
13. Id., at Spec. Rec. II.
14. Id.
15. Id., at introductory paragraph.
used, directly or indirectly, to finance or support terrorism.\textsuperscript{16} CFT efforts also require examination of alternative money transmission or remittance systems, such as \textit{hawalas}. This effort includes consideration of what measures should be taken to preclude the use of such entities by money launderers and terrorists.\textsuperscript{17}

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations. Consequently, this difference requires special laws to deal with terrorist financing. However, to the extent that funds for financing terrorism are derived from illegal sources, such funds may already be covered by a country’s AML framework, depending upon the scope of predicate offenses for money laundering.

\textbf{D. The Magnitude of the Problem}

By their very nature, money laundering and terrorist financing are geared towards secrecy and do not lend themselves to statistical analysis. Launderers do not document the extent of their operations or publicize the amount of their profits, nor do those who finance terrorism. Moreover, because these activities take place on a global basis, estimates are even more difficult to produce. Launderers use various countries to conceal their ill-gotten proceeds, taking advantage of differences among countries with regard to AML regimes, enforcement efforts and international cooperation. Thus, reliable estimates on the size of the money laundering and terrorist financing problems on a global basis are not available.

With regard to money laundering only, the International Monetary Fund has estimated that the aggregate amount of funds laundered in the world could range between two and five per cent of the world’s gross domestic product. Using 1996 statistics, these percentages would approximate between

\textsuperscript{16} \textit{Special Recommendations}, Spec. Rec. VIII.  
\textsuperscript{17} \textit{Special Recommendations}, Spec. Rec. VI.
US $590 billion and US $1.5 trillion.\textsuperscript{18} Thus, by any estimate, the size of the problem is very substantial and merits the complete attention of every country.

E. The Processes

The initial concern over money laundering began with its early connection to illegal trafficking in narcotic drugs. The objective of drug traffickers was to convert typically small denominations of currency into legal bank accounts, financial instruments, or other assets. Today, ill-gotten gains are produced by a vast range of criminal activities—among them political corruption, illegal sales of weapons, and illicit trafficking in and exploitation of human beings. Regardless of the crime, money launderers resort to placement, layering, and integration in the process of turning illicit proceeds into apparently legal monies or goods.

1. Placement

The initial stage of the process involves placement of illegally derived funds into the financial system, usually through a financial institution. This can be accomplished by depositing cash into a bank account. Large amounts of cash are broken into smaller, less conspicuous amounts and deposited over time in different offices of a single financial institution or in multiple financial institutions. The exchange of one currency into another, as well as the conversion of smaller notes into larger denominations, may occur at this stage. Furthermore, illegal funds may be converted into financial instruments, such as money orders or checks, and commingled with legitimate funds to divert suspicion. Furthermore, placement may be accomplished by the cash purchase of a security or a form of an insurance contract.

2. Layering

The second money laundering stage occurs after the ill-gotten gains have entered the financial system, at which point the funds, securities or insurance contracts are converted or moved to other institutions, further separating them from their criminal source. Such funds could then be used to purchase other securities, insurance contracts or other easily transferable investment instruments and then sold through yet another institution. The funds could also be transferred by any form of negotiable instrument such as check, money order or bearer bond, or the may be transferred electroni-
ally to other accounts in various jurisdictions. The launderer may also
disguise the transfer as a payment for goods or services or transfer the
funds to a shell corporation.

3. Integration

The third stage involves the integration of funds into the legitimate economy.
This is accomplished through the purchase of assets, such as real estate, secu-
rities or other financial assets, or luxury goods.

These three stages are also seen in terrorist financing schemes, except
that stage three integration involves the distribution of funds to terrorists
and their supporting organizations, while money laundering, as discussed
previously, goes in the opposite direction—integrating criminal funds into the
legitimate economy.

F. Where Do Money Laundering and Terrorist Financing Occur?

Money laundering and the financing of terrorism can, and do, occur in
any country in the world, especially those with complex financial systems.
Countries with lax, ineffective, or corrupt AML and CFT infrastructures are
also likely targets for such activities. No country is exempt.

Because complex international financial transactions can be abused to
facilitate the laundering of money and terrorist financing, the different stages
of money laundering and terrorist financing occur within a host of different
countries. For example, placement, layering, and integration may each occur
in three separate countries; one or all of the stages may also be removed from
the original scene of the crime.

G. Methods and Typologies

Money can be laundered in a number of ways, ranging from small cash
deposits in unremarkable bank accounts (for subsequent transfer) to the pur-
chase and resale of luxury items such as automobiles, antiques, and jewelry.
Illicit funds can also be transferred through a series of complex international financial transactions. Launderers are very creative—when overseers detect one method, the criminals soon find another.

The various techniques used to launder money or finance terrorism are generally referred to as methods or typologies. The terms, methods or typologies, may be referred to interchangeably, without any distinction between the two. At any point in time, it is impossible to describe accurately the universe of the different methods criminals use to launder money or finance terrorism. Moreover, their methods are likely to differ from country to country because of a number of characteristics or factors unique to each country, including its economy, complexity of financial markets, AML regime, enforcement effort and international cooperation. In addition, the methods are constantly changing.

Nevertheless, various international organizations have produced excellent reference works on money laundering methods and techniques. FATF has produced reference materials on methods in its annual reports and annual typologies report.¹⁹ The various FATF-style regional bodies also provide information on the various typologies seen in their regions. For the most up-to-date information on money laundering methods and typologies, please consult the websites for these entities.²⁰ In addition, the Egmont Group has produced a compilation of one hundred sanitized cases about the fight against money laundering from its member financial intelligence units.²¹

---

²⁰. See Chapter IV for a discussion of the FATF-style regional bodies.
Criminal enterprises and terrorist financing operations succeed largely to the extent that they are able to conceal the origins or sources of their funds and sanitize the proceeds by moving them through national and international financial systems. The absence of, or a lax or corrupt, anti-money laundering regime in a particular country permits criminals and those who finance terrorism to operate, using their financial gains to expand their criminal pursuits and fostering illegal activities such as corruption, drug trafficking, illicit trafficking and exploitation of human beings, arms trafficking, smuggling, and terrorism.

While money laundering and the financing of terrorism can occur in any country, they have particularly significant economic and social consequences for developing countries, because those markets tend to be small and, therefore, more susceptible to disruption from criminal or terrorist influences.

Money laundering and terrorist financing also have significant economic and social consequences for countries with fragile financial systems because
they too are susceptible to disruption from such influences. Ultimately, the economy, society, and security of countries used as money-laundering or terrorist financing platforms are all imperiled. The magnitude of these adverse consequences is difficult to establish, however, since such adverse impacts cannot be quantified with precision, either in general for the international community, or specifically for an individual country.

On the other hand, an effective framework for anti-money laundering (AML) and combating the financing of terrorism (CFT) have important benefits, both domestically and internationally, for a country. These benefits include lower levels of crime and corruption, enhanced stability of financial institutions and markets, positive impacts on economic development and reputation in the world community, enhanced risk management techniques for the country’s financial institutions, and increased market integrity.

A. The Adverse Implications for Developing Countries

1. Increased Crime and Corruption

Successful money laundering helps make criminal activities profitable; it rewards criminals. Thus, to the extent that a country is viewed as a haven for money laundering, it is likely to attract criminals and promote corruption. Havens for money laundering and terrorist financing have:

- A weak AML/CFT regime;
- Some or many types of financial institutions that are not covered by an AML/CFT framework;
- Little, weak or selective enforcement of AML/CFT provisions;
- Ineffective penalties, including difficult confiscation provisions; and
- A limited number of predicate crimes for money laundering.

If money laundering is prevalent in a country, it generates more crime and corruption. It also enhances the use of bribery in critical gateways to make money laundering efforts successful, such as:

- Employees and management of financial institutions,
- Lawyers and accountants,
- Legislatures,
- Enforcement agencies,
- Supervisory authorities,
- Police authorities,
- Prosecutors, and
- Courts.

A comprehensive and effective AML/CFT framework, together with timely implementation and effective enforcement, on the other hand, significantly reduce the profitable aspects of this criminal activity and, in fact, discourage criminals and terrorists from utilizing a country. This is especially true when the proceeds from criminal activities are aggressively confiscated and forfeited as part of a country’s overall AML/CFT legal framework.

2. International Consequences and Foreign Investment

A reputation as a money laundering or terrorist financing haven, alone, could cause significant adverse consequences for development in a country. Foreign financial institutions may decide to limit their transactions with institutions from money laundering havens; subject these transactions to extra scrutiny, making them more expensive; or terminate correspondent or lending relationships altogether. Even legitimate businesses and enterprises from money laundering havens may suffer from reduced access to world markets or access at a higher cost due to extra scrutiny of their ownership, organization and control systems.

Any country known for lax enforcement of AML/CFT is less likely to receive foreign private investment. For developing nations, eligibility for foreign governmental assistance is also likely to be severely limited.
Finally, the Financial Action Task Force on Money Laundering (FATF) maintains a list of countries that do not comply with AML requirements or that do not cooperate sufficiently in the fight against money laundering. Being placed on this list, known as the “non-cooperating countries and territories” (NCCT) list, gives public notice that the listed country does not have in place even minimum standards. Beyond the negative impacts referred to here, individual FATF member countries could also impose specific counter-measures against a country that does not take action to remedy its AML/CFT deficiencies.

3. Weakened Financial Institutions

Money laundering and terrorist financing can harm the soundness of a country’s financial sector, as well as the stability of individual financial institutions in multiple ways. The following discussion focuses on banking institutions, but the same consequences, or similar ones, are also applicable to other types of financial institutions, such as securities firms, insurance companies, and investment management firms. The adverse consequences generally described as reputational, operational, legal and concentration risks are interrelated. Each has specific costs:

- Loss of profitable business,
- Liquidity problems through withdrawal of funds,
- Termination of correspondent banking facilities,
- Investigation costs and fines,
- Asset seizures,
- Loan losses and
- Declines in the stock value of financial institutions.

Reputational risk is the potential that adverse publicity regarding a bank’s business practices and associations, whether accurate or not, will

---

2. See Chapter III, FATF, The NCCT List.
3. Id.
cause a loss of confidence in the integrity of the institution.\textsuperscript{5} Customers, both borrowers and depositors, as well as investors cease doing business with an institution whose reputation has been damaged by suspicions or allegations of money laundering or terrorist financing.\textsuperscript{6} The loss of high quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may also withdraw their funds, thereby reducing an inexpensive source of funding for the bank.

Moreover, funds placed on deposit with a bank by money launderers cannot be relied upon as a stable source of funding. Large amounts of laundered funds are often subject to unanticipated withdrawals from a financial institution through wire transfers or other transfers, causing potential liquidity problems.

Operational risk is the potential for loss resulting from inadequate or failed internal processes, people and systems, or external events.\textsuperscript{7} As noted above, such losses occur when institutions incur reduced, terminated, or increased costs for inter-bank or correspondent banking services. Increased borrowing or funding costs can also be included in such losses.

Legal risk is the potential for law suits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an institution, or even closure of such an institution.\textsuperscript{8} Money laundering involves criminals in almost every aspect of the money laundering process. As a consequence, legitimate customers may also be victims of a financial crime, lose money and sue the institution for reimbursement. There may be investigations, by banking or other law enforcement authorities resulting in increased costs, as well as fines and other penalties involved. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

Concentration risk is the potential for loss resulting from too much credit or loan exposure to one borrower.\textsuperscript{9} Statutory provisions or regulations usually restrict a bank’s exposure to a single borrower or group of related borrowers. Lack of knowledge about a particular customer, the customer’s

\begin{footnotesize}
\begin{enumerate}
\item Id., paragraph 11.
\item Id.
\item Id., paragraph 12.
\item Id., paragraph 13.
\item Id., paragraph 14.
\end{enumerate}
\end{footnotesize}
business, or what the customer’s relationship is to other borrowers, can place a bank at risk in this regard. This is particularly a concern where there are related counterparts, connected borrowers, and a common source of income or assets for repayment. Loan losses also result, of course, from unenforceable contracts and contracts made with fictitious persons.

Banks and their account holders are protected when effective due diligence regimes are in place. Identification of the beneficial owners of an account is critical to an effective AML/CFT regime. Such identification procedures protect against business relationships with fictitious persons or corporate entities without substantial assets, such as shell corporations, as well as known criminals or terrorists. Due diligence procedures also help the financial institution to understand the nature of the customer’s business interests and underlying financial issues.

4. Compromised Economy and Private Sector

Money launderers are known to use “front companies,” i.e., business enterprises that appear legitimate and engage in legitimate business but are, in fact, controlled by criminals.

These front companies co-mingle the illicit funds with legitimate funds in order to hide the ill-gotten proceeds. Front companies’ access to illicit funds, allows them to subsidize the front company’s products and services, even at below-market prices. As a consequence, legitimate enterprises find it difficult to compete with such front companies, the sole purpose of which is to preserve and protect the illicit funds, not to produce a profit.

By using front companies and other investments in legitimate companies money laundering proceeds can be utilized to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

---

10. See Chapter VI, Customer Identification and Due Diligence.
5. Damaged Privatization Efforts

Money launderers threaten the efforts of many countries to reform their economies through privatization. These criminal organizations are capable of outbidding legitimate purchasers of former state-owned enterprises. When illicit proceeds are invested in this manner, criminals increase their potential for more criminal activities and corruption, as well as deprive the country of what should be a legitimate, market-based, tax paying enterprise.

B. The Benefits of an Effective AML/CFT Framework

1. Fighting Crime and Corruption

A strong AML/CFT institutional framework that includes a broad scope of predicate offenses for money laundering helps to fight crime and corruption in general. When money laundering itself is made a crime, it provides another avenue to prosecute criminals, both those who commit the underlying criminal acts and those who assist them through laundering illegally obtained funds. Similarly, an AML/CFT framework that includes bribery as a predicate offense and is enforced effectively provides fewer opportunities for criminals to bribe or otherwise corrupt public officials.

An effective AML regime is a deterrent to criminal activities in and of itself. Such a regime makes it more difficult for criminals to benefit from their acts. In this regard, confiscation and forfeiture of money laundering proceeds are crucial to the success of any AML program. Forfeiture of money laundering proceeds eliminates those profits altogether, thereby reducing the incentive to commit criminal acts. Thus, it should go without saying that the broader the scope of predicate offenses for money laundering, the greater the potential benefit.

12. *Id.*
13. See Chapter I, What is Money Laundering; see also Chapter V, Scope of the Predicate Offense.
2. Enhancing Stability of Financial Institutions

Public confidence in financial institutions, and hence their stability, is enhanced by sound banking practices that reduce financial risks to their operations. These risks include the potential that either individuals or financial institutions will experience loss as a result of fraud from direct criminal activity, lax internal controls, or violations of laws and regulations.

Customer identification and due diligence procedures, also known as “know your customer” (KYC) rules, are part of an effective AML/CFT regime. These rules are not only consistent with, but also enhance, the safe and sound operation of banks and other types of financial institutions. These policies and procedures are an effective risk management tool. For example, in situations where a given individual or corporation may own several businesses that are seemingly separate entities and an institution has comprehensive knowledge of that particular customer’s operations by performing KYC procedures, that institution can limit its exposure to that borrower and, thereby, its lending risk. Because of the risk management benefits of KYC procedures, the Basel Committee on Banking Supervision incorporates a KYC policy as part of its Core Principles for Effective Banking Supervision, aside from the AML reasons.14

In addition to the public confidence benefits, an effective AML/CFT regime reduces the potential that the institution could experience losses from fraud. Proper customer identification procedures and determination of beneficial ownership provide specific due diligence for higher risk accounts and permit monitoring for suspicious activities. Such prudential internal controls are consistent with the safe and sound operation of a financial institution.

3. Encouraging Economic Development

Money laundering has a direct negative effect on economic growth by diverting resources to less productive activities. Laundered illegal funds follow a different path through the economy than legal funds. Rather than being

---

placed in productive channels for further investment, laundered funds are often placed into “sterile” investments to preserve their value or make them more easily transferable. Such investments include real estate, art, jewelry, antiques or high-value consumption assets such as luxury automobiles. Such investments do not generate additional productivity for the broader economy.

Even worse, criminal organizations may transform productive enterprises into sterile investments by operating them for the primary purpose of laundering illegal proceeds, rather than as profit-generating enterprises. Such an enterprise does not respond to consumer demand or to other legitimate and productive uses for capital. Having a country’s resources dedicated to sterile investments, as opposed to investments that drive other productive purposes, ultimately reduces the productivity of the overall economy.

Strong AML/CFT regimes provide a disincentive for the criminal involvement in the economy. This permits investments to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.
In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. The international response is, in large part, recognition of the fact that money laundering and terrorist financing take advantage of high speed international transfer mechanisms, such as wire transfers, to accomplish their goals. Therefore, concerted cross-border cooperation and coordination are needed to thwart the efforts of criminals and terrorists.

The international effort began with the recognition that drug trafficking was an international problem and could only be addressed effectively on a multilateral basis. Thus, the first international convention concerning money laundering had drug trafficking offenses as the only predicate offenses. (A predicate offense is the underlying crime that produces the proceeds that are the subject of money laundering.) Because many more types of crimes are now international concerns, most countries now include a wide range of serious offenses as money laundering predicate offenses.
This chapter discusses the various international organizations that are viewed as the international standard setters. It further describes the documents and instrumentalities that have been developed for anti-money laundering (AML) and combating the financing of terrorism (CFT) purposes.

A. The United Nations

The United Nations (UN) was the first international organization to undertake significant action to fight money laundering on a truly world-wide basis.\textsuperscript{1} The UN is important in this regard for several reasons. First, it is the international organization with the broadest range of membership. Founded in October of 1945, there are currently 191 member states of the UN from throughout the world.\textsuperscript{2} Second, the UN actively operates a program to fight money laundering; the Global Programme Against Money Laundering (GPML),\textsuperscript{3} which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (ODC).\textsuperscript{4} Third, and perhaps most importantly, the UN has the ability to adopt international treaties or conventions that have the effect of law in a country once that country has signed, ratified and implemented the convention, depending upon the country’s constitution and legal structure. In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other action on the part of an individual country.

1. The Vienna Convention

Due to growing concern about increased international drug trafficking and the tremendous amounts of related money entering the banking system, the UN, through the United Nations Drug Control Program (UNDCP) initiated...
an international agreement to combat drug trafficking and money laundering. In 1988, this effort resulted in the adoption of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention).\(^5\) The Vienna Convention, which was named for the city in which it was signed, deals primarily with provisions to fight the illicit drug trade and related law enforcement issues; 169 countries are party to the convention.\(^6\) Although it does not use the term money laundering, the convention defines the concept and calls upon countries to criminalize the activity.\(^7\) The Vienna Convention is limited, however, to drug trafficking offenses as predicate offenses and does not address the preventive aspects of money laundering. The convention came into force on November 11, 1990.

2. The Palermo Convention

In order to expand the effort to fight international organized crime, the UN adopted The International Convention Against Transnational Organized Crime (2000) (Palermo Convention).\(^8\) This convention, also named for the city in which it was signed, contains a broad range of provisions to fight organized crime and commits countries that ratify this convention to implement its provisions through passage of domestic laws. With respect to money laundering, the Palermo Convention specifically obligates each ratifying country to:

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;\(^9\)
- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;\(^10\)

\(^7\) The Vienna Convention, Article 3 (b) and (c) (i).
\(^8\) [http://www.undcp.org/adhoc/palermo/convmain.html](http://www.undcp.org/adhoc/palermo/convmain.html).
\(^9\) The Palermo Convention, Article 6.
\(^10\) Id., Article 7 (1) (a).
• Authorize the cooperation and exchange of information among admin-
istrative, regulatory, law enforcement and other authorities, both
domestically and internationally, and consider the establishment of a
financial intelligence unit to collect, analyze and disseminate informa-
tion; \(^{11}\) and
• Promote international cooperation. \(^{12}\)

This convention went into force on the 29th of September 2003, having
been signed by 147 countries and ratified by 82 countries. \(^{13}\) The Palermo
Convention is important because its AML provisions adopt the same
approach previously adopted by the Financial Action Task Force on Money
Laundering (FATF) in its Forty Recommendations on Money Laundering. \(^{14}\)

3. International Convention for the Suppression of the Financing of Terrorism

The financing of terrorism was an international concern prior to the attacks
on the United States of September 11, 2001. In response to this concern,
the UN adopted the International Convention for the Suppression of the
Financing of Terrorism (1999). \(^{15}\) This convention came into force on April
10, 2002, with 132 countries signing the convention and 112 countries rati-
fying it. \(^{16}\) (See Annex III of this Reference Guide for a listing of specified
conventions.)

This convention requires ratifying states to criminalize terrorism, terror-
ist organizations and terrorist acts. Under the convention, it is unlawful for
any person to provide or collect funds with the (1) intent that the funds be
used for, or (2) knowledge that the funds be used to, carry out any of the acts
of terrorism defined in the other specified conventions that are annexed to
this convention.

\(^{11}\) *Id.*, Article 7 (1) (b).
\(^{12}\) *Id.*, Article 7 (3) and (4).
    html.
\(^{14}\) See Discussion in this Chapter, FATF.
    policy/newsactionalerts/advocacy/fin_terr.asp.
4. Security Council Resolution 1373

Unlike an international convention, which requires signing, ratification, and implementation by the UN member country to have the effect of law within that country, a Security Council Resolution passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorists, including freezing funds or assets of persons, organizations or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorists; and
- cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

5. Security Council Resolution 1267 and Successors

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the “Sanctions Committee” (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999, dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002),

provided some exclusions (1452 of December 20, 2002\textsuperscript{23}), and measures to improve implementation (1455 of January 17, 2003\textsuperscript{24}).

The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.\textsuperscript{25}

6. Global Programme against Money Laundering

The UN Global Programme against Money Laundering (GPML) is within the UN Office of Drugs and Crime (ODC).\textsuperscript{26} The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request. It focuses its efforts in the following areas:

- Raise the awareness level among key persons in UN member states;
- Help create legal frameworks with the support of model legislation for both common and civil law countries;
- Develop institutional capacity, in particular with the creation of financial intelligence units;
- Provide training for legal, judicial, law enforcement regulators and the private financial sectors;
- Promote a regional approach to addressing problems; develop and maintain strategic relationships with other organizations; and
- Maintain a database of information and undertake analysis of relevant information.

Thus, the GPML is a resource for information, expertise and technical assistance in establishing or improving a country’s AML infrastructure.

\textsuperscript{24} http://www.un.org/Docs/sc/unsc_resolutions03.html.
\textsuperscript{26} “Global Programme against Money Laundering,” http://www.imolin.org/imolin/gpml.html.
7. The Counter-Terrorism Committee

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism. The CTC, which is comprised of the 15 members of the Security Council, is not a law enforcement agency; it does not issue sanctions, nor does it prosecute or condemn individual countries. Rather, the Committee seeks to establish a dialogue between the Security Council and member countries on how to achieve the objectives of Resolution 1373.

Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution’s measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373. The CTC identifies the areas where a country needs to strengthen its statutory base and infrastructure, and facilitate assistance for countries, although the CTC does not, itself, provide direct assistance.

The CTC maintains a website with a directory for countries seeking help in improving their counter-terrorism infrastructures. It contains copies of model legislation and other helpful information.

B. The Financial Action Task Force on Money Laundering

Formed in 1989 by the G-7 countries, the Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body whose purpose is to develop and promote an international response to combat money launder-
In October of 2001, FATF expanded its mission to include combating the financing of terrorism.

FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 31 countries and territories and two regional organizations. In addition, FATF works in collaboration with a number of international bodies and organizations. These entities have observer status with FATF, which does not entitle them to vote, but otherwise permits full participation in plenary sessions and working groups.

FATF’s three primary functions with regard to money laundering are:

1. monitoring members’ progress in implementing anti-money laundering measures;
2. reviewing and reporting on laundering trends, techniques and countermeasures; and
3. promoting the adoption and implementation of FATF anti-money laundering standards globally.

32. Id. at Terrorist Financing.
33. The 31 member countries and territories are: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong-China, Iceland, Ireland, Italy, Japan, Luxemburg, Mexico, Kingdom of the Netherlands, New Zealand, Norway, Portugal, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States. The two regional organizations are the European Commission and the Gulf Co-operation Council.
34. The international bodies are regional FATF-style regional bodies (FSRBs) that have similar form and functions to those of FATF. Some FATF members also participate in the FSRBs. These bodies are: Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CAFTF), Council of Europe MONEYVAL (previously PC-R-EV) Committee, Eastern and Southern Africa Anti-Money Laundering Group (ESAMLG) and Financial Action Task Force on Money Laundering in South America (GAFISUD). For a discussion of these organizations, see Chapter IV, Regional Bodies and Relevant Groups, FATF-Style Regional Bodies. FATF also works with the Egmont Group.
35. Each of the international organizations, which have, among other functions, a specific anti-money laundering mission or function, are: African Development Bank, Asia Development Bank, The Commonwealth Secretariat, European Bank for Reconstruction and Development, European Central Bank (ECB), Europol, Inter-American Development Bank (IDB), Intergovernmental Action Group Against Money-Laundering in Africa (GIABA), International Association of Insurance Supervisors (IAIS), International Monetary Fund (IMF), Interpol, International Organization of Securities Commissions (IOSCO), Organization of American States/Inter-American Committee Against Terrorism (OAS/CICCTE), Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD), Organization for Economic Co-operation and Development (OECD), Offshore Group of Banking Supervisors (OGBS), United Nations Office on Drugs and Crime (UNODC), World Bank and World Customs Organization (WCO).
1. The Forty Recommendations

FATF has adopted a set of 40 recommendations, *The Forty Recommendations on Money Laundering (The Forty Recommendations)*, which constitute a comprehensive framework for AML and are designed for universal application by countries throughout the world.36 *The Forty Recommendations* set out principles for action; they permit a country flexibility in implementing the principles according to the country’s own particular circumstances and constitutional requirements. Although not binding as law upon a country, *The Forty Recommendations* have been widely endorsed by the international community and relevant organizations as the international standard for AML.

*The Forty Recommendations* are actually mandates for action by a country if that country wants to be viewed by the international community as meeting international standards. The individual recommendations are discussed in detail throughout this Reference Guide and, particularly in Chapters V, VI, VII, and VIII.

*The Forty Recommendations* were initially issued in 1990 and have been revised in 1996 and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally.

2. Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of *The Forty Recommendations* is facilitated by a two-stage process: self assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of *The Forty Recommendations*. In the mutual evaluation stage, each member is examined and assessed by experts from other member countries.

In the event that a country is unwilling to take appropriate steps to achieve compliance with *The Forty Recommendations*, FATF recommends that all financial institutions give special attention to business relations and transactions with persons, including companies and financial institutions, from such non-compliant countries and, where appropriate, report questionable transactions, i.e., those that have no apparent economic or visible lawful

---

purpose, to competent authorities. Ultimately, if a member country does not take steps to achieve compliance, membership in the organization can be suspended. There is, however, the process of peer pressure before these sanctions are enforced.

3. Reporting on Money Laundering Trends and Techniques

One of FATF’s functions is to review and report on money laundering trends, techniques and methods (also referred to as typologies). To accomplish this aspect of its mission, FATF issues annual reports on developments in money laundering through its Typologies Report. These reports are very useful for all countries, not just FATF members, to keep current with new techniques or trends to launder money and for other developments in this area.

4. The NCCT List

One of FATF’s objectives is to promote the adoption of international AML/CFT standards for all countries. Thus, its mission extends beyond its own membership, although FATF can only sanction its member countries and territories. Thus, in order to encourage all countries to adopt measures to prevent, detect and prosecute money launderers, i.e., to implement The Forty Recommendations, FATF has adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in this area. The process uses 25 criteria, which are consistent with The Forty Recommendations, to identify such non-cooperative countries and territories (NCCT’s) and place them on a publicly available list.

An NCCT country is encouraged to make rapid progress in remedying its deficiencies. In the event an NCCT country does not make sufficient progress, counter-measures may be imposed. Counter measures consist of specific actions by FATF member countries taken against an NCCT-listed country.

37. Id., Rec. 21.
In addition to the application of applying special attention to business relationships and transactions from such countries, the FATF can also impose further counter-measures, which are to be applied in a gradual, proportionate and flexible manner; these include:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;
- In considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of banks, taking into account the fact that the relevant bank is from an NCCT;
- Warning non-financial sector businesses that transactions with entities within the NCCTs might run the risk of money laundering.

Finally, these counter measures may include FATF-member countries terminating transactions with financial institutions from such a country.

Most countries make a concerted effort to be taken off the NCCT list because it causes significant problems for their financial institutions and businesses with respect to international transactions, as well as their reputation internationally.

5. Terrorist Financing

FATF also focuses its expertise on the world-wide effort to combat terrorist financing. To accomplish this expanded mission FATF has adopted nine *Special Recommendations on Terrorist Financing (Special*

---

Recommendations). As part of this effort, FATF members use a self-assessment questionnaire of their country’s actions to come into compliance with the Special Recommendations. FATF is continuing to develop guidance on techniques and mechanisms used in the financing of terrorism. Chapter IX of this Reference Guide contains a more detailed discussion of the Special Recommendations and the Questionnaire.

6. Methodology for AML/CFT Assessments

In 2002, following lengthy consultations, the FATF, International Monetary Fund (IMF), and World Bank adopted a single assessment methodology to be used both by FATF in its mutual evaluations and by the IMF and World Bank in their assessments under their financial sector assessment and offshore financial center programs. The FATF-style regional bodies (FSRBs), geographical sector organizations, which had been involved in the development of the methodology, subsequently agreed to use it for their mutual evaluations.

The methodology was revised in 2004, following the 2003 revision of The Forty Recommendations. The methodology sets out over 200 “essential criteria” that assessors should examine when carrying out assessments of an AML and CFT regime. It covers the legal and institutional AML/CFT framework for a country, including financial intelligence units. The methodology also includes relevant elements from United Nations Security Council resolutions and international conventions, as well as supervisory and regulatory standards for the banking, insurance and securities sectors. Those essential criteria describe the mandatory elements that need to be present to comply fully with each of The Forty Recommendations and Special Recommendations. The methodology includes guidance on how to rate compliance and is based on performance against the essential criteria.

The methodology also includes a number of “additional elements,” which are options for further strengthening AML/CFT systems. Although performance against these elements is reviewed as part of the overall assessment, they are not mandatory and are not assessed for compliance purposes.

---

The adoption of this single, comprehensive assessment methodology by the FATF, IMF, World Bank, and the FSRBs means a more uniform approach worldwide to the conduct of assessments and the ratings of country performance. A country undergoing an assessment will be required, at the first stage of the assessment, to prepare a self-assessment of its AML/CFT system according to the methodology document. The document is also a useful detailed guide to a country on measures that need to be in place to comply with the international standards.44

C. The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee)45 was formed in 1974 by the central bank governors of the Group of 10 countries.46 Individual countries are represented by their central bank, or by the relevant authority with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank supervisory issues. These standards and guidelines are adopted with the expectation that the appropriate authorities within each country will take all necessary steps to implement them through detailed measures, statutory, regulatory or otherwise, that best suit that country’s national system. Three of the Basel Committee’s supervisory standards and guidelines concern money laundering issues.

44. The methodology may be found at Methodology on AML/CFT, http://www.fatf-gafi.org/pdf/ Merh_2002_en.pdf. See also Chapter X, Development of a Universal AML/CFT Assessment Methodology, for a more detailed discussion of the methodology and its use by the World Bank and the IMF.
46. The Group of 10 countries is a misnomer, since there are actually 13 member countries. The Basel Committee members, (as well as the Group of 10) are: Belgium, Canada, France, Germany, Italy, Japan, Luxemburg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States.
1. Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its *Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention)*. The *Statement on Prevention* outlines basic policies and procedures that bank managements should ensure are in place within their institutions to assist in suppressing money laundering through the banking system, both domestically and internationally. The statement notes that banks can be used “unwittingly” as intermediaries by criminals. Thus, the committee considers the first and most important safeguard against money laundering to be “the integrity of banks own managements and their vigilant determination to prevent their institutions from becoming associated with criminals or being used as a channel for money laundering.”

There are essentially four principles contained in the *Statement on Prevention*:

- Proper customer identification;
- High ethical standards and compliance with laws;
- Cooperation with law enforcement authorities; and
- Policies and procedures to adhere to the statement.

First, banks should make reasonable efforts to determine the true identity of all customers requesting the institution’s services. It should be a bank’s explicit policy that significant business transactions are not conducted with customers who fail to provide evidence of their identity.

Second, banks should ensure that business is conducted in conformity with high ethical standards and that banks should adhere to laws and regulations pertaining to financial transactions. Here, banks should not offer services or provide active assistance in transactions where the bank has good reason to believe they are associated with money laundering.

Third, banks should cooperate fully with national law enforcement authorities to the extent permitted by local laws or regulations relating to

---

48. *Id.*, at Preamble paragraph 6.
49. *Id.*, at Customers identification.
50. *Id.*, at Compliance with laws.
customer confidentiality.\textsuperscript{51} No support or assistance should be provided to customers seeking to deceive law enforcement authorities through altered, incomplete or misleading information. Where a bank has a reasonable presumption that funds on deposit are from criminal activity or that transactions entered into are for a criminal purpose, the bank should take appropriate measures, including denial of assistance, severing of the customer relationship, and closing or freezing the account.

Fourth, banks should adopt formal policies consistent with the \textit{Statement on Prevention}.\textsuperscript{52} Furthermore, banks should assure that all staff members are aware of the bank’s policies and given proper training in matters covered by the bank’s policies. As part of a bank’s policies, specific procedures for customer identification should be adopted. Finally, the internal audit function within the institution should establish an effective means of testing for compliance.

2. Core Principles for Banking

In 1997, the Basel Committee issued its \textit{Core Principles for Effective Banking Supervision (Core Principles)},\textsuperscript{53} which provides a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. Of the total 25 Core Principles, one of them, Core Principle 15, deals with money laundering; it provides:

Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict “know your customer” rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.\textsuperscript{54}

These “know your customer” or “KYC” policies and procedures are a crucial part of an effective AML/CFT institutional framework for every country.

\textsuperscript{51} Id., at Cooperation with law enforcement authorities.
\textsuperscript{52} Id., at Adherence to the Statement.
\textsuperscript{53} http://www.bis.org/publ/bcbs30.pdf.
\textsuperscript{54} Id. Core Principle 15.
In addition to the Core Principles, the Basel Committee issued a “Core Principles Methodology” in 1999, which contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures.\textsuperscript{55} These, additional criteria include specific reference to compliance with The Forty Recommendations.\textsuperscript{56}

3. Customer Due Diligence

In October of 2001, the Basel Committee issued an extensive paper on KYC principles entitled, \textit{Customer due diligence for banks (Customer Due Diligence)}.\textsuperscript{57} This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards build upon and provide more specific information on the Statement on Prevention and Core Principle 15. The essential elements of KYC standards are set out in detail in this document.

It is worth noting that these KYC standards set out in \textit{Customer Due Diligence} are intended to benefit banks beyond the fight against money laundering by protecting the safety and soundness of banks and the integrity of banking systems. In addition, the Basel Committee, in this document, strongly supports the “adoption and implementation of the FATF recommendations, particularly those relating to banks,” and intends that the standards of \textit{Customer Due Diligence} “be consistent with the FATF recommendations.”\textsuperscript{58}

D. International Association of Insurance Supervisors

The International Association of Insurance Supervisors (IAIS), established in 1994, is an organization of insurance supervisors from more than 100 different countries and jurisdictions.\textsuperscript{59}

\textsuperscript{55} Core Principles Methodology at http://www.bis.org/publ/bcbs61.pdf.
\textsuperscript{56} Id., Annex 2, Excerpts from FATF recommendations.
\textsuperscript{57} Id.
\textsuperscript{58} Id., at paragraph 3.
\textsuperscript{59} For a list of member countries and jurisdictions, see Members at http://www.iaisweb.org/132_176_ENU_HTML.asp. The listing of members contains hyperlinks to individual member websites.
Its primary objectives are to:

- Promote cooperation among insurance regulators,
- Set international standards for insurance supervision,
- Provide training to members, and
- Coordinate work with regulators in the other financial sectors and international financial institutions.\(^{60}\)

In addition to member regulators, the IAIS has more than 60 observer members, representing industry associations, professional associations, insurance and reinsurance companies, consultants and international financial institutions.\(^{61}\)

While the IAIS covers a wide range of topics including virtually all areas of insurance supervision, it specifically deals with money laundering in one of its papers. In January 2002,\(^{62}\) the association issued Guidance Paper No. 5, Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities (AML Guidance Notes). It is a comprehensive discussion on money laundering in the context of the insurance industry. Like other international documents of its type, the AML Guidance Notes are intended to be implemented by individual countries taking into account the particular insurance companies involved, the products offered within the country, and the country’s own financial system, economy, constitution and legal system.

The AML Guidance Notes contain four principles for insurance entities:

- Comply with anti-money laundering laws,
- Have “know your customer” procedures,
- Cooperate with all law enforcement authorities, and
- Have internal AML policies, procedures and training programs for employees.

These four principles parallel the four principles in the Basel Committee’s Statement on Prevention. The AML Guidance Notes are entirely consistent

---

60. Id., at Home page.
61. Id., at Observers, for a listing of observer organizations.
with *The Forty Recommendations*, including suspicious activity reporting and other requirements. In fact, *The Forty Recommendations* are included in an appendix to the IAIS’s *AML Guidance Notes*.

### E. International Organization of Securities Commissioners

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 105 countries. In the event that there is no governmental authority charged with administration of securities laws in a given country, a self-regulatory body, such as a stock exchange, from that country is eligible for voting membership. There are also associate members, which are international organizations, and affiliate members, which are self regulatory organizations; neither of these two types of membership has voting privileges.

IOSCO has three core objectives for securities regulation:

- The protection of investors;
- Ensuring that markets are fair, efficient and transparent; and
- The reduction of systematic risk.

With regard to money laundering, IOSCO passed a “Resolution on Money Laundering” in 1992. Like other international organizations of this type, IOSCO does not have law-making authority. Similar to the Basel Committee and IAIS, it relies on its members to implement its recommendations within their respective countries. The resolution provides as follows:

Each IOSCO member should consider:

1. The extent to which customer identifying information is gathered and recorded by financial institutions under its supervision, with a view to

---

enhancing the ability of relevant authorities to identify and prosecute
money launderers;
2. The extent and adequacy of record-keeping requirements, from the per-
spective of providing tools to reconstruct financial transactions in the
securities and future markets;
3. Together with their national regulators charged with prosecuting
money laundering offenses, the appropriate manner in which to address
the identification and reporting of suspicious transactions;
4. The procedures in place to prevent criminals from obtaining control of
securities and futures businesses, with a view to working together with
foreign counterparts to share such information as needed;
5. The appropriate means to ensure that securities and futures firms
maintain monitoring and compliance procedures designed to deter and
detect money laundering;
6. The use of cash and cash equivalents in securities and futures trans-
actions, including the adequacy of documentation and the ability to
reconstruct any such transactions;
7. The most appropriate means, given their particular national authorities
and powers, to share information in order to combat money laundering.66

F. The Egmont Group of Financial Intelligence Units

As part of the effort to fight money laundering, governments have created
agencies to analyze information submitted by covered entities and persons
pursuant to money laundering reporting requirements. Such agencies are
commonly referred to as financial intelligent units (FIUs). These units serve
as the focal point for national AML programs, because they provide for the
exchange of information between financial institutions and law enforcement.
Because money laundering is practiced on a worldwide scale, there has also
been the need to share information on a cross-border basis.67

In 1995, a number of governmental units known today as FIUs began
working together and formed the Egmont Group of Financial Intelligence

67. See discussion in Chapter VII of this Reference Guide.
The Egmont Group was expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country’s FIU must first meet the Egmont FIU definition, which is “a central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing.”

A member must also commit to act in accordance with the Egmont Group’s Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These principles include conditions for the exchange of information, limitation on permitted uses of information, and confidentiality.

Membership of the Egmont Group is currently comprised of 94 jurisdictions. Members of the Egmont Group have access to a secure website, which is not available to the public, to exchange information.

The Egmont Group is an informal body without a secretariat or a permanent location. The Egmont Group meets in a plenary session once a year, and in working group sessions three times a year. Within the Egmont Group, the FIU heads make all the policy decisions, including membership. The group
established the Egmont Committee to help coordinate with the Working Groups and the FIU heads in between the annual plenary sessions.

Finally, the Egmont Group has produced training material with access for the public. The group compiled sanitized cases about the fight against money laundering from its member FIUs. It has also produced a video and Egmont-related documents that are available on its website.

Chapter IV

Regional Bodies and Relevant Groups

A. FATF-Style Regional Bodies

1. Asia/Pacific Group on Money Laundering
2. Caribbean Financial Action Task Force
3. Council of Europe–MONEYVAL
4. Eastern and Southern Africa Anti-Money Laundering Group
5. Financial Action Task Force on Money Laundering in South America

B. Wolfsberg Group of Banks

1. Anti-Money Laundering Principles for Private Banking
2. Statement on the Suppression of the Financing of Terrorism
3. Anti-Money Laundering Principles for Correspondent Banking

C. The Commonwealth Secretariat

D. Organization of American States–CICAD

In addition to the International Standard Setters discussed in Chapter III, there are other international organizations that play crucial roles in the fight against money laundering and terrorist financing. These groups tend to be organized according to geographic region or by the special purpose of the organization.

A. FATF-Style Regional Bodies

Financial Action Task Force on Money Laundering (FATF) regional groups or FATF-Style Regional Bodies (FSRBs) are very important in the promotion and implementation of anti-money laundering (AML) and combating the financing of terrorism (CFT) standards within their respective regions. FSRBs are to their regions what FATF is to the world.

They are modeled after FATF and, like FATF, have AML and CFT efforts as their sole objectives. They encourage implementation and enforce-
The FSRBs are voluntary and cooperative organizations. Membership is open to any country or jurisdiction within the given geographic region that is willing to abide by the rules and objectives of the organization. Some members of FATF are also members of the FSRBs. In addition to voting members, non-voting observer status is available to jurisdictions and organizations that wish to participate in the activities of the organization.

The FSRBs that are currently recognized by FATF are:

1. Asia/Pacific Group on Money Laundering (APG)\(^2\)
2. Caribbean Financial Action Task Force (CFATF)\(^3\)

---


3. Member countries are: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, Netherlands Antilles, Nicaragua, Panama, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, Trinidad and Tobago, Turks and Caicos Islands and Venezuela. Co-operating and Supporting Nations are: Canada, France, Mexico, Netherlands, Spain, United Kingdom and United States. Observers are: Asia/Pacific Group Secretariat, Caribbean Customs and Law Enforcement Council (CCLEC), Caribbean Development Bank (CDB), CARICOM, Commonwealth Secretariat, European Commission, FATF Secretariat, UN Global Programme on Money Laundering (GPML), Inter-American Development Bank (IADB), Interpol, Offshore
3. Council of Europe–MONEYVAL
4. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

Certain FSRBs have issued their own conventions or instruments on AML. For example, in 1990, CFATF issued its “Aruba Recommendations,” which are 19 recommendations that address money laundering from the Caribbean regional perspective and which complement The Forty Recommendations. Further, in 1992, a Ministerial meeting produced the “Kingston Declaration,” which affirmed the CFATF respective governments’ commitment to implementing international AML standards. Similarly, the Council of Europe, in 1990, adopted its “Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime” (the Strasbourg Convention). These are important instruments in the implementation of AML standards for their respective regions.

---


5. Members who have signed the ESAAMLG memorandum of understanding are: Botswana, Kenya, Malawi, Mauritius, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda. Members who have not signed the ESAAMLG MOU are: Lesotho, Zambia, and Zimbabwe. Observers are: Commonwealth Secretariat, FATF Secretariat, the UN Global Programme Against Money Laundering, Interpol, The World Custom Organization (WCO), African Development Bank (ADB), SADC Secretariat, the COMESA Secretariat, EAC Secretariat, East African Development Bank, Eastern and Southern Africa Development Bank, United Kingdom, United States, the IMF and World Bank. http://www.esaamlg.org.


In addition, the establishment of three other FSRBs is either under consideration or actively underway. The three new geographic areas would be for:

- The Middle East and North Africa (MENA);
- Central and Western Africa (GIABA); and
- Eurasia

Membership and other organizational issues need to be resolved, as well as mutual evaluation procedures, before any of these organizations will be recognized by FATF.

B. Wolfsberg Group of Banks

The Wolfsberg Group is an association of 12 global banks, representing primarily international private banking concerns. The group, which was named after the Château Wolfsberg in north-eastern Switzerland where the group was formed, has established four sets of principles for private banking.

1. Anti-Money Laundering Principles for Private Banking

These principles represent the group’s view of appropriate AML guidelines when dealing with the high net worth individuals and the private banking departments of financial institutions. They deal with customer identification, including establishing beneficial ownership for all accounts, and situations involving extra due diligence, such as unusual or suspicious transactions.

11. Id.; Preparatory meetings involved representations from the following countries: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, United Arab Emirates and Yemen.
The eleven principles involve:

1. Client acceptance: general guidelines
2. Client acceptance: situations requiring additional diligence/attention
3. Updating client files
4. Practices when identifying unusual or suspicious activities
5. Monitoring
6. Control responsibilities
7. Reporting
8. Education, training and information
9. Record retention requirements
10. Exceptions and deviations
11. Anti-money-laundering organization

2. Statement on the Suppression of the Financing of Terrorism

The Wolfsberg Statement on the Suppression of the Financing of Terrorism describes the role that financial institutions should play in combating terrorist financing, with a view toward enhancing the contribution financial institutions can make toward this international problem. The statement emphasizes that financial institutions need to assist competent authorities in fighting terrorist financing through prevention, detection and information sharing.

This statement provides that “know your customer” (KYC) policies and procedures should be enhanced with searches of lists of known or suspected terrorists. In addition, banks should play an active role in helping governments by applying extra due diligence whenever they see suspicious or irregular activities. Extra due diligence is especially important when customers are engaged in sectors or activities that have been identified by competent authorities as being used for the financing of terrorism. The statement goes on to endorse the need for enhanced global cooperation and adoption of the FATF Special Recommendations.

15. Id., principles 4 and 5.
3. Anti-Money Laundering Principles for Correspondent Banking

The Wolfsberg Group has adopted a set of 14 principles to govern the establishment and maintenance of correspondent banking relationships on a global basis.\textsuperscript{17} The principles prohibit international banks from doing business with “shell banks.”\textsuperscript{18} In addition, the principles use a risk-based approach to correspondent banking that is designed to ascertain the appropriate level of due diligence that a bank should adopt with regard to its correspondent banking clients.

In evaluating prospective risks, the Wolfsberg principles require a correspondent bank to consider the client bank’s:

- Domicile;
- Ownership and management structure;
- Business portfolio, and
- Client base.\textsuperscript{19}

This risk profile is intended to assist the banks in the application of KYC procedures when providing correspondent banking services. The principles also specify the identification and follow-up of unusual or suspicious transactions or activities.

The principles for correspondent banking cover the following topics:

1. Preamble
2. Correspondent Banking
3. Responsibility and Oversight
4. Risk-Based Due Diligence
5. Due Diligence Standards
6. Enhanced Due Diligence
7. Shell Banks
8. Central Banks and Supra-National Organizations
9. Branches, Subsidiaries and Affiliates

\textsuperscript{17} http://www.wolfsberg-principles.com/corresp-banking.html.
\textsuperscript{18} Id., principle 7.
\textsuperscript{19} Id., principle 5.
10. Application to Client Base
11. Updating Client Files
12. Monitoring and Reporting of Suspicious Activities
13. Integration with Anti-Money Laundering Programme
14. Recommendation for an International Registry.

4. Monitoring Screening and Searching

This set of principles identifies issues that should be addressed in order for financial institutions to develop suitable monitoring, screening and searching processes,\textsuperscript{21} using a risk-based profile approach. The principles recognize that the risk profile may be different for a financial institution, as a whole, than for its individual units, depending on the business conducted in a particular unit (e.g., retail, private banking, correspondent banking, broker-dealer). The principles further recognize that any process for monitoring, screening or searching is limited to detecting those clients and transactions that have identifiable characteristics that are distinguishable from apparently legitimate behavior.

Under these principles, financial institutions should have appropriate processes in place that provide for the identification of unusual activity and unusual patterns of activity or transactions. Since unusual transactions, patterns or activity need not be suspicious in all cases, financial institutions must have the ability to analyze and determine if particular activity, patterns and transactions are suspicious in nature with regard to, among other things, potential money laundering.\textsuperscript{22}

The principles encourage the use of a risk-based approach to monitoring activities.\textsuperscript{23} Further, the principles encourage the use of real-time screening or filtering, which involves the examination of the transaction prior to actual execution, whenever there is an embargo or sanction in place.\textsuperscript{24}

\textsuperscript{20}Id., Introduction Index.
\textsuperscript{21}http://www.wolfsberg-principles.com/monitoring.html.
\textsuperscript{22}Id., principle 3.
\textsuperscript{23}Id., principle 4.
\textsuperscript{24}Id., principle 4.1.
Retroactive searches are encouraged based upon the institution’s risk-based approach.

The majority of ongoing monitoring for unusual and potentially suspicious activity should be accomplished by transaction monitoring. Risk-based transaction monitoring for potential money laundering requires the development of risk models that identify the potential risks to money laundering and provide a means of ranking the risks in order to compare the risks to completed transactions. An appropriate transaction monitoring process should compare the transaction information against the identified risks (such as geographic location of transaction, the type of products and services being offered and the type of client engaging in the transaction) with the different typologies for money laundering and other illicit activities to determine if transaction is unusual or suspicious.

C. The Commonwealth Secretariat

The Commonwealth Secretariat is a voluntary association of 53 sovereign states that consult and cooperate in the common interest of their peoples on a broad range of topics, including the promotion of international understanding and world peace. All of the member states, except for Mozambique, have experienced direct or indirect British rule or have been linked administratively to another Commonwealth country.

With regard to AML and CFT, the Commonwealth Secretariat provides assistance to countries to implement The Forty Recommendations and Special Recommendations. It works with national and international organizations and assists governments in the implementation of the FATF recommendations. It is an observer of FATF, CFATF, APG and ESAAMLG.

25. Id., principle 5.
26. Commonwealth countries are: Antigua and Barbuda, Australia, Bangladesh, Barbados, Belize, Botswana, Brunei Darussalam, Cameroon, Canada, Cyprus, Dominica, Fiji Islands, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kiribati, Lesotho, Malawi, Malaysia, Maldives, Malta, Mauritius, Mozambique, Namibia, Nauru, New Zealand, Nigeria, Pakistan, Papua New Guinea, Samoa, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, Sri Lanka, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Swaziland, The Bahamas, The Gambia, Tonga, Trinidad and Tobago, Tuvalu, Uganda, United Kingdom, United Republic of Tanzania, Vanuatu and Zambia. http://www.thecommonwealth.org/.

D. Organization of American States–CICAD

The Organization of American States (OAS) is the regional body for security and diplomacy in the Western Hemisphere. All 35 countries of the Americas have ratified the OAS charter. In 1986, the OAS created the Inter-American Drug Abuse Control Commission (known by its Spanish acronym CICAD) to confront the growing problem of drug-trafficking in the hemisphere. By 1994, the Heads of State and Government of the Western Hemisphere endorsed the role of CICAD to include regional AML efforts. CICAD has developed comprehensive regional strategies and model regulations to combat drug trafficking and use, the proliferation of precursor chemicals and arms trafficking, as well as money laundering.

27. The manual is only available directly from the Commonwealth Secretariat; it is not currently available online.
28. OAS nations are: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, United States, Uruguay, Venezuela, Barbados, Trinidad and Tobago, Jamaica, Grenada, Suriname, Dominica, Saint Lucia, Antigua and Barbuda, Saint Vincent and the Grenadines, The Bahamas, St. Kitts and Nevis, Canada, Belize and Guyana. http://www.oas.org/main/english/.
Chapter V

Legal System Requirements

There are a number of steps that each country needs to take to assure that its anti-money laundering (AML) institutional framework meets international standards. International standard setters recognize that countries have diverse legal systems and, therefore, no country is in a position to adopt specific laws that are identical to those of another country. Specific requirements for combating the financing of terrorism (CFT) are discussed in Chapter IX. Consequently, this chapter discusses eight legal system requirements that concern primarily AML.

These eight requirements are categorized as legal system requirements for purposes of convenient discussion within the context of this Reference Guide. Some of the requirements could, however, just as easily be discussed under different categories. For example, “Supervision and Regulation—Integrity Standards” could be discussed in Chapter VI, “Preventative Measures.” Regardless of how they are categorized, each of these eight legal system requirements is necessary for a country’s legal framework against

<table>
<thead>
<tr>
<th>A. Criminalization of Money Laundering</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Defining the Crime</td>
</tr>
<tr>
<td>2. Scope of the Predicate Offense</td>
</tr>
<tr>
<td>3. Cross Border Considerations for International Cooperation</td>
</tr>
<tr>
<td>4. State of Mind—Knowledge of Intent</td>
</tr>
<tr>
<td>5. Corporate Liability</td>
</tr>
<tr>
<td>6. Predicate Offense Perpetrator Liability</td>
</tr>
<tr>
<td>7. Lawyers’ Fees</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B. Criminalization of Terrorism and the Financing of Terrorism</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>C. Seizure, Confiscation and Forfeiture</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Confiscation of Direct and Indirect Proceeds of Crime</td>
</tr>
<tr>
<td>2. Enforcement of Confiscated/Property</td>
</tr>
<tr>
<td>3. Third Party Liability</td>
</tr>
<tr>
<td>4. International Aspects of Confiscation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D. Types of Covered Entities and Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Financial Institutions</td>
</tr>
<tr>
<td>2. Designated Non-Financial Businesses and Professions</td>
</tr>
<tr>
<td>3. Other Potential Covered Persons and Entities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E. Supervision and Regulation—Integrity Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Financial Institutions</td>
</tr>
<tr>
<td>2. Designated Non-Financial Businesses and Professions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F. Laws Consistent with Implementation of FATF Recommendations</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>G. Cooperation Among Competent Authorities</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>H. Investigations</th>
</tr>
</thead>
</table>
money laundering. Under these principles, each country is permitted to adopt laws that are consistent with its own cultural circumstances, legal precepts and constitution, as well as international standards. They are:

- Criminalization of money laundering in accordance with the Vienna and Palermo Conventions;
- Criminalization of terrorism and terrorist financing;
- Laws for seizure, confiscation and forfeiture and illegal proceeds;
- The types of entities and persons to be covered by AML laws;
- Integrity standards for financial institutions; and
- Consistent laws for implementation of FATF recommendations.
- Cooperation among competent authorities
- Investigations

The legal system requirements for AML, and the other international standards in this Reference Guide, are based upon The Forty Recommendations on Money Laundering (The Forty Recommendations) issued by the Financial Action Task Force on Money Laundering (FATF); countries may also wish to consult the Methodology for AML/CFT for further explanations of these requirements and how they are evaluated. The Forty Recommendations are phrased as recommendations, but are much more than mere suggestions or recommendations. They are mandates for action by every country, not just FATF members, if that country is to be viewed as compliant with international standards. Thus, each FATF recommendation should be considered very carefully by a country in crafting the language of its laws.

A. Criminalization of Money Laundering

The starting place for a country to establish or improve its AML framework is by making money laundering a crime within that country. Criminalization serves three principal objectives. First, it compels compliance with AML preven-

---

tive measures. Second, it ties acts that may appear innocent to outright criminal activity, i.e., the actions of the party processing illegal proceeds are made a criminal act. Third, criminalization establishes a specific basis for greater international cooperation in this critical law enforcement function. Because of the criminal nature and the international aspects of money laundering offenses, competent authorities within a country have recourse to powerful international tools, especially mutual legal assistance mechanisms and, thereby, can more effectively track, enforce, and prosecute international money laundering.

1. Defining the Crime

The criminalization of money laundering should be done in accordance with the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention)\(^2\) and the United Nations Convention against Transnational Organized Crime (2000) (Palermo Convention).\(^3\) The relevant provisions of these conventions are Articles 3 (1) (b) and (c) of the Vienna Convention and Article 6 (1) of the Palermo Convention. Criminalization of money laundering according to those articles is the first recommendation of FATF.\(^4\) Many countries have signed and ratified these conventions, but this is not sufficient to comply with Recommendation 1. Countries must implement domestically the requirements of the relevant Articles.

Although the Vienna Convention is limited in scope to drug trafficking and does not use the term “money laundering,” the three categories of offenses specified in the Vienna Convention form the basis of the money laundering offense. The categories are:

i. the conversion or transfer of property with the knowledge that such property is derived from a drug-trafficking offense for the purpose of concealing and disguising its illicit origin or assisting any person

---

involved in a drug-trafficking offense to evade the legal consequences of his or her actions;\(^5\)

ii. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property with the knowledge that the property was derived from a drug-trafficking offense;\(^6\)

iii. the acquisition, possession, or use of property with the knowledge that the property is derived from a drug-trafficking offense.\(^7\)

According to the Vienna Convention, the first two categories must be incorporated into domestic law; the third offense is not mandatory, but subject to each country’s “constitutional principles and basic concepts of its legal system.”\(^8\)

The Vienna Convention’s definition of money laundering offenses is the most widely accepted and is used in all current international legal instruments on this topic.\(^9\) Using the Vienna Convention’s definition, the Palermo Convention expands the money laundering definition to:

a. when committed intentionally:
   i. the conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of his or her action;
   ii. the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

b. subject to the basic concepts of its legal system:
   i. the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

---

5. Vienna Convention, article 3(1)(b)(i).
6. Id., article 3(1)(b)(ii).
7. Id., article (3)(c)(i).
8. Id.
9. See also Chapter III, the United Nations, the Vienna Convention.
ii. Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the offenses established in accordance with this article.10


2. Scope of the Predicate Offense

a. Widest Possible Range of Offenses to be Included as Predicate Offenses

A predicate offense for money laundering is the underlying criminal activity that generates proceeds, which when laundered, leads to the offense of money

---

10. Palermo Convention, article 6 (1).
Designating certain criminal activities as predicate offenses for money laundering is necessary to comply with international standards. The designation of an increasingly wider range of criminal offenses as money laundering predicates has occurred as international standards have developed.

The first international effort against money laundering was contained in the Vienna Convention. However, the Vienna Convention is an international drug control instrument and the predicate offenses for money laundering relate only to drug trafficking offenses. The Palermo Convention imposes an obligation on all State parties to apply the Convention’s money laundering offenses to “the widest range of predicate offenses.” Recommendation 4 of the 1996 version of the FATF 40 Recommendations specified that predicate offenses should be “based on serious offenses.” However, neither the Palermo Convention nor the 1996 version of the 40 Recommendations defined in any detail what constituted the “widest range” of predicate offenses or “serious offenses.” Thus, the scope of the predicate offense was left to the judgment of each country, subject only to the Vienna Convention’s requirement that drug trafficking should be a predicate offense.

The scope of predicate offenses used in the current version of The Forty Recommendations is much more widely based. Recommendation 1, which is quite lengthy, begins by repeating the previous language of the Palermo Convention and the 1996 version of the 40 Recommendations that countries should apply the crime of money laundering to all serious offenses, with a view to including the widest range of offenses as money laundering predicate offenses. After setting out the various methods of describing predicate offenses (see below) the recommendation states that, (as a minimum), countries must include “a range of offenses within each of the designated categories of offenses.”

There are 20 designated categories of offenses:

- Participation in an organized criminal group and racketeering;
- Terrorism, including terrorism financing;

---

17. See Palermo Convention, article 2(h); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 1(e).
18. Vienna Convention, article 3.
19. Palermo Convention, article 2(a).
21. Id.
22. Id., Rec. 1.
Legal System Requirements

- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint and hostage taking;
- Robbery or theft;
- Smuggling;
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.23

There are two further important points concerning the description of predicate offenses. First, the requirement is to include “a range of offenses” within each of the designated categories of offenses. For example, a country would not comply with this recommendation if under “robbery or theft” it designated only the proceeds of “vehicle theft” as a money laundering predicate offense and excluded the proceeds of thefts of other goods. Second, countries are provided with discretion on how to define the offenses in the above list and the nature of any particular elements of those offenses that make them money laundering predicate offenses.

The essential requirement is to criminalize the proceeds from the type of conduct described in the above list. Furthermore, it is not necessary to have an offense in the penal code described in exactly the terms that are used in the above list. For example, some countries do not have a specific offense designated as “fraud,” but criminalize fraudulent behavior under some other

23. See the definition of “designated category of offences” in the Glossary of The Forty Recommendations.
offense, such as “theft.” Provided that it is possible to obtain a conviction for laundering the proceeds of fraudulent behavior, the country has discretion in terms of how to describe or categorize the conduct of that behavior.

The one exception to this discretion is terrorist financing. Under the nine Special Recommendations on Terrorist Financing (Special Recommendations) FATF specifically requires that the financing of terrorism, terrorist acts and terrorist organizations should be designated as money laundering predicate offenses.24 It is not acceptable to criminalize these activities solely on the basis of legislation against aiding and abetting, attempting or conspiracy.

b. Methods of Describing Predicate Offenses

FATF describes the types or categories of criminal conduct that should be money laundering predicate offenses, but each individual country has the discretion to determine the specific legal method of criminalization. This can be accomplished by reference to:

- All offenses;
- A threshold linked either to a category of serious offenses or to the penalty of imprisonment applicable to the predicate offense (threshold approach);
- A list of predicate offenses; or
- A combination of these approaches.

Where countries apply a threshold approach, predicate offenses must, at a minimum, cover all offenses that are designated “serious offenses” under national law or offenses punishable by a maximum penalty of more than one year's imprisonment (for countries with minimum penalties, more than six months). Examples of categories of serious offenses, include “indictable offenses” (as opposed to summary offenses), “felonies” (as opposed to misdemeanors), and “crimes” (as opposed to delits). It should be noted that

countries using the threshold approach for designated predicate offenses are subject to two additional minimum requirements, which are not alternatives:

- The threshold must cover all 20 designated categories of offenses (see above); and
- All serious offenses or all offenses with a maximum period of imprisonment exceeding one year (six months for countries applying minimum thresholds)

This means that any offense that is not on the designated categories of offenses list, but that is defined by the country as a “serious offense” or punished by a maximum prison term exceeding one year would also have to be designated as a money laundering predicate offense by that country.

3. Cross Border Considerations for International Cooperation

As noted above, the FATF recommendations establish a minimum category of offenses that must be predicate offenses for money laundering, but encourage countries to go beyond this. How far beyond the minimum and the method of criminalization is left to the discretion of each country. The extent to which a country does so, however, has implications for that country’s ability to cooperate internationally and exchange information with other national authorities.

Recommendation 1 provides that predicate offenses should extend to conduct that occurred in another country, which constitutes an offense in that country, and which would have constituted an offense if it had occurred domestically. This is the so-called “dual criminality” test, under which the conduct committed in the other country must be a predicate offense both in the other country and domestically. This is, however, the minimum standard. This recommendation also states that countries may provide that the only condition for prosecuting money laundering is that the conduct committed in the other country would have constituted a predicate offense had it occurred domestically.

---

26. Id.
domestically. This approach would allow for prosecution where the proceeds were generated by conduct that was not a predicate offense in the country where the conduct was committed, but was an offense in the country where the proceeds were laundered.

While FATF does not necessarily encourage countries to adopt this latter approach, FATF does encourage countries to provide mutual legal assistance even if dual criminality is absent.

FATF also provides that where dual criminality is required for mutual legal assistance or extradition, that requirement should be regarded as satisfied regardless of whether the offenses are described under the same category in the different countries, provided both countries criminalize the underlying conduct. For example, if country A requests assistance from country B with respect to laundering the proceeds of fraud and country B has no specific offense of fraud, country B should provide assistance if it criminalizes fraudulent conduct under some other offense (e.g., theft).

4. State of Mind—Knowledge and Intent

According to the Vienna Convention, the perpetrator’s state of mind—his or her intent or purpose in committing the money laundering offense—means “knowing” that the proceeds are the product of the predicate offense. Countries may extend the scope of liability, however, to “negligent money laundering,” where the perpetrator should have known that the property was, or was obtained with, the proceeds of a criminal act.

Countries have various options in determining the “state of mind” connected with a money-laundering offense. The legislature of a country may decide that actual knowledge about the illicit origin of property, or that mere suspicion about that illicit origin, constitutes the requisite state of mind or mental element for obtaining convictions for money laundering. The legislature may also accept a “should have known” standard of culpability. This latter definition constitutes a form of negligent money

29. Vienna Convention, article 3(b)(i).
laundering. In addition to this general intent requirement, the law might provide for a specific intent to “conceal or disguise the illicit origin” of the property, or the intent to help another “evade the legal consequences of his or her actions.”

According to the UN Model Legislation, actual knowledge, or “having reason to believe,” that property is derived from criminal acts, constitutes the so-called mental element of money laundering. The Model Bill envisages, however, that specific intent may apply to certain money-laundering offenses, such as concealing or disguising the origin, nature, location, disposition, movement, or ownership of the property. Also, certain money-laundering offenses could require proving the specific intent of an individual to assist another, for example, in evading the legal consequences of his or her actions.

A broad definition of the “state of mind” was adopted in the OAS Model Regulations. These model regulations address three different states of mind: (i) the accused had knowledge that the property constitutes proceeds of a criminal activity as defined in the convention; (ii) the accused should have known that the property was obtained with the proceeds of criminal activity; and (iii) the accused was intentionally ignorant of the nature of the proceeds. Under this third category of state of mind, the accused neither “did not know” nor “should have known” the source of the proceeds, but nevertheless suspected its criminal provenance and chose not to conduct further investigation to verify or dispel this suspicion. In that sense, the accused intended to remain ignorant of the nature of proceeds or was “willfully blind” when he or she “could have known” of the criminal offense by investigation or inquiry. In terms of culpability, this state of mind standard falls between the negligence and specific knowledge standard of intent. The OAS Model Regulations further provide that these three culpable states of mind can be inferred from objective and factual circumstances.

32. Id., at subparagraph (a).
33. UN Model Crime Bill, at Section 17(a).
34. Id., at subparagraph (b).
35. OAS Model Regulations.
36. OAS Model Regulations, Article 2.
37. Id., at subparagraph (5).
Finally, it may be very difficult to prove the state of mind of a person engaging in an activity that otherwise appears to be ordinary on its face. Thus, the Vienna Convention, the Palermo Convention, the Forty Recommendations and many of the other legal instruments provide that the law should permit the inference of the required state of mind from objective factual circumstances. If the objective factual circumstances fit the situation, the state of mind requirement is satisfied.

5. Corporate Liability

Money laundering often takes place through corporate entities. The concept of corporate criminal liability, however, varies greatly among different countries. Some countries, mainly those with a common law tradition, subject corporations to criminal liability laws. In countries with a tradition of civil law, corporations may not be covered by criminal laws. Thus, consideration should be given to modifying such a country’s laws to provide for corporate criminal liability where permissible.

FATF recommends that corporations, not only their employees, be subject to criminal liability whenever possible under the general principles of a country’s legal system. Significant civil or administrative sanctions could be a sufficient substitute in cases where the legal or constitutional framework does not subject corporations to criminal liability.

The UN Model Legislation does not provide for criminal liability for corporations. It does provide, however, for applying other sanctions to corporate entities and for applying them whenever money laundering offenses are committed on behalf of, or for the benefit of, a corporation by one of the corporation’s agents or representatives. The sanctions envisioned by the UN Model Legislation include fines, bans on carrying out certain business activities, closure or winding up, and the publication of rulings. The UN Model Legislation does not categorize these as criminal sanctions and it specifically
provides that these should not derogate from the personal liability of the agent or the employee of the corporation for the acts.42

Criminal liability is extended to corporate entities on the same basis as natural persons in the OAS Model Regulations. In fact, one provision specifically defines a “person” for the purposes of the regulation as meaning “any entity, natural or juridical, including among others a corporation, partnership, trust or estate, joint stock company, association, syndicate, joint venture, or other unincorporated organization or group, capable of acquiring rights or entering into obligations.”43 In the UN Model Crime Bill, the term, “person” is defined to include both natural and legal persons.44 While this language defines “person” more narrowly than that of the OAS, it still acknowledges the principle of criminal liability for corporations.

6. Predicate Offense Perpetrator Liability for Laundering

An important question is whether money laundering liability extends to the person who committed the predicate offense, as well as to the person who has laundered the ill-gotten proceeds. Some countries do not hold the perpetrator of the predicate offense liable for laundering the proceeds of his or her criminal actions, if he or she is not involved in the laundering activity. The basic rationale for this approach is that punishing the perpetrator for evading the legal consequences of his or her criminal activity could amount to double jeopardy, i.e., multiple punishments for a single criminal offense.

Other countries hold the perpetrator of the predicate offense liable for laundering the ill-gotten proceeds on the basis that the conduct and the harm of evasion are distinct from the predicate offense. There are also practical reasons for this approach. Exempting perpetrators of predicate offenses from money-laundering liability could severely penalize third parties for their conduct in handling criminal proceeds, while perpetrators remain immune from liability. This could occur when the predicate offense has been committed extraterritorially, placing it beyond the jurisdiction of the state prosecuting third parties for their laundering activities.

42. Id.
43. OAS Model Regulations, Article 1(6).
44. Section 2(l).
Overall, the general international standard in this area provides for a broad laundering offense that permits the perpetrator to be liable for laundering the proceeds of his or her own criminal activities regardless of active participation in laundering activities. This standard, however, also permits national variations to be employed in this regard.

7. Lawyers’ Fees

Lawyers are now included in the list of designated non-financial businesses and professions that must be considered as covered by AML/CFT regimes. This deserves special attention in the drafting of predicate offenses.

Predicate offenses for money laundering can be defined in legislation so broadly that, in their totality, they include any transaction involving the use of the proceeds derived from a criminal activity. Given such a broad interpretive construction, these laws could have the effect of criminalizing the mere receipt of a fee by a lawyer for the purpose of providing criminal defense. This poses unique problems of due process.

Considering that the right of the accused to adequate defense in criminal trials is now established as one aspect of the right to a fair trial, countries should be careful in drafting the scope of the money laundering offenses.

Countries may also wish to consider an effective provision excluding lawyers from such potential criminal liability for merely rendering their services, provided that the services were limited to, or were rendered only in connection with, defending the accused at trial.

Notwithstanding the right of an accused to a fair trial, lawyers also have a duty regarding the integrity of the financial system and integrity of their profession. If a lawyer has knowledge that his or her fees were derived from a criminal activity, the attorney should observe these integrity standards and

---

45. United Nations Convention against Transnational Organized Crime (2000), article 6(2)(f); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 6(2)(b); UN Model Legislation, Article 1.1.1; UN Model Crime Bill, Sec. 17; OAS-Model Regulations, Article 2.
46. See this Chapter, Designated Non-Financial Businesses and Professions.
47. Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime: Explanatory Report, para. 33. The model laws and regulations in this area are silent on this point. See UN Model Legislation; UN Model Crime Bill; OAS Model Regulations.
not blindly accept laundered money, especially if he or she is also rendering other services to the client besides defending the accused in a trial.

**B. Criminalization of Terrorism and the Financing of Terrorism**

Those who finance terrorism, like other criminals, may use the national and international financial systems to hide the funds they need to support their activities, even if these funds have legitimate sources. Criminalizing all aspects of terrorism and terrorist financing is a practical way to undermine the capacity of terrorist organizations by preventing their funds from entering the financial system. In addition, a country needs legislation to help detect when terrorist funds are within its borders so that the funds can be confiscated and forfeited. This further helps thwart terrorist efforts.

In its nine *Special Recommendations on Terrorist Financing (Special Recommendations)*, FATF urges countries to criminalize the financing of terrorism, terrorist acts and terrorist organizations and to designate these as predicate offenses of money laundering.48

As noted above in “Scope of the Predicate Offense,” FATF provides that one of the designated categories of offenses is terrorism, including terrorist financing.49 Thus, taking *The Forty Recommendations* and the *Special Recommendations* together, terrorism, terrorist acts, terrorist organizations and terrorist financing each should be deemed a predicate offense for a country’s money laundering laws.

**C. Seizure, Confiscation, and Forfeiture**

The current approaches to international crime and terrorist financing are designed to make criminal activities unprofitable and keep terrorists from accessing funds. These goals cannot be achieved without effective confiscation

---

49. *The Forty Recommendations*, Glossary, Designated categories of offenses; and *Special Recommendations*, Spec. Rec. II.
laws, whereby authorities may permanently deprive criminals and terrorists of their ill-gotten proceeds.\footnote{50. Vienna Convention, article 1(f), Council of Europe Convention, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 1(d).}

1. Confiscation of Direct and Indirect Proceeds of Crime

FATF encourages countries to adopt laws permitting a broad interpretation of the confiscation of proceeds of crime, in accordance with the Vienna and Palermo Conventions.\footnote{51. The Forty Recommendations, Rec.3.} In the past under most legal systems, confiscation has largely been confined to the instruments used in the commission of the crime, such as the murder weapon, or the subjects of the crime, such as drugs in drug trafficking, as opposed to the proceeds derived from the crime. The Vienna Convention and the Palermo Convention define the term, “proceeds of crime,” as “any property derived from or obtained, directly or indirectly, through the commission of an offense.”\footnote{52. Vienna Convention, article 1(p); Palermo Convention, article 2(e).} Many countries have now adopted this broader understanding of forfeitable property in response to the profits generated by certain criminal activities, particularly in light of the fungibility of these profits and the ease with which funds can be moved into, and out of, the international financial system.

FATF encourages countries to adopt laws that permit the confiscation of the laundered property, the proceeds of laundering and predicate offenses, the instrumentalities used, or intended for use in, laundering, and property of corresponding value.\footnote{53. The Forty Recommendations, Rec. 3.} This broad definition is useful since criminals are likely to convert property to some other form if only specifically-named property is subject to confiscation prior to the issuance of the confiscation order or its enforcement. Criminals are also likely to transfer the property beyond the reach of authorities or to commingle it with property legitimately derived. In order to address these various situations, which under a traditional understanding of confiscation could render confiscation orders useless, governments should consider adopting the “value confiscation” approach, which gives
the government the power to confiscate any property of the perpetrator of a value equivalent to the value of the ill-gotten proceeds.54

2. Enforcement of Confiscated Property

The effective enforcement of confiscation orders requires that the relevant authorities possess the powers necessary to identify, trace and evaluate property that could be subject to confiscation.55 This in turn requires that such authorities have the power to require disclosure or to seize commercial and financial records.56 FATF specifically recommends that banking secrecy laws, or other privacy protection statutes, for example, should be designed so that they do not create barriers to such disclosure or seizure for these purposes.57

Today, funds can now be transferred out of a national jurisdiction with a keystroke on a computer. Thus, authorities should also be granted the power to take preventive measures. For example, they should be able to freeze and seize assets that might be subject to confiscation. This power is a necessary condition for an effective law enforcement framework for preventing the laundering of money.58 (See Chapter IX, Freezing and Confiscating Terrorist Assets for a detailed discussion of freezing, seizing and confiscating assets. That discussion is equally applicable to AML-related assets.)

3. Third Party Liability

While international law on confiscation does not preclude the confiscation of assets in the hands of third parties, FATF and various international agreements qualify the permissibility of such action by requiring countries to take

---

54. Vienna Convention, article 5; Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 2.
55. The Forty Recommendations, Rec. 3.
56. Vienna Convention, article 5(3); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 4(1).
57. The Forty Recommendations, Rec. 4; Vienna Convention, article 5(3); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 4(1).
58. The Forty Recommendations, Rec. 3; Vienna Convention, article 5(2); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 3.
measures to protect the rights of *bona fide* third parties.\(^{59}\) Third parties that enter into an agreement, and either know or should know that the contract would prejudice the capacity of the state to enforce its confiscation are not *bona fide*. A country’s laws should address specially the issue of validity of such agreements under such circumstances.\(^{60}\)

According to the OAS Model Regulations, the relevant authority is required to give notification of the proceedings.\(^{61}\) The notification must allow potential third parties to make claims to the property subject to confiscation. According to the model regulations, the court or other competent authority should return the property to the claimant, if it is satisfied that the claimant: (1) has proper legal title to the property; (2) did not participate in, collude with, or was not in any other way involved in the predicate offense; (3) did not have knowledge of the use of property for illegal purposes and did not consent freely to this use; (4) did not acquire rights that were specifically designed to evade the confiscation proceedings; and (5) did whatever could reasonably be expected to prevent the illegal use of the property.

In addressing the question of *bona fide* third parties, the UN Model Crime Bill provides that the court can deny the third-party claim to the property in cases where the court finds that the person (1) was involved in the commission of the predicate offense; (2) acquired the property for insufficient consideration; or (3) acquired the property knowing its illicit origin.\(^{62}\) By comparison, the UN Model Legislation uses a more strict standard, which does not require involvement in the predicate offense as a basis for denying the claim to the property.\(^{63}\)

4. International Aspects of Confiscation

Establishing an effective confiscation regime for domestic purposes is only the first step toward eliminating the profitability at the heart of so many interna-

\(^{59}\) *The Forty Recommendations*, Rec. 3; *The Vienna Convention*, article 5(8); *Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime* (1990), article 5; *The Palermo Convention*, article 12(8).

\(^{60}\) *The Forty Recommendations*, Rec. 3.

\(^{61}\) OAS Model Regulations, Article 6.4.

\(^{62}\) UN Model Crime Bill, Section 36. This is a model law designed for common law jurisdictions.

\(^{63}\) See UN Model Legislation, Article 4.2.9. This is a model Law designed for civil law jurisdictions.
tional money laundering activities. The second necessary step, and one vital to the overall success of this effort, is creating cooperative mechanisms for enforcing cross-border confiscation orders. Countries may enable the relevant authorities to implement confiscation requests from other countries, employing such measures as tracing, identification, freezing, and seizure.

As an incentive for international cooperation, countries may consider establishing asset-sharing arrangements. The general principle in the disposal of confiscated assets is that such disposal be subject to the domestic laws and regulations of the country that executed the confiscation order. The international legal instruments, however, encourage countries to enter into mutual arrangements that provide for the sharing of the confiscated property among all the countries that cooperated in the investigation and confiscation process. The legal instruments also encourage allocating some of the confiscated funds to the intergovernmental agencies that are dedicated to the fight against crime.

D. Types of Covered Entities and Persons

FATF recommendations impose numerous requirements upon financial institutions and non-financial businesses and professions to prevent money laundering and terrorist financing. Moreover, the recommendations provide exceptions in applying these preventative measures. Thus, a crucial decision for a country is to determine which entities and persons should be covered by which requirements. In this regard, all of the preventative measures apply to "financial institutions," while certain of the preventive measures apply to certain "designated non-financial businesses and professions" on a more limited basis.

64. Vienna Convention, article 5(a); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 15; The Palermo Convention, article 14(1).
65. Vienna Convention, article 5(b); The Palermo Convention, article 14(3)(b); OAS-Model Regulations, article 7(d).
66. Vienna Convention, article 5(b)(i); The Palermo Convention (2000), article 14(3)(a); OAS Model Regulations, article 7(e).
67. The Forty Recommendations, see generally Recs. 5–25.
68. Id.
1. Financial Institutions

It is axiomatic that money launderers and those who finance terrorism must have access to financial institutions. These institutions provide the means for such individuals to transfer funds among other financial institutions, both domestically and internationally. These institutions also provide the means to convert currencies and pay for the assets used in the money laundering and terrorist financing process. The types of financial institutions and their capabilities vary greatly among different countries. Under FATF recommendations, the term, “financial institutions,” is defined as “any person or entity who conducts as a business one or more of the following activities, or operations on behalf of a customer”:

- Acceptance of deposits and other repayable funds from the public (including private banking);
- Lending (including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting);
- Financial leasing (but excluding financial leasing for consumer products);
- The transfer of money or value\(^{69}\) (including formal and informal sectors, such as alternative remittance activity);
- Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveler’s cheques, money orders and banker’s drafts, electronic money);
- Financial guarantees and commitments;
- Trading in:
  a. money market instruments (cheques, bills, CDs derivatives, etc);
  b. foreign exchange;
  c. exchange, interest rate and index instruments;
  d. transferable securities;
  e. commodity futures trading;
- Participation in securities issues and the provision of financial services related to such issues;
- Individual and collective portfolio management;

\(^{69}\) See also interpretive note to The Special Recommendations, Spec. Rec. VI and VII.
• Safekeeping and administration of cash or liquid securities on behalf of other persons;
• Otherwise investing, administering or managing funds or money on behalf of other persons;
• Underwriting and placement of life insurance and other investment related insurance (this applies to both insurance undertakings and intermediaries, such as agents and brokers); and
• Money and currency changing. 70

This is a functional definition rather than an institutional or designation one. The test is whether an entity or individual carries out any of the above functions or activities for customers, not what the business is called or how the business is designated. For example, any person or business that accepts deposits and/or makes loans to the public is covered, regardless of whether the person or business is called a bank. In many cases, law or regulation will limit the conduct of such activities to licensed financial institutions and, in those situations, countries that apply AML/CFT controls to licensed financial institutions would satisfy the standard. On the other hand, if such activities can be carried out legally by unlicensed entities, the AML/CFT controls should apply to these entities as well.

There are two qualifications to this requirement. First, if a financial activity, described above, is carried out occasionally or on a very limited basis, such that there is little money laundering risk, a country may decide not to apply all, or indeed any, money laundering requirements. 71 A possible example of such a case might be a hotel, which offers very limited foreign currency exchange facilities to its guests on an occasional basis or a travel agency which can wire money to clients overseas in emergencies.

A second qualification is that in “strictly limited and justified circumstances” and when there is “a proven low risk of money laundering” a country may decide not to apply some or all of The Forty Recommendations to the above list of financial activities. 72 The FATF does not offer clear guidance as to what those circumstances might be. However, countries are encouraged to adopt a risk-based approach, which may lead to increased measures

70. The Forty Recommendations, Glossary, Financial Institutions.
71. Id.
72. Id.
in high-risk areas, or in strictly limited and justified circumstances, may lead to lesser measures based on a proven low AML/CFT risk. Financial activity should only be excluded or subject to limited controls generally after a proper study has established that the money laundering risk is low. The starting presumption should be that all of the above financial activities should be subject to all of the AML requirements.

2. Designated Non-Financial Business and Professions

The FATF recommendations were revised in 2003 to include certain designated non-financial businesses and professions within coverage of The Forty Recommendations for the first time. The requirements applicable to these entities and professionals are more limited and apply in more limited circumstances than financial institutions. Details of what requirements apply to which non-financial businesses and professions are described in Chapter VI, but countries are required to bring the following entities and persons within coverage of certain AML/CFT provisions:

- Casinos (which also includes internet casinos);
- Real estate agents;
- Dealers in precious metals;
- Dealers in precious stones;
- Lawyers, notaries, other independent legal professionals, and accountants which refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering;
- Trust and company service providers, which refers to all persons or businesses that are not covered elsewhere under these recommendations, and which as a business, provide any of the following services to third parties:
a. Acting as a formation agent of legal persons;
b. Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
c. Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
d. Acting as (or arranging for another person to act as) a trustee of an express trust; or
e. Acting as (or arranging for another person to act as) a nominee shareholder for another person.73

3. Other Potential Covered Entities and Persons

Finally, in a separate, and all-embracing recommendation, FATF states that countries should consider applying the recommendations to businesses and professions, other than those listed above, that pose a money laundering or terrorist financing risk.74 It is a matter for each country to consider which businesses or professions would be included and to determine what is the appropriate response to the risk. Examples could include dealers in high value and luxury goods (antiques, automobiles, boats, etc.), pawnshops, auction houses and investment advisers. There is no requirement to cover any or all of this list of any other but there is a requirement to consider the risks and appropriate response to such risks.

E. Supervision and Regulation—Integrity Standards

Money cannot be laundered, nor terrorism financed, without the involvement of financial institutions, certain business entities and certain persons. When criminals control financial institutions or hold senior management positions in financial institutions, countries find it exceedingly difficult to prevent and

73. The Forty Recommendations, Glossary, Designated Non-Financial Businesses and Professions.
74. Id., Rec. 20.
detect money laundering. Similarly, when certain persons are involved with money laundering actions, countries find prevention and detection more difficult. Integrity and licensing requirements help prevent such entities and individuals from participation in money laundering and terrorist financing efforts.

1. Financial Institutions

a. Core Principles Institutions

These institutions, i.e., banks, insurance companies, securities industry, are subject to comprehensive supervisory regimes as set out in the standards issued by the Basle Committee on Banking Supervision, International Association of Insurance Supervisors, and International Organization of Securities Commissions, respectively.75 The provisions include requirements for:

- Licensing and authorization to engage in business;
- Evaluation (fit and proper determination) of directors and senior managers, with regard to integrity, expertise and experience;
- Prohibitions against participation by directors and managers with criminal records or adverse regulatory findings; and
- Prohibitions against ownership or control by those with criminal records.

These requirements should apply both for prudential purposes and for purposes of AML/CFT controls, and supervision includes the authority to compel the production of records and information for determining compliance.76

b. Other Financial Institutions

These institutions are not normally subject to the same stringent requirements as Core Principles Institutions (largely because the same prudential issues do not arise). For example, directors and senior management are not evaluated

75. See Chapter IV.
76. The Forty Recommendations, Rec. 23.
as to their “fit and proper” standing in relation to their integrity, expertise and experience. For AML/CFT purposes, the minimum requirements for these other financial institutions are as follows:

- Such institutions should be licensed or registered;
- They should be subject to supervision or oversight for AML purposes according to the risk of money laundering and terrorist financing in the that sector.77

This imposes a licensing or registration requirement with respect to all of those “other financial institutions,” but allows each country discretion over the extent to which there should be oversight of their implementation of AML/CFT measures. In some cases, the oversight could be limited to law enforcement action against institutions that do not comply with applicable regulations, but no proactive inspection or oversight of compliance.

However, for money transfer and exchange businesses, the FATF requires that, as well, as licensing or registration, there should be “effective systems” for monitoring and ensuring compliance.78 What constitutes an effective system in practice is not described further in the recommendation, but the implication is that the requirement goes beyond law enforcement action against non-compliant institutions.

2. Designated Non-Financial Businesses and Professions

Non-financial businesses and professions fall into two categories: casinos and all other non-financial businesses and professions (other NFBPs).

For casinos, there are strict requirements involving:

- Licensing;
- Measures to prevent casinos being owned, controlled or operated by criminals; and
- Supervision of their compliance with AML/CFT requirements.

---

77. Id.
78. Id.
For all other NFBPs, the requirement is that effective systems for monitoring and ensuring compliance on a risk-sensitive basis are in place. The monitoring may be carried out either by a government agency or a self-regulatory organization. Unlike other financial institutions (see above), there is no licensing or registration system.

F. Laws Consistent with Implementation of FATF Recommendations

A crucial aspect of any legal system is to have laws and regulations that are internally consistent and work in coordination with each other. Thus, it is important that one law not conflict with another law, unless there is a basis in policy for making an exception, and that the two laws can be read as working together without contradiction.

One area where there is potential for conflict is with secrecy laws. Often, countries have general laws protecting the privacy of financial information from disclosure. Such laws may conflict with the specific requirement, for example, that financial institutions report suspicious transactions.79

In order to effectuate AML/CFT requirements, FATF provides that each country should make sure that its financial institution secrecy laws do not inhibit implementation of the FATF recommendations.80

G. Cooperation Among Competent Authorities

Each country needs to provide that there are effective mechanisms in place to enable its policy makers, FIU, law enforcement authorities (including customs where appropriate), financial institution supervisors and other relevant authorities to cooperate with each other.81 If appropriate under the country’s laws and enforcement system, this requirement extends to coordinating the development and implementation of policies and activities to combat money laundering and terrorist financing.

---

80. Id., Rec. 4.
81. Id., Rec. 31.
Ideally, this recommendations means that a country’s laws and mechanisms should be viewed as facilitating cooperation among the various competent authorities, as well as facilitating coordination among such authorities, involved in AML and CFT efforts. Most importantly, a country’s laws and mechanisms should not be viewed as prohibiting or restricting such cooperative efforts.

H. Investigations

Each country should assure that designated law enforcement authorities are responsible for money laundering and terrorist financing investigations.82 In the effort to utilize investigations to the fullest extent in the fight against money laundering and terrorist financing, FATF encourages countries to authorize, support and develop special investigative techniques and mechanisms, such as undercover operations, specialized asset investigations and cooperative investigations with other countries.83

Investigative endeavors, as with all competent authorities involved in the fight against money laundering and terrorist financing in a country, should receive adequate financial, staffing and technical resources, including staff that meet high integrity standards.84

Finally, the effectiveness of a country’s AML/CFT regime depends upon useful information. Thus, each country should maintain statistics on the effectiveness and efficiency of its investigations and other aspects of its regime.85

82. Id., Rec. 27.
83. Id.
84. Id., Rec. 30.
85. Id., Rec. 32.
Money launderers and those who finance terrorism use various types of financial institutions and certain non-financial businesses and professionals to help in their criminal activities. In fact, access to such entities and persons is crucial if criminals are to succeed because financial institutions, and other, provide the means to transfer funds to other financial institutions, both domestically and internationally; to exchange currencies, and to convert proceeds of crime into different financial instruments and other assets.

In *The Forty Recommendations on Money Laundering (The Forty Recommendations)*, the Financial Action Task Force on Money Laundering (FATF) has established a number of preventative measures that a country should adopt in the anti-money laundering (AML) area. These preventative

---

measures are applicable to all financial institutions and, on a more limited basis, to designated non-financial businesses and professions. Furthermore, these preventative AML measures are equally applicable in combating the financing of terrorism (CFT) under FATF's Special Recommendations on Terrorist Financing (Special Recommendations).²

Like all of The Forty Recommendations, the preventative measures, generally recommendations 5–25, are not recommendations, but mandates for action by a country if that country wishes to be viewed as compliant with international standards in AML and CFT. These mandates for action are also flexible, however, to permit a country to adopt requirements that are consistent with its own economic circumstances, legal system and constitution. Countries may also wish to examine the Methodology for Assessing Compliance with The Forty and Special Recommendations for further explanation of the requirements.³

A. Customer Identification and Due Diligence

In accordance with international standards set by the Basel Committee on Banking Supervision (Basel Committee)⁴ and by FATF⁵ countries must assure that their financial institutions have appropriate customer identification and due diligence procedures in place. These procedures apply to a financial institution's individual and corporate customers alike. These rules or procedures ensure that financial institutions maintain adequate knowledge about their customers and their customers’ financial activities. Customer

---

³ http://www.fatf-gafi.org/pdf/Meth-2004_en.PDF.
identification requirements are also known as “know your customer” (KYC) rules, a term employed by the Basel Committee.  

KYC policies not only help financial institutions detect, deter, and prevent money laundering and terrorist financing, they also confer tangible benefits on the financial institution, its law-abiding customers, and the financial system as a whole. In particular, KYC practices:

- Promote good business, governance, and risk management among financial institutions;
- Help maintain the integrity of the financial system and enable development efforts in emerging markets;
- Reduce the incidence of fraud and other financial crime; and
- Protect the reputation of the financial organization against the detrimental effect of association with criminals.

1. Scope of Customer Identification and Due Diligence

The customer identification and due diligence procedures employed by a financial institution must also apply to its branches and majority-owned subsidiaries—both domestically and internationally—provided local law is not in conflict. Where local law prohibits implementation, relevant authorities in the home country should be informed that these procedures cannot be applied by their host country institutions. Host country supervisors should make efforts to change such laws and regulations in the local jurisdiction. Absent any legal restrictions in the host country, when two different levels of

6. Basel Committee, Core Principle for Effective Banking Supervision, Principle 15 states, “Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.”

7. Basel Customer Due Diligence for Banks states: “Supervisors around the world are increasingly recognizing the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls.” http://www.bis.org/publ/bcbs85.pdf.


10. Id.
regulatory standards exist between the home and host country, the higher or more comprehensive, of the two standards should be applied.\textsuperscript{11}

2. Who Is a Customer

The Basel Committee defines a customer as:

- A person or entity who maintains an account with a financial institution or on whose behalf an account is maintained (i.e., beneficial owners);
- Beneficiaries of transactions conducted by professional intermediaries (e.g., agents, accountants, lawyers); and
- A person or entity connected with a financial transaction who can pose a significant risk to the bank.\textsuperscript{12}

A crucial aspect of customer identification is establishing whether the customer is acting on his, her or its own behalf, or whether there is a beneficial owner of the account that may not be identified in the documents maintained by the financial institution. If there is any reason to suspect that the customer is acting on behalf of another person or entity, appropriate due diligence measures should be instituted.

Beneficial ownership is also difficult in the case of legal entities or corporations where there is tiered ownership involved. Tiered ownership involves one corporation owning or controlling one or more other corporate entities. In some cases, there can be numerous corporations each, in turn, owned by another corporation and, ultimately, owned or controlled by a parent corporation. When corporations or legal entities are involved, appropriate due diligence measures should be employed to determine the identity of the actual parent or controlling entity.

\textsuperscript{11} Basel Customer Due Diligence for Banks (provision 66).
\textsuperscript{12} Id. (provision 21).
3. Customer Acceptance and Identification Procedures

Financial institutions should develop and enforce clear customer acceptance and identification procedures for clients and those acting on behalf of clients. These procedures should include the development of high-risk-customer profiles. Such profiles would include standard risk indicators such as personal background, country of origin, possession of a public or high-profile position, linked accounts, and type and nature of business activity.

When crafting customer acceptance policies, financial institutions must take great care to strike the appropriate balance between risk aversion regarding criminal activities and the willingness to take on new clients. As a general rule, the rigidity of the acceptance standards should be commensurate with the risk profile of a potential customer. It is strongly recommended that only senior management should render decisions on customers whose profiles suggest they pose a high risk of money-laundering activities.

Financial institutions should design their customer acceptance policies so that the socially disadvantaged are not excluded. Nor should these customer acceptance policies in any way restrict the general public’s access to financial services. This is particularly important for countries moving toward a broader use of financial instruments, including the use of checks, credit or debit cards, electronic and other payment mechanisms, and shifting away from a cash-based economy.

Accounts should be opened only after the new customer’s identity has been satisfactorily verified. No customer should be permitted to open or maintain an account using an anonymous or fictitious name. This prohibition also applies to a numbered account if that account is accessed by use of a number or code once the account does not require the customer identification procedures using official documentation. Numbered accounts are only permitted when the same customer identification procedures and supporting documentation (with record keeping) are employed. Under these guidelines,

---

13. Id. (provision 20).
14. Id.
15. Id.
16. Id.
19. Id.
financial institutions must check and verify their customers’ official identifying document. The best documents for verifying the identity of potential or actual customers are those that are the most difficult to reproduce.\(^\text{20}\) In this regard, countries should require the use of “official” documents issued by appropriate authorities such as a passport, driver’s license, personal identification or tax identification document.

In those instances where an agent is representing a beneficiary (e.g., through trusts, nominees, fiduciary accounts, corporations, and other intermediaries), financial institutions need to take reasonable measures to verify the identity and nature of the persons or organizations on whose behalf an account is being opened or for whom a transaction is being completed.\(^\text{21}\) Financial institutions need to verify the legality of such entities by collecting the following information from potential customers:

- Name and legal form of customer’s organization;
- Address;
- Names of the directors;
- Principal owners or beneficiaries;
- Provisions regulating the power to bind the organization;
- Agent(s) acting on behalf of organization; and
- Account number (if applicable).\(^\text{22}\)

In cases of fund transfers, such as money remittances, financial institutions should include accurate and meaningful originator information (name, address, and account number) and pass this information along the payment chain with the fund transfer.\(^\text{23}\)

A client’s identity should be confirmed through due diligence procedures in cases where he or she is an occasional customer who has exceeded the designated threshold or when there is any doubt of that customer’s actual identity.\(^\text{24}\) The same would apply in the event of the occasional corporate customer.

\(^{20}\) Basel Customer Due Diligence for Banks (provision 23).
\(^{21}\) The Forty Recommendations, Rec. 5.
\(^{22}\) Id., Rec. 5.
\(^{23}\) Special Recommendations, Spec. Rec. VII.
\(^{24}\) Basel Customer Due Diligence for Banks, provision 53; and FATF, The Forty Recommendations, Rec. 11.
Customer identification is an ongoing process that requires, as a general rule, financial institutions to keep up-to-date records on all relevant client information. Records should be updated in the event, for example, of significant transactions, changes in customer documentation standards, material changes in an account’s operation, and the realization that current records are insufficient. A country’s financial institution supervisors are strongly encouraged to assist financial institutions in developing their own customer acceptance and identification procedures.

4. Low and High Risk Accounts and Transactions

The customer due diligence measures described above should be applied in accordance with the risk attached to the type of customer and transaction. This general principle is central to both the FATF Recommendations and the Basle Committee paper on Customer Due Diligence. For higher risk categories, enhanced measures should be taken and some particular cases are discussed below. For lower risk categories, a country may allow its financial institutions to apply reduced or simplified measures. FATF and the Basel Committee have identified some examples of such customers or transactions, but this is not exhaustive and it is a matter for a country’s discretion. Examples of such lower risk customers are financial institutions, public companies and government enterprises. Examples of such transactions are pooled accounts, pension schemes, and small scale insurance policies.

Nevertheless, there is an expectation that customers should always be identified and some basic steps taken to verify identity. The reduced or simplified measures might apply to the extent of the verification process and/or the amount of information collected about the purpose and nature of the business relationship and transactions.

A particular issue on which risk is a factor concerns establishing the identity of customers who already had accounts before verification of identity for new customers became a requirement. Neither the Basel Committee

27. See The Forty Recommendations, Interpretive Notes to Rec. 5, paragraphs 11 and 12.
nor FATF requires a comprehensive program to be instituted to verify the identity of existing customers or conduct other due diligence measures.\(^{29}\) However, it is required that financial institutions should verify identity and carry out further due diligence on existing customers depending on materiality and risk.

5. Circumstances Requiring Increased Due Diligence

In certain cases, *The Forty Recommendations* provide that certain enhanced due diligence measures should be taken in addition to those performed in the normal course by financial institutions. The following discusses those cases requiring additional due diligence procedures.

a. Politically Exposed Persons

FATF defines Politically Exposed Persons (PEPs) as:

Individuals who are or have been entrusted with prominent public functions in a foreign country, 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior officials in the forgoing categories.\(^{30}\)

This definition covers only those customers who have public functions in a “foreign” country. Thus, it does not apply to “domestic” PEPs. However, FATF encourages countries to extend extra due diligence to domestic PEPs, but requires that extra due diligence be applied to foreign PEPs.\(^{31}\)

\(^{29}\) See *The Forty Recommendations*, Interpretive Notes to Rec. 5, paragraph 8.

\(^{30}\) *The Forty Recommendations*, Glossary, Politically Exposed Persons.

\(^{31}\) *The Forty Recommendations*, Interpretive Notes to Rec. 6.
The additional due diligence measures consist of the following:

- Identifying PEPs;
- Approval at senior management level to account opening;
- Establishing the source of wealth and funds;
- Enhanced ongoing monitoring.

Actually finding out whether a customer is a PEP is often the biggest challenge for a financial institution given the definition of the term. No official organization issues a list of such individuals, but various commercial entities maintain and regularly update such lists.

**b. Cross-Border Correspondent Banking Relationships**

Cross-border correspondent banking relationships are another source of potentially high risk accounts for financial institutions. Such relationships could be a way for entities or persons from countries with lax arrangements to gain access to the global financial system without undergoing proper due diligence procedures. Before entering into correspondent banking relationships with a cross-border institution, a bank should:

- Establish the nature of the respondent bank’s business, its reputation, and the quality of its supervision;
- Assess the AML/CFT controls of the respondent bank;
- Obtain senior management approval for the relationship;
- Document respective responsibilities;
- If “payable-through-accounts” are to be a feature of the business relationship, assure that the respondent bank verifies the identity and conducts ongoing due diligence of its customers.32

Correspondent banking relationship with institutions located in countries classified by FATF as “non-cooperative countries and territories”

---

(NCCTs) should be avoided.\textsuperscript{33} No transactions should be undertaken with “shell banks” (i.e., a bank that is incorporated in a jurisdiction in which it has no physical presence and that is not affiliated with a regulated financial group).\textsuperscript{34}

c. Non Face-to-Face Customers

As technology develops, the phenomenon of “non face-to-face” customers and business relationships is growing as customers use the telephone and internet to obtain financial services without necessarily visiting the provider. There is no intention on the part of the international standard setters to obstruct such developments, which give customers greater choice and services as well as benefit the economy. Financial institutions and others providing such services need to be aware that the AML/CFT risks are rather different with respect to such customers and need to take appropriate steps to deal with them.\textsuperscript{35}

While FATF raises the issue of increased risk with such accounts, it does not provide any guidance on which steps should be taken to address such increased risks. Thus, it is left to each country’s discretion to establish appropriate policies and procedures.

d. Introduced Business

In some countries, financial businesses have customers “introduced” to them by intermediaries or third parties and will not have carried out any due diligence on these customers. In such circumstances, financial institutions should do three things.\textsuperscript{36} First, the institution should make sure that the introducer is subject to customer due diligence requirements and that its compliance with such due diligence requirements is subject to supervision. Second, the

\textsuperscript{33} For the complete list of FATF’s “no cooperative” jurisdictions, see http://www.fatf-gafi.org/NCCT_en.htm.

\textsuperscript{34} The Forty Recommendations, Rec. 18. See also Basel Customer Due Diligence for Banks (Provision 51).

\textsuperscript{35} Id., Rec. 8.

\textsuperscript{36} Id., Rec. 9.
Preventive Measures

institution should make certain that the introducer has collected sufficient information about identity and other relevant due diligence documentation about the customer. Third, the institutions should make sure that the introducer can make that information available on request without delay.

The introducer can be domestic or international. Where it is an international party that is the introducer, the financial institution needs to be especially vigilant that the above requirements are met. Several countries, which permit introduced business, require that the introducer should be an individual or an institution that is subject to AML controls, is supervised by a regulatory body with responsibility for compliance with AML controls, and is located in a country that complies with FATF standards.

e. Other High Risk Business

FATF also draws attention to two other categories of transactions that require special attention. First, there are complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined and the findings recorded. Where the financial institution cannot discover such information and/or is uneasy about the business, it should consider declining the business and/or making a suspicious transaction report.

Second, there are countries that have been identified as non-compliant with FATF recommendations that merit special attention. While transactions with such countries are not prohibited, financial institutions should pay special attention to them and, when there is doubt about their purpose, investigate further and record the outcome. If the financial institution is not satisfied that the transaction is bona fide it should consider declining the business and/or making a suspicious transaction report.

37. Id., Rec. 11.
38. Id., Rec. 21.
6. Extending Due Diligence to Vendors and Others

The supply-chain structure of many businesses has become increasingly complex and interconnected with the advance in global commerce. Consequently, many financial institutions have found it necessary to exercise greater diligence over the vendors, suppliers, and agents of organizations as well as with employees and correspondent banks of financial institutions. Each country’s financial institution supervisors may wish to consider implementing policies that incorporate these trends in due diligence, especially when such relationships may be considered higher risk as described above.

7. Insurance Sector Measures

The International Association of Insurance Supervisors (IAIS) maintains its own guidelines for customer identification and due diligence; the insurance industry must adhere to these in addition to the relevant requirements of The Forty Recommendations discussed above. The IAIS guidelines recommend that insurance companies:

- Establish to their “reasonable satisfaction” that every party relevant to the insurance application actually exists. For large numbers of subjects (e.g., group life policies and pensions), it may be sufficient to use a limited group such as the principal shareholders or main directors;
- Verify all underlying principals as well as their relationship with the policyholders—the principals and not the policyholders should be questioned regarding the nature of the relationship;
- Prohibit anonymous and fictitious accounts;
- Verify claims, commissions, and other money administered to no policyholders (e.g., partnerships, companies);
- Increase due diligence when the policyholder’s financial flows or transaction patterns change in significant, unexpected, or unexplained ways;
- Increase due diligence regarding the purchase and sale of second-hand endowment policies and the use of single-unit-linked policies; and
• Monitor reinsurance or retrocession on a regular basis as a way to ensure payments to bona fide reinsurance entities at rates justified by the risk level.39

8. Security Sector Measures

The International Organization of Securities Commissions (IOSCO) has not established separate customer identification or due diligence requirements for securities firms, brokers, or collective investment entities. Although IOSCO has not established such specific requirements, the customer identification requirements of The Forty Recommendations (as described more fully in the Methodology40) do apply to the securities sector.

9. Measures for Designated Non-Financial Businesses and Professions

These requirements for customer due diligence, as well as those relating to record keeping, apply to designated non-financial businesses and professions in a more limited manner than to financial institutions. The following discussion outlines the applicable circumstances where due diligence procedures apply to these entities and persons.

a. Casinos

Due diligence procedures for financial institutions apply when casino customers engage in financial transactions equal to or exceeding USD/EUR 3000. Examples of such transactions include buying or cashing-in casino chips, opening accounts, wire transfers, and currency exchange. This does not mean that every gambling transaction has to be monitored or recorded for 5 years.41

41. The Forty Recommendations, Rec. 12, paragraph a. The applicable recommendations are Recs. 5, 6, and 8–11.
b. Real Estate Agents

Transactions for a client concerning the buying and selling of real estate require due diligence procedures. However, identification and other customer due diligence need only be conducted when a transaction takes place and only with respect to the party who is the client of the estate agent. In many countries, the client will be the seller, rather than the buyer.

c. Dealers in Precious Metals and Stones

Cash transactions, equal to or exceeding USD/EUR 15,000, are to be covered by the due diligence requirements.

d. Lawyers, Notaries, Other Independent Legal Professional, and Accountants

Identification and due diligence requirements apply to transactions prepared or carried out for a client with respect to the following specific activities:

- Buying and selling of real estate;
- Managing of client money, securities or other assets;
- Management of bank, savings or securities accounts;
- Organization of contributions for the creation, operation or management of companies;
- Creation, operation or management of legal persons or arrangements, buying and selling of business entities.

The key phase is “prepare for or carry out transactions.” This means that merely providing advice on how to undertake such a transaction is not covered. Identification and customer due diligence (and record keeping) are required after the professional becomes involved in carrying out the transaction, which includes the preliminary work on drawing up the transaction as

42. Id., Rec. 12, paragraph b.
43. Id., Rec. 12, paragraph c.
44. Id., Rec. 12, paragraph d.
Preventive Measures

These are situations in which lawyers and accountants are functioning as “gatekeepers” to the financial system by providing services that would permit clients to engage in potential money laundering or terrorist financing transactions.

**e. Trust and Company Service Providers**

Due diligence procedures are applicable to transactions for a client prepared for and carried out in relation to the following specific activities:

- Acting as a formation agent of legal persons;
- Acting as (or arranging for anchor person to act as) a director or secretary of a company, a partner of a partnership of a similar position in relation to other legal persons;
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- Acting as (or arranging for another person to act as) a trustee or an express trust; or
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.  

In some countries the above-described transactions are performed by lawyers. To be consistent with the criteria for lawyers set out above, the relevant test is again “prepare for and carry out,” which excludes merely providing advice, but includes preliminary work on carrying out a specific transaction.

---

45. *Id.*, Rec. 12, paragraph e.
B. Record Keeping Requirements

1. Financial Institutions

Financial institutions should keep customer identity and transaction records for a minimum of five years following the termination of an account.\footnote{46. The Forty Recommendations, Rec. 10.} Institutions may be required to retain records for longer than five years if required by their regulators. Contents of the records should be made readily available to authorities upon request and, further, be of sufficient detail to permit the prosecution for criminal behavior.\footnote{47. Id.}

Maintaining records is important for both prevention and detection of money laundering and terrorist financing purposes. If a potential customer knows that records are being maintained, the customer may not be as likely to try to use the institution for these illegal purposes. Record maintenance also helps detect those involved and provides a financial trail to help competent authorities pursue those involved.

The following information should be included when recording a customer’s transaction:

- Name of the customer and/or beneficiary;
- Address;
- Date and nature of the transaction;
- Type and amount of currency involved in the transaction;
- Type and identifying number of account; and
- Other relevant information typically recorded by the financial institution.\footnote{48. Id.}

2. Insurance Sector

The IAIS maintains its own set of record keeping requirements; the insurance entities must adhere to these, in addition to the relevant guidelines of The Forty Recommendations. The insurance entity must also obtain the following information (where applicable) when recording a customer’s transaction:

\footnote{46. The Forty Recommendations, Rec. 10.}
\footnote{47. Id.}
\footnote{48. Id.}
• Location completed;
• Client’s financial assessment;
• Client’s need analysis;
• Payment method details;
• Benefits description;
• Copy of documentation used to verify customer identity;
• Post-sale records associated with the contract through its maturity; and
• Details of maturity processing and claim settlement (including “dis-
  charge documentation”).

Financial institution supervisors must verify that all representatives for
insurance companies are licensed under appropriate insurance law and juris-
diction. Representatives may retain documents on behalf of an insurance
entity, but the integrity of the records rests on the insurance entity as the
product provider. In such cases, a clear division of responsibility between
the insurance entity and its representative is necessary.

3. Securities Sector

The IOSCO has established its own set of record keeping requirements, which
securities firms should follow in addition to adhering to the applicable gen-
eral requirements of The Forty Recommendations discussed above. IOSCO
requires that the national centralized authority on financial crime or other
competent authority ensure that intermediaries maintain records as needed
demonstrating their adherence to the regulatory rules. These records
should be legible, understandable, and comprehensive, and should include all
transactions involving collective investment assets and transactions.

49. See IAIS Anti–Money Laundering Guidance Notes.
50. Id.
51. Id.
52. Id.
53. See IOSCO Principles for the Supervision of Operators of Collective Investment Schemes (CIS
54. Id.
4. Designated Non-Financial Businesses and Professions

Record keeping requirements for designated non-financial businesses and professions apply in the same circumstances as are applicable to customer identification and customer due diligence requirements. See section A.9, above, Customer Due Diligence and Identification, Measures for Designated Non-Financial Businesses and Professions.

C. Suspicious Transactions Reporting

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should report its suspicions to the applicable financial intelligence unit. Moreover, banks should be required to report suspicious activities and significant incidents of fraud to the supervisors, and supervisors do need to ensure that appropriate authorities have been alerted. Financial institutions, when filing suspicious activity reports (STRs), should not, under any circumstances, notify a customer that his/her behavior has been reported as suspect to authorities. From that point on—which is to say, upon notification—financial institutions should comply fully with instructions from government authorities, including the production of records.


Suspicious transactions have certain broad characteristics, including, most obviously, transactions that depart from normal patterns of account activity. Any complex or unusually large transactions—in addition to any unusual patterns of transactions absent an apparent economic, commercial, or lawful purpose—are suspect and, therefore, merit further investigation by the finan-

---

59. Id., Recs. 10 and 28.
Preventive Measures

A financial institution and, if necessary, by the appropriate authorities. To assist financial institutions in screening for suspicious transactions, these financial institutions should establish risk-sensitive limits to monitor particular classes or categories of accounts. Specific examples of suspicious activity (e.g., very high account turnover inconsistent with balance size) are useful for individual financial institutions and should be provided to them in some form by supervisors.

Financial institutions and their employees should always be vigilant for suspicious transactions. While the following are indications of suspicious transactions, the listing is not exhaustive:

- **General Signs**
  - Assets withdrawn immediately after they are credited to an account.
  - A dormant account suddenly becomes active without any plausible reason.
  - The high asset value of a client is not compatible with either the information concerning the client or the relevant business.
  - A client provides false or doctored information or refuses to communicate required information to the bank.
  - The arrangement of a transaction either insinuates an unlawful purpose, is economically illogical or unidentifiable.

- **Signs Regarding Cash Transactions**
  - Frequent deposit of cash incompatible with either the information concerning the client or his business.
  - Deposit of cash immediately followed by the issuance of checks or transfers towards accounts opened in other banks located in the same country or abroad.
  - Frequent cash withdrawal without any obvious connection with the client’s business.

---

60. *Id.*, Rec. 11.
61. *Id.*, Rec. 25; See also Basel Customer Due Diligence for Banks, (provision 53).
– Frequent exchange of notes of high denomination for smaller denominations or against another currency.
– Cashing checks, including travelers’ checks, for large amounts.
– Frequent cash transactions for amounts just below the level where identification or reporting by the financial institution is required.

• Signs Regarding Transactions on Deposit Accounts

– Closing of an account followed by the opening of new accounts in the same name or by members of the client’s family.
– Purchase of stocks and shares with funds that have been transferred from abroad or just after cash deposit on the account.
– Illogical structures (numerous accounts, frequent transfers between accounts, etc.).
– Granting of guarantees (pledge, bonds) without any obvious reason.
– Transfers in favor of other banks without any indication of the beneficiary.
– Unexpected repayment, without a convincing explanation, of a delinquent loan.
– Deposit of checks of large amounts incompatible with either the information concerning the client or the relevant business.

2. “Safe Harbor” Provisions for Reporting

“Safe harbor” laws help to encourage financial institutions to report all suspicious transactions. Such laws protect financial institutions and employees from criminal and civil liability when reporting suspicious transactions to competent authorities in good faith. These legal provisions should provide financial institutions, and their employees or representatives, protection against lawsuits for any alleged violation of confidentiality or secrecy laws provided that the suspicious report was filed in good faith (i.e., it was not frivolous nor malicious).62

3. Scope of Reporting Obligation

An STR is a way of alerting authorities to the possibility that a particular transaction could involve money laundering or terrorist financing and should, therefore, be investigated. In most cases, the reporting financial institution will not have evidence that the transaction represents the proceeds of crime, and is less likely to know of what specific crime might be involved. The financial institution will simply be aware that the transaction is unusual and not consistent with the normal type of transaction on the account. Most likely, it will not be aware of the source of the funds or the reason for the transaction and cannot inquire of the customer without the risk of tipping-off the customer. In such situations, the institution should submit a suspicious transaction report and leave it to the authorities to further investigate.

Because reporting institutions will usually not know the underlying basis of the transaction, a suspicious transaction reporting system should base the requirement to report on “suspicion” that funds may be related to a criminal offense. It is not necessary to require the reporting institution to investigate the transaction or have actual evidence that the funds relate to criminal activity.

4. Fiscal Crimes

Some countries do not classify fiscal crimes, such as tax evasion, as a money laundering predicate offense. Thus, laundering the proceeds of tax evasion is not necessarily a money laundering offense. However, financial institutions should still report transactions that they find suspicious and leave it to the authorities to determine whether money laundering is involved. Otherwise, there is a risk that customers would attempt to explain away transactions related to money laundering predicates as the proceeds of tax evasion and pressure institutions not to file STRs.
5. Insurance Sector

The IAIS has established its own set of guidelines for reporting suspicious transactions. The insurance industry should follow these, in addition to the requirements of The Forty Recommendations noted above. Insurance companies should report suspicious activity to the financial intelligence unit or other national centralized authority. The following are insurance sector-specific cases of suspicious transactions meriting additional investigation:

- Unusual or disadvantageous early redemption of an insurance policy;
- Unusual employment of an intermediary in the course of some usual transaction or financial activity (e.g., payment of claims or high commission to an unusual intermediary);
- Unusual payment method; and
- Transactions involving jurisdictions with lax regulatory instruments regarding money laundering and/or terrorist financing.

6. Securities Sector

The IOSCO has not established separate suspicious activity reporting requirements for securities firms, brokers, or collective investment entities. Although IOSCO has not established separate or additional requirements in this area, the suspicious activity reporting requirements of The Forty Recommendations do apply to the securities sector.

7. Designated Non-Financial Businesses and Professions

Under the 2003 revision of The Forty Recommendations, designated non-financial businesses and professionals are now required to file suspicious transactions reports, but on a more limited basis than their obligation to identify customers and carry out due diligence.

63. See IAIS Anti-Money Laundering Guidance Notes.
64. Id.
65. The Forty Recommendations, Rec. 16.
For lawyers, notaries, other independent legal professionals and accountants, there is only an obligation to file an STR only when they engage in a financial transaction for, or on behalf of, a client. This is narrower than the obligation to identify clients and conduct due diligence upon them in two respects:

- The reporting obligation covers only “financial transactions,” not all transactions; and
- There is a reporting obligation only at the point at which the professional engages in a financial transaction for his or her client.\(^\text{66}\)

There is no obligation to report in legally privileged circumstances. Individual countries determine when such reporting obligations arise, but the privilege normally covers information obtained either in ascertaining the legal position of a client or representing the client in proceedings. Countries may provide that members of this group may report to their respective self-regulatory organizations (SRO), rather than the FIU, provided the SRO cooperates with the FIU.\(^\text{67}\)

Dealers in precious metals and precious stones are required to file STRs only when they engage in a cash transaction with a customer equal to or exceeding the USD/EUR 15,000 threshold.\(^\text{68}\)

Trust and company service providers are required to file STRs only in circumstances where they engage in transactions on behalf of a client.\(^\text{69}\) As a consequence, any transaction, not just a financial transaction, that is suspicious should be reported. The reporting is limited, however, to situations where the trust or company service provider actually carries out the transaction; mere providing advice or preparing a transaction is not reportable.

\(^{66}\) Id., Rec. 16, paragraph a.  
\(^{67}\) Id., Interpretive Note to Rec. 16.  
\(^{68}\) Id., Rec. 16, paragraph b.  
\(^{69}\) Id., Rec. 16, paragraph c.
D. Cash Transaction Reporting

Countries should consider the possible benefits of requiring all cash transactions that exceed a fixed threshold amount to be reported. It is not mandatory, however, that a country have such a requirement. Cash transaction reporting has significant resource and privacy implications, which countries need to take into account in considering the issue. Each country or jurisdiction establishes its own reporting threshold based upon its own circumstances. For example, the United States requires that financial institutions record and report to designated authorities all transactions involving currency or bearer instruments in excess of $10,000.

Other countries require reporting at similar levels. Such thresholds may be established by statute, or by regulation under the authority of the appropriate government supervisory agency. Depending on circumstances in a country, such requirements may also apply to non-financial businesses and professionals, such as casinos, antique or automobile dealers, lawyers, accountants or other situations where large purchases are paid for in cash.

Relevant authorities should take great care in designating a country’s threshold level; it must be high enough to screen out insignificant transactions yet low enough to detect transactions potentially connected with financial crime. In addition, countries may wish to add exemptions to reporting requirements for transactions where reporting is burdensome to the system and not particularly productive for enforcement purposes.

In addition, certain entities can represent a low risk for engaging in money laundering, and, therefore, may be eligible for exemption. These entities include governments, certain financial institutions or corporations that are reasonably assumed to be corruption-free, and customers that make frequent, large cash transactions due to the nature of their businesses. Such exceptions should be reviewed on a regular basis to determine if the exception remains appropriate, both as a general rule and for specific entities, under relevant circumstances.

70. The Forty Recommendations, Rec. 19.
71. See, for example, U.S. Bank Secrecy Act of 1970.
1. Multiple Cash Transactions

Cash reporting requirements also apply to same-day multiple transactions, a practice called “smurfing.” If the consolidated transaction amount exceeds the designated reporting threshold, financial institutions need to report the entire series of transactions. This safeguard against smurfing—whereby many individual transactions involving multiple accounts at a financial institution manage to take place just below the country’s reporting threshold—is a vital part of the effort to prevent money laundering and terrorist financing. Criminals and terrorists obviously resort to their own countermeasures to avoid detection by software programs. This is why it is absolutely crucial for the relevant authorities to use proactive analysis in detecting criminal and terrorist financial activity.

Of course, a transaction can also be reported as a suspicious transaction that does not meet the threshold or multiple transactions test. For example, a single deposit of 9,900 may be considered suspicious, under various circumstances when the country has a reporting threshold of 10,000 because it suggests structuring of transactions by a customer in order to evade the reporting requirements.

2. Cross Border Movements

Money launderers engage in cross-border transfers of cash, bearer negotiable instruments and high-value commodities as a scheme for laundering funds. It is important that countries have a mechanism in place to detect when such transfers may be used for money laundering or terrorist financing purposes.

Authorities should consider establishing a minimum reporting limit for cross-border movements of currency, other negotiable instruments, and high-value commodities (i.e., precious metals or gems). Unusual or suspicious international movement of such goods, their point of origin and destination should be reported to the country’s customs service or other appropriate authorities.

---

73. The Forty Recommendations, Rec. 19.
3. Modern Money Management Techniques

The monitoring capabilities of financial institutions and government officials have benefited from the movement away from cash and currency transfers toward checks, payment cards, direct deposit, and book-entry recording of securities. These transactions leave a helpful paper trail when wrongdoing is suspected and permit competent authorities to make investigations. Success in investigations depends upon accurate and complete record keeping. For this reason, the use of these modern money management and payment transfer methods is highly encouraged.74

E. Balancing Privacy Laws with Reporting and Disclosure Requirements

The reporting of information, e.g., suspicious transactions and cash transactions, or the disclosure of records by a financial institution to a competent authority, necessarily involves information that is normally treated confidentially under a country’s bank secrecy or privacy laws.

In requiring the reporting or disclosure of such information for AML and CFT purposes, a country needs to make appropriate exceptions in its privacy laws or otherwise specifically authorize the reporting and disclosure for those limited purposes. FATF specifically provides that financial institution privacy laws should be drafted so as not to inhibit the implementation of any of its recommendations.75 At the same time, a country needs to build in protections to assure that confidentiality will be observed, except where public policy needs, such as prosecution for money laundering, outweigh the overall need to protect privacy of financial information. By assuring confidentiality and privacy in the overall scheme, a country protects reporting and disclosure from abuse. In doing so, a country encourages maximum cooperation and proper reporting and disclosure by those entities and persons subject to such requirements.

---

74. Id., Recs. 20 and 28.
75. Id., Recs. 4 and 28.
F. Internal Controls, Compliance, and Audit

Countries should require all financial institutions covered by their AML and CFT laws to establish and maintain internal policies and procedures to prevent their institutions from being used for purposes of money laundering and terrorist financing. Internal policies and procedures will vary among different institutions and different types of institutions, but they should nevertheless all consider the size, scope, and nature of that institution’s operation.

Internal procedures include ongoing training that keeps employees informed and up-to-date about developments on AML and CFT. Employee training needs to (1) describe the nature and processes of money laundering and terrorist financing; (2) explain AML/CFT laws and regulatory requirements; and (3) explain an institution’s policies and systems with regard to reporting requirements regarding suspicious activity, with emphasis on customer identification, due diligence and reporting requirement.

In addition, financial institutions should screen job applicants for possible intent to use their institutions to launder money and/or to finance terrorism.

The designation of an AML/CFT compliance officer at the management level, by each financial institution, is recommended. Such a compliance officer helps to ensure that appropriate management attention is devoted to the institution’s compliance efforts.

An audit function is also a required internal policy and procedure that needs to be established; the audit function should be separate from the compliance administration function, in order to test and assure the adequacy of the overall compliance function.

G. Regulation and Supervision—Integrity Standards

The foregoing discussions deal with AML and CFT preventative measures that should be applied by national authorities to financial institutions and certain

---

76. Id., Rec. 15.
77. Id.
78. Id., Interpretive Note to Rec. 15.
79. Id.
designated non-financial businesses and professions. It is not sufficient for national authorities to impose those requirements in legislation. Countries also need to take measures to ensure that they are implemented in practice. Like many other elements of the international standards, the extent of regulation and supervision should be based on the money laundering and terrorist financing risk to the institution in question. The framework established by the standard setters envisages different types of regulation and supervision for:

- Core Principle Institutions,
- Other Financial Institutions, and
- Designated Non Financial Businesses and Professions.

The regulations and supervision recommendations regarding integrity standards of The Forty Recommendations are discussed in detail in Chapter V, under Supervision and Regulation—Integrity Standards.

H. Legal Entities and Arrangements

Each country should take appropriate measures to prevent the unlawful use of corporations and other forms of legal entities by money launderers and those who finance terrorism. Such measures should include accurate and timely information about the beneficial ownership and control of legal entities; such information should be accessed in an expeditious manner by competent authorities. In addition, in countries where bearer shares of securities are permissible, appropriate measures should be taken to assure that such bearer instruments are not abused for money laundering or terrorist financing purposes.

A country should also take appropriate measures to assure that trust and similar legal arrangements are not misused by those involved in money laundering or terrorist financing. Such preventative measures should include access to details about the settler, trustee and beneficiaries of these types of legal arrangements.

80.Id., Rec. 33.
81.Id.
82.Id., Rec. 34.
83.Id.
Those involved in the fight against money laundering and terrorist financing must have access to certain kinds of financially related information in order to conduct financial investigations. In this regard, the financial intelligence unit (FIU) plays an increasingly important role in this process.¹

Money launderers manipulate their illicit proceeds in an endeavor to conceal or disguise their true nature, source, location, disposition, and movement, with the ultimate objective of integrating these proceeds into, and through, the legitimate economy.² Those who finance terrorism seek to conceal the source of the funds and disguise the illicit use of funds in support of terrorism. Financial investigations are assisted greatly by a country’s compre-

---

1. For a comprehensive discussion on FIUs, see Financial Intelligence Units, An Overview 2004, (FIUs Overview) by the International Monetary Fund and World Bank, available (read-only) at www.amlcft.org.

hensive regime that requires the reporting of certain information and record keeping, and that facilitates information sharing among competent authorities, both domestically and internationally. The primary goals of financial investigations are to identify, trace, and document the movement of funds; to identify and locate assets that are subject to law enforcement measures; and to support the prosecution of criminal activity.

Financial investigations seek to discover the financial trail left by criminals. As part of this process, investigators analyze financial institution account records, real estate records, documents on liens and judgments, corporate registries, brokerage and mutual fund accounts, insurance contracts and a full spectrum of other financial and business relations records. Illicit financial operations have recently grown more sophisticated and complex, requiring traditional investigators to acquire new and specialized financial intelligence tools.

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering (AML) and combating the financing of terrorism (CFT), provides in *The Forty Recommendations on Money Laundering (The Forty Recommendations)*, that each country should establish an FIU.3 Further, FATF urges countries to impose measures on financial institutions and certain non-financial businesses and professions requiring them to maintain records on the identities of their clients and their transactions, and to report any suspicious transactions.4 Information generated by these reporting and record keeping requirements is to be reported to the country’s FIU and is used to reconstruct transactions, to establish the link between individual clients and a particular business, to prove the “state of mind” of an individual, and finally, to identify the role of an individual in a criminal or terrorist financing activity.

Information reporting and record keeping requirements generate substantial financial data, much of which is not easily useable by competent authorities without further analysis. If a country’s AML and CFT institutional frameworks are to be at all effective, the country must institute a reliable, efficient system for processing, analyzing, and disseminating this information. Without such a system in place, law enforcement has a much

4. *Id.*, Recs. 10–22.
The Financial Intelligence Unit

more difficult time detecting criminal or terrorist financial dealings. The pressing need for effective data analysis of possible financial crime explains, in part, the proliferation of FIUs and the growing importance of their roles in the international effort to prevent, detect and prosecute money laundering and terrorist financing.⁵

A. Definition of a Financial Intelligence Unit

The Egmont Group of Financial Intelligence Units (Egmont Group), which is the international standard setter for FIUs, adopted the following definition of an FIU in November 1996:

A central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities, disclosures of financial information (i) concerning suspected proceeds of crime, or (ii) required by national legislation or regulation, in order to counter money laundering.⁶

The United Nations Convention against Transnational Organised Crime (2000) (Palermo Convention) adopted this definition, stating, “Each state Party...shall...consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering.”⁷

Expanding on this definition, FATF requires countries to establish an FIU, which has these three essential functions, i.e., the collector or “repository” of reported information, analysis and financial information sharing,⁸ for detecting and countering money laundering and terrorist financing. The FATF

---

⁵ As of June 2004, 94 countries have established financial intelligence units that are members of the Egmont Group. The Egmont Group, Financial Intelligence Units of the World, available at http://www.egmontgroup.org/.
⁶ The Egmont Group is an informal organization of financial intelligence units named after the location of the group’s first meeting at the Egmont-Arenberg Palace in Brussels. The goal of the group is to provide a forum for FIUs to improve support to their respective national anti-money laundering programs. See Egmont Group, “Information Paper on Financial Intelligence Units and the Egmont Group,” available at http://www.egmontgroup.org/info_paper_final_092003.pdf. See also Chapter III, the Egmont Group.
⁷ The Palermo Convention, Article 7(1)(b).
⁸ The Forty Recommendations, Recs. 36, 37 and 40.
also has a general requirement that all national authorities exchange information and co-operate with their domestic and international counterparts.  

In 2004, the Egmont Group revised its definition of an FIU to include specifically the combating of terrorist financing. The current definition of an FIU as follows:

A central, national agency responsible for receiving (and as permitted, requesting), analyzing and disseminating to competent authorities, disclosures of financial information:
  i. concerning suspected proceeds of crime and potential financing of terrorism, or
  ii. required by national legislation or regulation, in order to combat money laundering and terrorist financing.

As a result, the Egmont Group’s definition of an FIU is entirely consistent with *The Forty Recommendations*.

**B. Core Functions**

FIUs vary from country to country, but all of them share three core functions; they receive, analyze and disseminate information to combat money laundering and terrorist financing. The dissemination of financial information should be done on both a domestic and international basis.

Because money laundering is often a cross-border activity, it is important for FIUs to join forces with other national intelligence units. Thus, even the best domestic laws and regulations against money laundering, including those for an FIU, need an effective international information sharing mechanism in order to combat effectively money laundering and terrorist financing.

---

9. *Id.*, Recs. 26 and 31.
11. *Id.*
1. Centralized Repository of Reported Information

Financial institutions must report all suspicious activity reports and other required disclosures (such as cash transaction reports) to their country’s FIU. The centralization of this “repository function”—designating the FIU as the recipient of financial disclosures—is a prerequisite for an effective preventive national and international framework against money laundering.

The use of a centralized repository for the reporting of information and required disclosures ensures that all of the relevant information is in one place, facilitating the processing of information and analysis on a consistent basis. Centralization also ensures greater efficiency in information gathering.

2. Analytical Function

FIUs are more than mere databases for financial information required to be submitted by legislation or national regulatory authorities. FIUs must analyze the data they receive because so many suspicious transaction reports (STRs) and other financial disclosures often appear to be innocent transactions. Ordinary deposits, withdrawals, fund transfers, or the purchase of a security or an insurance policy may, however, be important pieces of information in detecting and prosecuting money laundering and terrorist financing.

Only through examination and analysis can FIUs detect criminal financial transactions. Distinguishing truly suspect transactions from those that are only benignly unusual requires informed analysis. Without it, the most sophisticated data gathering in the world will not be productive.

These analytical functions require countries to vest their FIUs with the necessary legal authority, proper human resources, and sufficient technical capacity. In particular, the FIU’s analytical functions require extended powers to access information. These powers should include: access to certain commercial or government databases; the authority to request additional information from reporting entities and other sources as necessary; and access to

---

13. See FIUs Overview, Chapter 3, Receiving Transaction Reports.
advanced intelligence techniques and apparatus, such as wire tapping and covert operations, subject to domestic legal principles.

Each country must balance very real privacy concerns against the FIU’s need for an effective analytical function. While utilizing publicly available commercial databases does not raise privacy concerns, authorizing centralized intelligence units to request additional information does. The same caution applies to FIU surveillance and other intelligence techniques. Financial institution privacy laws should be drafted so as not to interfere with there functions of the FIU, yet protect the privacy of information.\(^\text{14}\)

FIUs perform three specialized analytical functions: tactical, operational and strategic.\(^\text{15}\)

\(a. \text{Tactical Analysis}\)

Tactical analysis is the process of collecting the data needed to build a case and to provide the accompanying facts behind the commission of a criminal offense. Although tactical analysis may be performed on all incoming reports, it is likely that STRs will provide the most directly useful information.

Tactical analysis includes the matching of data received from reporting institutions and others with data held by the FIU or accessible to it. Such data includes lists of names, addresses, phone numbers, and data in the other reports forwarded by reporting institutions. While some reporting institutions produce the simplest form of tactical information themselves, FIUs add to these reports related information on the reported client or transaction that they have in their databases.

Upon receipt of an STR, staff of the FIU will look for additional information on the subject, the company, the transactions, or other elements involved in a particular case to provide the basis for further analysis. The main sources of such additional information are:

- The FIU’s own data,
- Publicly available sources,

\(^{14}\) \(\text{The Forty Recommendations}, \text{Rec. 4.}\)
\(^{15}\) \(\text{id.}, \text{Chapter 3, Analyzing Reports}.\)
• Government-held databases,
• Additional information from reporting entities and other entities, and
• Other FIUs.16

b. Operational Analysis

Operational analysis uses tactical information to formulate different hypotheses on the possible activities of a suspected criminal. Operational analysis supports the investigative process. It uses all sources of information available to the FIU to produce activity patterns, new targets, relationships among the subject and his or her accomplices, investigative leads, criminal profiles, and, where possible indications of possible future behavior.

One technique of operations analysis is financial profiling. This provides the analyst with methods for developing indicators of concealed income of an individual, a group of individuals, or an organization. It is an effective indirect method of gathering, organizing, and presenting evidence related to the financial status of subjects. The relevance of the profile is to show that the target cannot demonstrate a legitimate source for the difference between his or her outflow of cash versus the income. The tracing of a person’s assets may also provide leads linking the subject with predicate offenses.

Through operational analysis, the information received by the FIU is developed into operational intelligence, which can be transmitted to law-enforcement agencies or prosecutors for further action.17

c. Strategic Analysis

Strategic analysis develops knowledge to be used for the future work of the FIU. The main characteristic of strategic intelligence is that it is not related to individual cases, but rather to new issues or trends. The scope of any strategic analysis varies greatly depending upon the FIU’s mandate. It may consist of the identification of evolving criminal patterns in a particular group or

16. Id.
17. Id.
the provision of broad insights into emerging patterns of criminality at the national level.

Strategic analysis is developed after all available information has been collected and analyzed. It requires a wider range of data than operational analysis, as well as experienced analysts. The data comes from reports provided by the reporting entities, the FIU’s own operational intelligence and tactical information, public sources, law enforcement and other governmental agencies. At a broader level, strategic analysis may suggest the need to impose reporting and other AML/CFT obligations on new entities or enhance existing reporting requirements.18

3. Domestic Information Sharing

If it suspects money laundering or the financing of terrorism, the FIU should have the authority to share, or route, financial information and intelligence to other domestic authorities for investigation or action. The FIU should also be authorized to cooperate and coordinate its actions with the other domestic authorities devoted to the detection, prevention and prosecution of money laundering and terrorist financing.

The importance of timely information sharing with the proper authorities cannot be overstated. Effective measures against money laundering rely on getting the available information to the appropriate authority. For most FIUs, the sharing of information usually follows some analysis of reported financial disclosures. For other FIUs, especially those that receive an enormous volume of financial disclosures, the financial disclosures are made available to law enforcement authorities immediately; these FIUs conduct analysis on financial disclosures and other financial information upon request of law enforcement as needed at a later time. In either case, the key is for the FIU to provide the competent authority with financial intelligence as quickly as possible so that the competent authority can pursue the leads provided by the FIU.19

Domestic coordination is vital. The FIU has to be an essential partner in domestic coordination and could even be empowered to assume the lead role

18. Id.
19. Id., Chapter 3, Dissemination Reports.
in coordinating the relevant authorities that fight money laundering—which is to say, the FIU, regulators and supervisors of the financial sector, the police, the judicial authorities, and other relevant ministries or administrations.20

4. International Information Sharing
Because so much of money laundering and terrorist financing are cross-border activities, FIUs must be able to share financial intelligence with other FIUs worldwide in order to be effective partners in the international fight against these crimes. A core feature of an FIU is its ability to cooperate in an efficient and rapid manner with all of its foreign counterparts. Information sharing at the international level should occur through direct and secure communication with the competent foreign authorities.21

C. Types or Models of FIUs

Countries generally choose one of four basic models in establishing or improving the operations of an FIU:

a. The administrative model, which is either attached to a regulatory/supervisory authority, such as the central bank or the ministry of finance, or as an independent administrative authority;
b. The law enforcement model, whereby the agency is attached to a police agency, whether general or specialized;
c. The judicial or prosecutorial model, where the agency is affiliated with a judicial authority or the prosecutor's office; or
d. The hybrid model, which is some combination of the above three.

These variations arise primarily from different country circumstances and from the lack of an internationally accepted model, when the first such units were established in the early 1990s. For example, in some countries, the function of the FIU as an additional tool for law enforcement organiza-

tions in combating money laundering and associated crimes was emphasized, and this led to the establishment of the FIU in an investigative or prosecutorial agency. Other countries emphasized the need for a “buffer” between the financial institutions and the police and, consequently, their FIUs were established outside of these agencies.

It should be emphasized, however, that the four classifications are, to a certain degree, arbitrary and that there are other ways of classifying FIUs. Discussed below is a description of each model, advantages and disadvantages (although this listing is not exhaustive) and examples of countries that use the model.

1. Administrative

Administrative-type FIUs are usually part of the structure, or under the supervision of, an administration or an agency other than law-enforcement or judicial authorities. Sometimes, the administrative type constitutes a separate agency, placed under the supervision of a ministry or administration (autonomous) or not placed under such supervision (independent). The main rationale for such an arrangement is to establish an “buffer” between the financial sector (and, more generally, non-financial businesses and professionals subject to reporting obligations) and the law enforcement authorities in charge of financial crime investigations and prosecutions.

The advantages of an administrative-type FIU are:

- The FIU acts as an interface between the financial and other sectors subject to reporting obligations, on the one hand, and law-enforcement authorities, on the other hand; this avoids the creation of direct institutional links between reporting parties and law enforcement agencies, while bringing disclosures to the attention of law enforcement agencies.
- Financial institutions and others are more confident about disclosing information if they know that dissemination will be limited to cases of money laundering and terrorist financing and will be based on the FIU’s own analysis, rather than the reporting institution’s limited information.

22. FIUs Overview, Establishing an FIU.
• The FIU is a “neutral,” technical, and specialized interlocutor for the reporting parties.
• If the FIU is placed in a regulatory agency, it is the natural interlocutor of the financial institutions.
• Information can be easily exchanged with all types of FIUs.

The disadvantages are:

• Because the FIU is not part of the law enforcement administration, there may be a delay in applying law enforcement measures, such as freezing a suspicious transaction or arresting a suspect, on the basis of financial disclosures.
• The FIU usually does not have the range of legal powers that law enforcement agencies and judicial authorities have to obtain evidence.
• The administrative-type FIUs (unless that are truly independent) are more subject to the direct supervision of political authorities.23

Examples of countries with administrative-type FIUs include Andorra, Aruba, Australia, Belgium, Bolivia, Bulgaria, Canada, Colombia, Croatia, the Czech Republic, France, Israel, the Republic of Korea, Liechtenstein, Malta, Monaco, the Netherlands, the Netherlands Antilles, Panama, Poland, Romania, Russia, Slovenia, Spain, Ukraine, the United States, and Venezuela.24

By making an administrative authority a “buffer” between the financial institution and other reporting sectors and the law enforcement sectors, authorities can more easily enlist the cooperation of reporting institutions, which are often conscious of the drawbacks vis-à-vis their clients of having direct institutionalized links with law enforcement agencies. Administrative-type FIUs are often preferred by the banking sector. They may also appeal to other institutions and professionals that have been added to the list of reporting entities for the same reasons.

23. Id.
24. Id.
2. Law Enforcement

In some countries, the emphasis on the law-enforcement aspects of the FIU led to the creation of the FIU as part of a law enforcement agency, since this was the easiest way to establish a body with appropriate law-enforcement powers without having to design a new entity and a new legal and administrative framework.\textsuperscript{25}

Operationally, under this arrangement, the FIU will be close to other law enforcement units, such as a financial crimes unit, and will benefit from their expertise and sources of information. In return, information received by the FIU can be accessed more easily by law enforcement agencies and can be used in any investigation, thus increasing its usefulness. Exchanges of information may also be expedited through the use of existing national and international criminal information exchange networks.

The advantages of a law enforcement type of FIU are:

- It is built on an existing infrastructure, so there is no need to set up a new agency.
- Maximum law enforcement use can be made of financial disclosure information.
- There is quick law enforcement reaction to indicators of money laundering and other crimes.
- Information can be exchanged using the extensive network of international criminal information exchange networks (such as Interpol).
- There is relatively easy access to criminal intelligence and to the intelligence community at large.

The disadvantages are:

- This type of FIU tends to be more focused on investigations than on prevention measures.
- Law enforcement agencies are not a natural interlocutor for financial institutions; mutual trust must be established, which may take some time.

\textsuperscript{25} Id.
time, and law enforcement agencies may lack the financial expertise required to carry out such a dialogue.

- Gaining access to a financial institutions’ data (other than the reported transactions) usually requires the launching of a formal investigation.
- Reporting institutions may be reluctant to disclose information to law enforcement if they know the information could be used in the investigation of any crime (not just money laundering and the financing of terrorism).
- Reporting institutions may be reluctant to disclose information to law enforcement on transactions that are no more than “suspicions.”

Examples of law enforcement FIUs include Austria, Estonia, Germany, Hungary, Iceland, Ireland, Slovakia, Sweden, and the United Kingdom.

Also, a law enforcement-type of FIU will normally have all the powers of the law enforcement agency itself, without the need for separate, specific legislative authority. These powers include the power to freeze transactions and seize assets (with the same degree of judicial supervisions as applies to other law enforcement powers in the country).

3. Judicial or Prosecutorial

This type of FIU is generally established within the judicial branch of the country and most frequently under the prosecutor’s jurisdiction. Such an arrangement is typically found in countries with a continental law tradition, where the public prosecutors are part of the judicial system and have authority over the investigatory bodies.26

Judicial or prosecutorial-type FIUs can work well in countries where banking secrecy laws are so strong that a direct link with the judicial or prosecutorial authorities is needed to ensure the cooperation of financial institutions.

The advantages of a judicial or prosecutorial-type FIU are:

26. Id.
They usually possess a high degree of independence from political interference.

The disclosure of information is provided directly to the agency authorized to investigate or prosecute the crime.

The judiciary’s powers (e.g., seizing funds, freezing accounts, conducting interrogations, detaining people, conducting searches) are immediately brought into play.

The disadvantages are:

• Generally, the same disadvantages of law enforcement-type FIUs apply to judicial or prosecutorial-type FIUs except for the reluctance to disclose information upon “suspicion.”
• This type of FIU may have difficulty exchanging information with non-judicial or prosecutorial FIUs.27

Examples of judicial or prosecutorial FIUs include Cyprus and Luxembourg.28

4. Hybrid FIUs

This last category encompasses FIUs that contain different combinations of the arrangements described in the other three categories. This hybrid type of arrangement is an attempt to obtain the advantages of the different types of FIUs put together in one organization. Some FIUs combine the features of administrative-type and law enforcement-type of FIUs, while others combine the powers of the customs office with those of the police. It may be noted that in some FIUs, staff from various regulatory and law enforcement agencies work in the FIU, while continuing to exercise the powers of their agency of origin. Among the countries that have established “hybrid” FIUs are Denmark, Jersey, Guernsey, and Norway.29

27. Id.
28. Id.
29. Id.
D. Possible Additional Functions

In addition to its core function responsibilities, an FIU could be given a number of other functions, regardless of which model is utilized.

1. Supervisory and Regulatory Responsibilities

The FIU could be granted the power to supervise financial institutions and non-financial businesses and professions with regard to their compliance with record keeping and reporting requirements. In such cases, the FIU could also be authorized to impose sanctions or penalties against such entities and persons for failing to comply with their reporting or recordkeeping obligations—for example, meaningful fines and/or license suspensions. Furthermore, the FIU could be authorized to promulgate regulations necessary for the implementation of laws against money laundering and terrorist financing.

Some authority within the country needs to be responsible for these compliance matters. In most countries, this responsibility belongs to the supervisory authority of each financial sector, non-financial business or profession. But, because the FIU is the unique recipient of financial intelligence, in addition to which it analyzes financial intelligence, the FIU is well placed to monitor compliance with AML and CFT obligations. Some countries have opted to give the AML/CFT compliance responsibility to the FIU. In certain countries, some reporting entities and persons are not subject to any supervision other than that of the FIU, which makes it the most suitable body to address the compliance issues raised in this context.

In addition, the FIU could be authorized to issue regulations for the financial and other reporting sectors with regard to the implementation of laws against money laundering. Giving such responsibilities to the FIU, however, should take into account issues of balancing AML/CFT needs with other supervisory concerns. To be effective, an FIU must receive adequate resources and appropriate government support for the FIU to accomplish its core functions and any additional responsibilities. If the FIU’s staffing capacity is lim-
ited, additional supervisory or regulatory functions could undermine its core functions.

2. Investigations

Countries may grant their FIUs the function of providing investigative support to other law enforcement agencies in the course of ongoing investigations on money laundering. In this case, the FIU would be expected to share information with investigative authorities upon request. These powers may entail the exercise of additional powers that would enable the FIU to request additional information from financial institutions or even to carry out investigations, including identifying potential assets, to be frozen, seized, or confiscated.

3. Enforcement and Blocking of Assets

Countries may also grant their FIU the power to take provisional measures to deal effectively with cases where urgent action is needed. Because the FIU is a crucial governmental point for identifying suspicious transactions, it is logical to grant the FIU provisional powers to preserve assets that might become subject to confiscation. Such measures could include the temporary freezing of assets as well as other measures that restrain any legal disposition of these assets.

Such provisional powers require, however, that the FIU be able to investigate and identify any assets vulnerable to confiscation under the laws against money laundering and terrorist financing. In doing so, however, particular care should be taken to assure that the FIU has sufficient resources to perform its core functions—that is, receiving and analyzing the suspicious-transaction reports, as well as sharing information with domestic and international counterparts.

Where provisional powers of blocking transactions and/or freezing assets are authorized, such powers are usually limited in terms of the duration of
the blocking or freezing. Freezing or seizing assets usually requires judicial authorities or a government authority outside the FIU.31

4. Training

Because of focused and multidisciplinary expertise of an FIU, it could easily serve as the governmental unit to advise and train personnel from financial institutions in measures to fight money laundering and terrorist financing.

Again, countries must consider resource limitations in deciding whether to attach this function to the FIU. Capacity, funding and expertise are crucial concerns in this area, since demand for such services could become extensive.

5. Research

The FIU is in a unique position to provide research to its government based upon its experience of receiving, analyzing an disseminating financial information on money laundering and terrorist financing. This is especially true if the FIU is given a broad mandate with regard to strategic analysis, as discussed above in this chapter. Its strategic function could easily be expanded to authorize separate research and reports on its findings.

As with so many functions, the addition of research and the scope of that research depend upon funding, staffing and expertise. Without such resources, the core functions of the FIU could suffer.

E. Organizing the FIU

There are numerous decisions that have to be made in establishing the FIU or enhancing the operations of an existing FIU.

31. Id.
1. Choosing the Right Model

Good decisions about the proper model to adopt for an FIU proceed from equally sound knowledge about a country’s cultural and economic characteristics and its legal and law enforcement traditions. Although no single model will work for all countries, some criteria are essential; the discussion below is given in the form of questions:

- Will or does the FIU possess relevant capacity and expertise in financial operations? If not, what is needed?
- What is the relationship between the proposed or existing FIU and the financial industry in the domestic context? What would enhance that relationship?
- Will or does the institution possess a culture conducive to protecting the confidentiality of financial information and to mitigating potential harm to individual privacy?
- Will or does the proposed FIU possess the actual legal authority, technical capacity, and experience to provide appropriate and timely international cooperation?
- Would the legal framework applicable to the proposed or existing FIU allow it to take part in the international administrative type of cooperation and would the legal framework allow for rapid, efficient, spontaneous and/or “upon request” international information exchanges relating to suspicious transactions?

2. Capacity Considerations

Financial investigations are only as good as the individual investigators and the technological infrastructure that supports the financial intelligence efforts. A country must make policy determinations on how the FIU can make the best use of the financial analytical skills of its staff members. In this regard, the country must also determine the best institutional setting for these skills—the central bank, ministry of finance, the police, the judiciary. Fashioning an FIU as a wholly separate agency from a country’s existing regulatory, administrative, or law enforcement agencies could also have serious resource implications.
3. Staffing Considerations

Recruitment policies have implications for matters relating to resources, privacy, and institutional effectiveness. The relative rarity of investigatory financial expertise means that staffing considerations should be driven by the multidisciplinary nature of financial investigations in order to make recruitment as diverse as possible.

Staff background and the terms of employment are both important. On the one hand, treasury or finance ministry officials, banking supervisors, and customs officers could bring their respective financial expertise and their understanding of transactions involving reporting entities. On the other hand, police or judicial officers bring useful law enforcement experience, particularly if the FIU has been granted law enforcement powers.

The terms of employment also impact the degree of independence, and the degree of confidentiality in the work of the FIU. The rarity of the high level skills/experience required of FIU analysts means that some countries might opt for staffing their units with experts seconded from other agencies. Although this is a less-costly staffing option—and probably one that is more conducive to effective information sharing—governments need to weigh the privacy and longer term implications of such decisions.

F. Privacy Safeguards

FIUs are repositories, as well as guardians, of highly sensitive information, a fact that calls for constant vigilance regarding legal and systemic safeguards.

1. The Main Policy Tension: Privacy Versus Efficiency

Certain policy tensions emerge as FIUs take shape; these stem mostly from the ambitious goals of AML and CFT laws and regulations, which compete with or erode rival privacy interests.32

32. The Egmont Group’s statement of purpose, in the preamble, provides that it is “mindful of…the sensitive nature of disclosures of financial information.” The Group also holds that “FIUs should work to encourage that national legal standards and privacy laws are not conceived
Laws against money laundering have emerged, in part, as a response to the obstacles that bank secrecy laws posed to supervisory and law enforcement efforts. In some jurisdictions, strong bank secrecy requirements have frequently defeated investigative efforts to obtain financial information required to detect crimes and regulatory breaches, or for tracing or confiscating assets. Such a result is contrary to the FATF recommended structure, which provides that financial institution privacy laws should not inhibit any of the FATF recommendations.33 Cumbersome procedures also hamper investigative efforts to gather information and/or evidence abroad. With financial globalization, such concerns have become even more acute. AML/CFT laws can be seen as an attempt to ensure efficient information exchange and evidence gathering, both domestically and internationally, as prerequisites for effective regulatory and criminal law enforcement in today’s globalized economy.

The very sensitive and confidential nature of financial information means that FIUs need to institute stringent procedural safeguards for their important financial evidence gathering and information sharing functions. Effective law enforcement rests on efficient and speedy access to financial information. But this law enforcement need pushes against the boundaries of financial privacy concerns, raising legitimate concerns about the potential for abuse.

In its roles as repository, processor, and clearinghouse of financial information relating to the crime of money laundering and terrorist financing, FIUs are at the forefront of this debate about efficiency versus privacy. This tension is reflected in the choices countries make about the structure, functions, powers, and procedures of their financial intelligence units. Countries need to make realistic assessments of the costs to privacy inherent in each of the choices they make about the FIU’s authorities and restrictions.

2. Confidentiality Principle

Imposing the confidentiality principle on FIUs is one of the most important protections against abuse of financial information privacy. This principle will

---

33. The Forty Recommendations, Rec. 4
also enable the FIU to exercise its functions as an intermediary between the reporting parties and the criminal justice system.

In cases where the FIU is part of another agency, such as the police or the office of the public prosecutor, the unit is usually governed by a general duty of confidentiality. In the absence of such a general duty, however, a specific duty of confidentiality should be expressed in the legal provisions governing and creating the FIU, and should be enforced by criminal and/or effective civil sanctions.34 The duty of confidentiality may also be contained in domestic privacy laws of general application.

The FIU’s duty of confidentiality, however, should be drafted so as not to restrict unduly the possibility of providing feedback to the reporting entities, as feedback is important both for the relationship between the FIU and the financial intermediaries and for enabling the reporting institutions to develop efficient reporting mechanisms.35 Confidentiality requirements should be drafted in a way that does not inhibit international cooperation among FIUs.36

3. Specialty Principle

To complement the duty of confidentiality, FIUs can adopt a “specialty principle,” which serves to limit the use of information reported to it by financial institutions and others, or as requested by the FIU from reporting parties. If an FIU is prohibited from using information provided to it for any purpose other than fighting money laundering and terrorist financing (and related crimes), countries can develop a sense of trust between reporting institutions and other parties and the FIU.

The specialty limitation necessarily depends on what it means to “fight money laundering and terrorist financing.” The restriction could be drafted to mean the financial information managed by the FIU could be used only for the performance of the agency’s duties, as described in the law that estab-

lished the FIU. It could also be expressed in a specific statutory or regulatory stipulation regarding the conditions for the dissemination of information by the FIU.

The specialty principle should be drafted in sufficiently broad language so that the FIU is not prevented from enforcing the laws and regulations against money laundering and terrorist financing. This should also allow for information supplied to the FIU to be used to enforce laws and regulations relating to the underlying predicate offense or offenses. In addition, if the specialty principle applies to international information exchanges among FIUs, it should be drafted so as not to inhibit or damage the efficiency of international cooperation among FIUs. 37

Breaches of the specialty limitation should be sanctioned by procedural laws about inadmissibility of the evidence before the courts, and/or by some form of civil or statutory liability for breach of confidentiality.

4. Independence and Accountability

Countries must assure the independence of the FIU from political influence, as well as independence from the competent or other supervisory authority in deciding which transactions to analyze or what information to disseminate. Independence provides another measure of protection against the abuse or misuse of financial disclosures. Independence is not an absolute concept, there will always be some measure of accountability, but the FIU should not be subject to abuse or undue influence from other government authorities. This sense of independence further supports a sense of trust between the FIU and reporting financial entities, which, in turn, promotes the prevention and detection of money laundering and terrorist financing.

This independence could be guaranteed in several ways. In certain instances it could be accomplished by creating the FIU as a separate agency with an autonomous budget and staff without accountability to any agencies that might be inclined to use the system beyond its proper limits. This inde-

37. Id., at Principles of Information Exchange between Financial Intelligence Units for Money Laundering Cases (June 13, 2001), Principles 11 and 12.
pendence should, however, be accompanied by proper accountability mechanisms, such as parliamentary reporting, audits, and/or judicial oversight.

G. Information and Feedback

It is important that the FIU work closely with reporting entities and persons, as well as a country’s competent authorities, to fight money laundering and terrorist financing. Consistent with its privacy obligations, the FIU should provide feedback about money laundering and terrorist financing trends and typologies that will assist financial institutions and non-financial businesses and persons to improve their AML/CFT practices and controls and, in particular, their reporting of suspicious transactions. It is a frequent criticism by reporting institutions that they receive little or no feedback from their FIUs about the usefulness of their reports. Thus, reporting entities have no guidance about whether their approach to reporting is helpful in the fight against money laundering and terrorist financing.

While there are obviously constraints on what an FIU can tell a reporting institution about a particular report (especially if that report involves an ongoing enquiry), it should be possible for the FIU to give general feedback to institutions about the quality and usefulness of their reports. FIUs will also have collected data, which once analyzed, should produce useful information about developments and trends in money laundering. This should be shared with reporting entities and persons so that they know what to look out for in designing their AML/CFT systems. Feedback about particular case histories, once any investigation and legal proceedings are over, should also prove useful.

The FATF now provides that all competent authorities, including FIUs, should establish guidance and provide feedback. Authorities can expect this issue to feature prominently in AML/CFT assessments. FIUs will also need to maintain comprehensive statistics on STRs received and disseminated.

38. The Forty Recommendations, Rec. 25.
39. Id., Rec. 32.
Chapter VIII

International Cooperation

Organized crime and other large and highly profitable criminal activities are increasingly being perpetrated on a cross-border basis. This is particularly the case for money-laundering operations, where criminals use the open international financial system to benefit from free movement of capital throughout the world in order to hide the illicit origins of the proceeds of their crime and further their illicit activities. In the context of fighting money laundering from the global standpoint, rapid exchanges of information and effective international cooperation among the various agencies in countries throughout the world have become a prerequisite to success.

International cooperation is needed more and more at all stages (i.e., the financial intelligence gathering, investigative and prosecution stages) of anti-money laundering (AML) investigations. At the financial intelligence gathering stage of a money laundering case, for instance, financial intelligence units (FIUs) need to exchange information with their foreign counterparts in order to be able to analyze properly suspicious activity reports and other financial
disclosures. The same can be said for the investigating stage in order for
the police to investigate successfully money laundering cases. The ability to
exchange rapidly information with their foreign counterparts, without undue
obstacles or delay, is increasingly becoming a key feature of any FIU, law
enforcement or prosecution authority.

In addition, having in mind that money launderers are always look-
ing for safe havens with lax, ineffective or corrupt AML and combating the
financing of terrorism (CFT) regimes, or those with limited international
cooperaion capabilities, countries will find that having a proper interna-
tional cooperation framework in place helps them to prevent, detect and
prosecute money laundering in their own domestic financial system.

A. Prerequisites for Effective International Cooperation

In order for countries to be able to use the existing channels of interna-
tional cooperation, they need to meet several prerequisites, including:
(1) building a comprehensive and efficient domestic capacity; (2) ratify-
ing and implementing the international conventions regarding money
laundering and terrorism financing; and (3) complying with the recom-
mandations of the Financial Action Task Force on Money Laundering
(FATF), i.e. The Forty Recommendations on Money Laundering (The Forty
Recommendations)¹ and the nine Special Recommendations on Terrorist
Financing (Special Recommendations),² as well as with other sector-specific
international standards.

1. Prerequisite Conditions for International Cooperation: Building a Comprehensive
and Efficient Domestic Capacity

Naturally, putting in place all the necessary authorities and providing them
with all the necessary powers, responsibilities, staffing and budget so that

Annex IV of this Reference Guide.
of this Reference Guide.
they can perform efficiently their duties is a prerequisite for a country to be able to cooperate at the international level with its partners. ³

Among others, in order to have an effective AML/CFT framework, a country should have established administrative supervisory authorities to oversee financial institutions in each sector, as well as an FIU—that is, a central authority charged with receiving and analyzing suspicious transaction activities (STA) and other types of mandatory reporting (such as cash transaction reports) for the purpose of fighting money laundering and terrorist financing.

Similarly, on the criminal justice system side, countries should have effective police services with specialized skills and training in money laundering and terrorist financing investigations, as well as a functioning, non corrupt judicial/prosecutorial system.

Properly building and staffing these authorities provide the foundation for an effective and comprehensive framework for fighting money laundering and terrorist financing at both the domestic and international levels.

2. Ratifying and Implementing the International Conventions

All countries should sign and ratify the relevant conventions adopted by the United Nations (UN): In particular, countries should sign and ratify the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention),⁴ the UN Convention for the Suppression of the Financing of Terrorism (1999),⁵ and the UN Convention Against Transnational Organized Crime (2000) (Palermo Convention).⁶ These actions are part of FATF’s recommendations.⁷

In addition, countries should sign and ratify the other AML and CFT conventions adopted by organizations in their respective region, such as the Council of Europe’s Convention on Laundering, Search, Seizure

---

³. The Forty Recommendations, Rec. 36.
and Confiscation of the Proceeds from Crime (1990) (the Strasbourg Convention). 8

Countries should implement fully all of the provisions of these conventions in their domestic laws, including those related to the criminalization of money laundering and international cooperation, which will enable them to take part in the mutual legal assistance arrangements provided by these conventions. 9

3. Complying with the FAFT Recommendations and Other Sector Specific International Standards

Countries should comply with the existing international standards for fighting organized crime, money laundering, and combating the financing of terrorism. These standards include the FATF recommendations, which apply to all aspects of a country’s laws and regulations against money laundering and the financing of terrorism. It includes as well the Core Principles for Effective Banking Supervision adopted by Basel Committee on Banking Supervision (the Basel Committee), and its Customer Due Diligence Principles; Other standards have been set by the International Association of Insurance Supervisors (IAIS), the International Organization of Securities Commissions (IOSCO) and the Egmont Group.

Each of these standard setters requires that each country establish international channels of cooperation with their foreign partners. For instance, FATF recommends that “each country should make efforts to improve a spontaneous or upon request international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities.” 10 In addition to general principles on international cooperation against money laundering, specific conditions apply to the international cooperation between FIUs, financial supervisory authorities, and between law enforcement and judicial authorities.

9. *Id.*, at Rec. 36.
10. *Id.*, at Rec. 40.
B. General Principles of International Cooperation Against Money Laundering

According to the relevant international standards, the following general principles should be implemented by countries in order to ensure that effective gateways for the exchange of information and the provision of international cooperation exist at each stage of a money laundering or terrorist financing investigation:

- When an authority in country A has information officially requested by an authority in country B, the requested country-A authority should be in a position to provide the information promptly to the requesting authority in country B.
- When an authority in country A has information it knows would be useful for an authority in country B, the country-A authority should be able to provide the information spontaneously and promptly to the country-B authority.
- When an authority in country A is requested by a country-B authority to obtain information or a document, or to conduct an investigation or an inquiry, or to perform a particular action useful in the context of an analysis, investigation, or prosecution of money laundering, the requested country-A authority should be in a position to perform the requested action (naturally if this action is permitted by rules regulating the performance of its duties at the domestic level).\[^{11}\]

This exchange of information with, or provision of assistance and cooperation to, a foreign authority should not be subject to unduly restrictive conditions. It is generally accepted however that the requested authority can subject its assistance to certain conditions. For example, the requested authority could subject its assistance to the following conditions and stipulate that the requesting authority:

- Perform similar functions as the requested authority (specialty principle);
- Describe in its request the purpose and the scope of information to be used, and the information, once transmitted by the requested authori-

\[^{11}\] Id., at Recs. 36 and 40.
ty, should be treated by the requesting authority according to the scope of its request (transparency);

• Is subject to confidentiality provisions similar to those applicable to the requested authority (confidentiality); and

• Is itself in a position to exchange information with the requested authority (reciprocity).

C. International Cooperation Between FIUs

Because money laundering is a cross-border activity, the detection of money laundering operations often depends on information sharing among FIUs in different countries and on their ability to cooperate, efficiently and speedily, with their foreign counterparts. In addition, countries should be aware of the possible consequences of choosing a particular organizational structure when establishing their FIU.

1. The Core Features of FIU International Cooperation

An FIU’s ability to cooperate at the international level depends on a principle of mutual recognition among entities performing the same duties and on a foundation of mutual trust.12 The consequence is that each FIU should possess certain core features in accordance with the Egmont Group definition and act in accordance with the Egmont principles. This would enable the entity to qualify and to be treated as an FIU by other FIUs. These features are described in Chapter VII, the Financial Intelligence Unit.

In addition, each FIU should be authorized by law to share financial information and other relevant financial intelligence with its foreign counterparts. In particular, the FIU should be able to cooperate and exchange information either on its own initiative or upon request. This could be achieved on the basis of reciprocity or formal mutual agreement, such as memorandum of understanding (MOU). Finally, the requested FIU should

---

be authorized to produce, and be capable of producing, promptly any available information or analysis that may be relevant to an investigation by the requesting FIU.

2. Conditioning the FIU’s Ability to Cooperate at the International Level

The FIU’s ability to cooperate at the international level should not be subject to unduly restrictive conditions (see Part B of this Chapter for legislative restrictions). Adequate safeguards—including confidentiality provisions—should be in place to ensure that information exchanges between FIUs are consistent with fundamental domestic and internationally agreed-on principles of privacy and data protection. At a minimum, every country should ensure that information received from a foreign FIU is treated with and protected by the same confidentiality provisions that apply to similar information obtained from domestic sources.

3. The Relationship Between Different Organizational Models and International Cooperation

An FIU should be authorized to cooperate at the international level with all its foreign counterparts, regardless of their internal and organizational structure. This point is particularly important in light of the diverse organizational structures that exist among FIUs worldwide. Indeed, while most FIUs, as financial intelligence gathering bodies, are attached to administrative authorities, such as ministries of finance, treasury departments, regulatory/supervisory authorities, or other ad hoc administrative structures, other FIUs are attached to police units. Some are even attached to prosecutors’ offices. In addition, even if most FIUs share the same responsibilities, there could be some other structural differences among them, as well as certain legal/procedural differences. Therefore, the rules governing the ability of a particular FIU to cooperate to the fullest extent at the international level have to take

this diversity into account. In other words, the rules need to be sufficiently flexible so that FIUs can exchange information with all its counterparts, regardless of their nature or organizational structure.\footnote{The Forty Recommendations, Recs. 40.}

The question for a country is (1) whether there are or should be restrictions on sharing financial information; (2) if so, how much information should be shared; and (3) what type of information should be shared. Thus, policy makers must be aware that choosing a particular organizational model may have direct and/or indirect consequences on the FIU’s ability to cooperate at the international level. For instance, creating a purely judiciary-based FIU may hamper international cooperation with other countries that do not have a judicial FIU. Indeed, in many countries, fundamental or constitutional legal principles do not allow judicial authorities to have access to the same international cooperation or information-exchange channels as the administrative authorities or the police. In certain countries, these legal principles oblige the judicial authorities to cooperate at the international level only in accordance with the judicial cooperation procedures (mutual legal assistance mechanisms), which are governed by treaties and principles that may contain a number of restrictive conditions. Such conditions may inhibit the comprehensive and rapid exchange of information with other FIUs at the intelligence stage.

\textbf{D. International Cooperation Between Financial Supervisory Authorities}

It is widely recognized that financial supervisors (banking insurance and securities) should be authorized to cooperate—spontaneously or upon request—with their foreign counterparts with respect to AML/CFT analysis and regulatory investigations. The general principles of international cooperation, as described above in Part B, apply to these particular information exchange channels. In the supervisory context, this cooperation takes place in each specific sector between the relevant supervisors.
1. Cooperation Between Banking Supervisors

With respect to information sharing, the Basel Committee has issued additional principles, which apply to all banking supervisors. These principles have been established in the Customer Due Diligence paper, issued by the Basel Committee in October 2001. In particular, branch supervisors of banking groups should not be constrained from sharing consolidated reports pertaining to deposits, “borrower concentration,” or notification of funds under management if the home country supervisor needs this information.16

The host jurisdiction should permit foreign home-country supervisors or auditors to carry out on-site inspections to verify compliance with home country “Know Your Customer” (KYC) procedures and policies at the local branch level and among subsidiaries of foreign banks. This will require a view of customer files and random sampling of accounts.17

Foreign home-country supervisors, or auditors, should have access, in the host jurisdiction, to information on individual customer accounts, to the extent necessary. This is to say, to the extent that permits supervisors to properly evaluate the due diligence standards being applied to customer identification, as well as to evaluate the risk management practices in place.18

Finally, supervisors should have safeguards in place to ensure that information regarding individual accounts obtained through cooperative arrangements is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner.19

2. Cooperation Between Securities Supervisors

IOSCO has issued additional principles that apply to all securities supervisors. The securities supervisor should have authority to share both public and nonpublic information with domestic and foreign counterparts.20

---

17. Id.
18. Id.
19. Id.
20. International Organization of Securities Commissioners (IOSCO), Core Principle No. 11. http://www.iaisweb.org/35coreprinciplesmethodologyoct03revised.pdf. For further information, see the IOSCO Multilateral MOU (May 2002).
Cooperative mechanisms should be in place at the international level to facilitate the detection and deterrence of cross-border misconduct and assist in the discharge of licensing and supervisory responsibilities. Among these are memoranda of understanding.21

International cooperation can provide assistance in: (1) obtaining public or nonpublic information, for example, about a license holder, a listed company, shareholder, beneficial owner, or a person exercising control over a license holder or company; banking, brokerage, or other records; (2) arranging for voluntary cooperation from those who may have information about the subject of an inquiry; (3) procuring information under compulsion—either or both the production of documents and oral testimony or statements; (4) providing information on the regulatory processes in a jurisdiction; or (5) securing court orders, for example, or other urgent court injunctions.22

Information-sharing arrangements, whether formal or informal, should consider providing assistance in obtaining or providing (1) public or nonpublic information, for example, about a license holder, listed company, shareholder, beneficial owner or a person exercising control over a license holder or company; (2) banking, brokerage or other records; (3) voluntary cooperation from those who may have information about the subject of an inquiry; (4) information under compulsion—either or both the production of documents and oral testimony or statements; and (5) information on the regulatory process in a jurisdiction, or in obtaining court orders, for example, urgent injunctions.23

3. Cooperation Between Insurance Supervisors

Insurance supervisors have no formal rules governing cooperation with each other for specific AML purposes. This does not mean that they do not share information to the extent permitted by their respective jurisdictions. In any

23. IOSCO, Principles, Sec. 9.3.
E. International Cooperation Between Law Enforcement and Judicial Authorities

International cooperation among prosecutorial and judicial authorities is vital to any framework that hopes to be comprehensive and efficient against money laundering activities. Almost no prosecution of money laundering can succeed without the support of a foreign jurisdiction at one point of the investigation.24

International cooperation depends upon the signing and ratification of all the relevant conventions agreed by the United Nations and other regional international organizations. Indeed, these conventions often provide the necessary legal basis to exchange information with and undertake actions on behalf of foreign judicial authorities.

The general principles in this area are the same as those described in Part B, above. The unique nature of judicial international cooperation means that a number of additional and/or entirely specific principles have been established in this area. These principles come from the various United Nations conventions, as well as from the FATF recommendations.

It should be emphasized that varying constitutional requirements should be respected and addressed when negotiating arrangements among sovereign judicial authorities. In addition, care has to be taken not to allow suspects to take refuge in the non-extraditable category of “political crimes” in AML/CFT cases, especially when influential persons are involved.

1. Basic Principles

Laws and procedures should encourage and facilitate mutual legal assistance in AML/CFT law-enforcement matters, particularly with regard to the use of compulsory measures. These include the production of records by financial institutions and other persons; the search of persons and premises; the track-

---

ing of property and the identification of assets; and the seizure of assets and obtaining evidence for use in AML/CFT investigations and prosecutions and in related actions in foreign jurisdictions.25

Appropriate laws and procedures must provide for effective mutual legal assistance in AML/CFT investigations or proceedings where the requesting jurisdiction is seeking: (1) the production or seizure of information, documents, or evidence (including financial records) from financial institutions, other entities, or natural persons; (2) searches of financial institutions, other entities, and domiciles; (3) the taking of witnesses’ statements; and (4) the tracking, identifying, freezing, seizure, and confiscation of assets laundered or intended to be laundered, the proceeds of money laundering and assets used for or intended to be used for the financing of terrorism, as well as the instrumentalities of such offenses, or assets of corresponding value.26

Treaties or other formal arrangements (and informal mechanisms) must be in place to support international cooperation; such as through the use of bilateral or multilateral mutual legal assistance.27 Institutional and other arrangements should permit law enforcement authorities to exchange information with their international counterparts regarding the subjects of investigations; such arrangements should be based on agreements in force and by other mechanisms for cooperation. In addition, national authorities should record the number, source, and purpose of requests for such information exchange, as well as its resolution.

Countries should provide its relevant law enforcement and judicial authorities with adequate financial, human, and technical resources so that they can ensure adequate oversight, conduct investigations, and respond promptly and fully to requests for assistance received from other countries.

2. Additional Principles

To the greatest extent possible, differing standards in the requesting and requested jurisdictions concerning the “mental intent” of the offense under domestic law should not affect the ability to provide mutual legal assistance.28

25. Id., at Rec. 40.
26. Id., at Rec. 38.
27. Id., at Rec 27.
28. Id., at Rec 36.
Assistance should be provided in investigations and proceedings where persons have committed both laundering and the predicate offenses, as well as in investigations and proceedings where persons have committed money laundering only.

Authorities should be authorized to conduct cooperative investigations (including controlled delivery of confidential information) along with other countries’ appropriate competent authorities; assurance should be offered that adequate safeguards are in place.29

Arrangements should permit the effective cross-border coordination of seizure and forfeiture, including, where permissible, authorizing the sharing of confiscated assets with other countries when confiscation is directly or indirectly a result of coordinated law enforcement actions.30

Finally, procedures should allow for the extradition of individuals charged with a money-laundering, terror-financing, or related offense or for prosecution of the accused domestically when he or she is not extraditable.31

F. Considerations for Fiscal Matter Offenses

In general, countries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts. As noted above (Section B), countries are entitled to place certain conditions on their assistance, although they must avoid placing unduly restrictive conditions upon their assistance. A condition that may be applied to mutual legal assistance or extradition is dual criminality, although countries are encouraged to render such help even in the absence of dual criminality.

Some countries do not criminalize certain fiscal offenses, such as tax evasion, as offenses for money laundering predicate and, thus, may not be able to provide assistance if another country requests it in the context of an enquiry concerning the laundering of the proceeds of a fiscal crime. However, if fiscal matters are only a part of the request and it has a non-fiscal component as well, provided the non-fiscal component includes a money laundering predicate, the requested country should provide assistance.

29. Id., at Rec 27.
30. Id., at Rec 38.
31. Id., at Rec 39
Chapter IX

Combating the Financing of Terrorism

The terrorist attacks on the United States on September 11, 2001, increased the importance of preventing, detecting and suppressing the financing of terrorism and terrorist acts on the part of the international community. In October of 2001, the Financial Action Task Force on Money Laundering (FATF) expanded its mission beyond anti-money laundering (AML) to include the worldwide effort of combating the financing of terrorism (CFT).

To achieve these goals, FATF adopted the original eight Special Recommendations on Terrorist Financing (Special Recommendations) at the same time that it amended its mission. In October 2004, FATF adopted new Special Recommendation IX regarding cash couriers. Like its earlier efforts, The Forty Recommendations on Money Laundering (The Forty Recommendations), FATF’s Special Recommendations are not suggestions, but rather mandates for action by every country, not just FATF members, if that country is to be viewed as complying with international standards for

F. Alternative Remittance Systems
G. Wire Transfers
H. Non-Profit Organizations
I. Cash Couriers
J. Self-Assessment Questionnaire on Terrorist Financing

A. Ratification and Implementation of United Nations Instruments
B. Criminalizing the Financing of Terrorism and Associated Money Laundering
C. Freezing and Confiscating Terrorist Assets
D. Reporting Suspicious Transactions Related to Terrorism
E. International Cooperation
CFT.\(^1\) Countries may also wish to consult the Methodology on AML/CFT for information on how the **Special Recommendations** are evaluated.\(^2\) Moreover, FATF specifically invited all countries to adopt the **Special Recommendations** and participate in its self-assessment exercise.\(^3\) Implementation of the **Special Recommendations**, together with *The Forty Recommendations*, sets out the basic framework to detect, prevent and suppress terrorist financing.

The **Special Recommendations** are still relatively new. Thus, experience with interpreting and implementing them is somewhat limited. At first, FATF adopted general Guidance Notes to help explain the **Special Recommendations**.\(^4\) As it has gained experience over time, FATF has issued formal and more authoritative Interpretive Notes for several of the **Special Recommendations**.\(^5\) In addition, FATF has issued Best Practices guidance for several of the **Special Recommendations**.\(^6\) Finally, FATF has issued *Guidance for Financial Institutions in Detecting Terrorist Financing* as a means of helping financial institutions learn about mechanisms used to finance terrorism.\(^7\)

### A. Ratification and Implementation of United Nations Instruments

The first **Special Recommendation** consists of two parts.\(^8\) The first part provides that “each country is to take immediate steps to ratify and to implement fully the United Nations Convention for the Suppression of the Financing of Terrorism (1999).”\(^9\) Assessors of compliance with this recom-

---

mendation pay particular attention to the specific action that a country has taken to implement the various provisions of this convention.

The second part of the first Special Recommendation requires each country to implement fully United Nations (UN) Security Council Resolutions dealing with terrorist financing, particularly Security Council Resolution 1373. While the Special Recommendations specifically mention Resolution 1373, all such resolutions dealing with terrorist financing should be addressed by a country. Moreover, the universe of such resolutions is likely to change over time. Listed below, are the Security Council Resolutions currently listed as important in the “Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations”:

- S/RES/1267 (1999)
- S/RES/1363 (2001)

As with all UN conventions, actual implementation is the key to compliance for FATF purposes. Implementation means that a country has taken all appropriate and necessary measures in order to make the provisions of the UN Convention and the UN Security Council Resolutions effective, i.e. legally binding within its borders. These necessary measures may be accomplished by law, regulation, directive, decree or another appropriate legislative or executive action, according to the country’s constitutional and legal framework.

19. FATF, Guidance Notes, Paragraph 5.
20. Id.
Of the UN Security Council Resolutions dealing with terrorist financing, the one that is specifically mentioned in this Recommendation is Resolution 1373. This resolution obligates all UN member countries to:

- Criminalize actions to finance terrorism;
- Deny all forms of support for terrorist groups;
- Suppress the provision of safe haven or support for terrorists, including freezing funds or assets of persons, organizations or entities involved in terrorist acts;
- Prohibit active or passive assistance to terrorists; and
- Cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

B. Criminalizing the Financing of Terrorism and Associated Money Laundering

The second of the Special Recommendations contains two elements, which require that each country should:

- Criminalize the financing of terrorism, terrorist acts and terrorist organizations; and
- Establish terrorist offenses as predicate offenses of money laundering.

FATF has issued an Interpretive Note describing how a country should implement Special Recommendation II. This recommendation requires each country to criminalize the financing of terrorism, terrorist acts and terrorist organizations whether the funds were derived illegally (in which case the action should be a predicate offence for money laundering under the second element of the recommendation) or legally. The legislation should be specific in terms of criminalizing the financing of terrorism. It is not enough...
to criminalize “aiding and abetting” or “attempting” or “conspiracy.” This concept is not always clear enough in some legal systems. The legislation should also cover any person who collects or provides funds with the intention that the funds should be used for terrorism; it is not necessary to establish or prove that the funds were actually used for terrorism.

C. Freezing and Confiscating Terrorist Assets

Under the third Special Recommendation, each country should implement measures to freeze the “funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the UN resolutions.” Furthermore, each country should take appropriate action to authorize competent authorities within the country “to seize and confiscate property that are the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations.”

FATF has issued a formal Interpretive Note for the implementation of Special Recommendation III. In addition, FATF has also issued a set of Best Practices that should help countries understand how to best implement the requirements of this recommendation.

In this recommendation, there are three basic concepts that may have different meanings in different countries: freezing, seizure and confiscation (or forfeiture). “Freezing” means that a competent authority within a country has the authorization to block or restrain specific funds or assets and, thereby, prevent those funds or assets from being moved or otherwise dispersed. The “frozen” funds or assets remain the property of the owner and remain under the administration of the financial institution (or other entity) and under the control of existing management. The goal of freezing assets is to eliminate control over the assets by the owner so that the assets cannot be used for any prohibited purpose.

25. Id.
26. Id.
27. Special Recommendations, Spec. Rec. III.
28. Id.
“Seizure” means that the competent government authority has the authorization to take control of the specified funds or assets. 32 Under seizing, the assets or funds remain the property of the original owner, but possession, administration and management of the assets is taken over by the relevant competent authority. “Confiscation” or “forfeiture” means that the competent authority has authorization to transfer ownership of the specified funds or assets to the country itself. 33 Confiscation usually occurs when there is a criminal conviction or judicial decision that determined that the assets or funds were derived from criminal activity, or were intended to be used in violation of law.

The freezing of terrorist funds under the authority of the relevant UN resolutions should be done by administrative action without the need for further legislative or judicial procedures. Because implementation of U.N. Security Council resolutions is a binding legal obligation on member states, it should be possible for all countries to act immediately. Indeed it is very important that freezing action is immediate because if there is any delay, the funds are likely to be removed from the jurisdiction.

The United Nations 1267 Committee issues a consolidated list of individuals and organizations whose funds are ordered frozen under the various UNSCRs on Al-Qaeda, the Taliban and Osama bin-Laden. 34 The freezing order relates both to those individuals and organizations and anyone acting for them. The list is updated from time to time and a consolidated list is published on the UN website.

Under Special Recommendation III, countries should also have in place mechanisms to freeze funds of individuals or organizations involved in terrorism. This is also a general requirement under Security Council Resolution 1373. The Counter Terror Committee (CTC), acting under Resolution 1373, does not issue a list but gives the authority to individual countries to designate the persons and entities whose funds should be frozen. Countries should take into account the freezing action taken by other countries under Resolution 1373. 35 While there is no obligation to follow freezing action taken by other countries, such lists should be examined and, where appro-
D. Reporting Suspicious Transactions Related to Terrorism

Under the fourth of the *Special Recommendations*, financial institutions, that “suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations” should report promptly their suspicions to the competent authorities.36

This requirement applies to both financial institutions, as defined in *The Forty Recommendations*, and to the non-financial businesses and professions that are now defined in *The Forty Recommendations* (see Chapter 5).37 These reporting requirements must be consistent in the application of the country’s AML and CFT laws.

This recommendation involves reporting under two alternative circumstances: when there is a “suspicion” that funds are linked to terrorist financing; and when there are “reasonable grounds to suspect” that funds are linked to terrorist financing. The distinction between the two is the certainty that forms the standard for the required reporting of a transaction.38 The “suspect” standard is a subjective standard and is the same as that used in FATF’s AML recommendations.39 The “reasonable grounds to suspect” standard is consistent with the AML recommendation, but is somewhat broader than the pure “suspect” standards and, thereby, requires reporting under a broader set of circumstances. Countries can satisfy this reporting requirement based upon either the “suspicion” or “having reasonable grounds to suspect” standard.40

37. FATF, Guidance Notes, at Paragraph 19.
38. FATF, Guidance Notes, at Paragraph 21.
39. *The Forty Recommendations*, Rec. 1513, which provides: “If financial institutions suspect that funds stem from a criminal activity,” they should promptly report their suspicions.
40. FATF, Guidance Notes, at Paragraph 21.
E. International Cooperation

The fifth of the Special Recommendations, provides that each country should afford another country, through mutual legal assistance mechanism or other mechanisms, “the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.”41 Each country should also take all appropriate measures to assure that it does not provide safe havens for individuals charged with financing terrorism, terrorist acts or terrorist organizations, and should have procedures in place to extradite such persons, if possible.42

The first part of this recommendation mandates the exchange of information through mutual legal assistance mechanisms or means other than mutual legal assistance. “Mutual legal assistance” means the authority to provide a full range of legal assistance, including the taking of evidence; the search and seizure of documents or items relevant to criminal proceedings or criminal investigations; and the ability to enforce a foreign restraint, seizure, confiscation or forfeiture order in a criminal matter.43 Exchange of information by means “other than through mutual legal assistance” means any other arrangement, including an exchange occurring through financial intelligence units (FIUs) or other governmental agencies that exchange information bilaterally pursuant to memoranda of understanding (MOUs), exchange of letter or otherwise.44

The second part of this recommendation concerns the concepts of “safe haven” and “extradition.” These terms have the same meanings as the terms “safe haven,”45 as used in UN Security Resolution 1373,46 and “extradite,”47 as used in the UN International Convention for the Suppression of the Financing of Terrorism.48 With regard to extradition, countries should assure that “claims of political motivation are not recognized as a ground

42. *Id.*
43. FATF, Guidance Notes, at Paragraph 24.
44. *Id.*, at Paragraph 25.
45. *Id.*, at Paragraph 26.
46. UN Security Resolution 1373 (2001), at paragraph 2 (c).
47. *Id.*
for refusing requests to extradite persons alleged to be involved in terrorist financing.”49 This concept and phrasing are from the UN Convention on Suppression of the Financing of Terrorism.50

F. Alternative Remittance Systems

Under the sixth Special Recommendation, each country should take actions to ensure that individuals and legal entities that provide for “the transmission of money or value” are licensed or registered and subject to the same standards, i.e., The Forty Recommendations, that apply to other financial institutions.51 In addition, those entities that perform such services illegally should be subject to administrative, civil or criminal sanctions.52 Such requirements should apply the transmission of money or value through an informal transfer system.

FATF has issued an Interpretive Note as well as a set of Best Practices on Special Recommendation VI, in order to provide formal guidance and general assistance, respectively, to countries on how to implement this recommendation.53

Formal money remittance or transfer services are often provided by a distinct category of non-bank financial institutions, through which funds are moved on behalf of individuals or legal entities through a dedicated network or through the regulated banking system. For purposes of determining compliance with The Forty Recommendations, these money transmitters, which are included within the definition of the term “financial institutions,” should be subject to a country’s AML/CFT laws, and should be licensed or registered.54

The “money or value transfer system” refers to a type of financial service through which funds or value are moved from one geographic location to another through informal and unsupervised networks or mechanisms.55 In many jurisdictions, these informal systems have traditionally operated out-
side the regulated financial sector, as described above. Such informal systems include the Black Market Peso Exchange, hundi or Hawala systems.56

The goal of Special Recommendation VI is to assure that countries impose AML and CFT requirements on all forms of money/value transfer systems.57 Thus, at a minimum, a country should ensure that all money and value transmission services, including informal ones, are subject to specific FATF and international standards.58 Furthermore, a corollary requirement of this special recommendation is that a competent authority be designated to license or register all such informal money/value transmission services and to require these entities to have adequate programs to guard against money laundering and terrorist financing.59 Such a requirement is consistent with The Forty Recommendations.60

The international community is not, through this recommendation, attempting to eliminate informal money value transfer systems. In many cases, these systems provide a valuable service to people who cannot easily access the formal financial sector. However, there have been cases where such systems have been used to launder money and transfer funds to terrorists and this recommendation aims to apply AML/CFT controls to them. This recommendation also requires the compliance of such entities, but does not subject them to the same kind of requirements for regulation and supervision as an institution subject to the Basel Committee on Banking Supervision, International Association of Insurance Supervisors or International Organization of Securities Commissions.

G. Wire Transfers

Under the seventh Special Recommendation, each country should take appropriate actions to require covered financial institutions, including money remit-
Combating the Financing of Terrorism

Committed to include accurate and meaningful originator information (name, address and account number) on fund transfers and related messages that are sent, and further require that the information should remain with the transfer or related message throughout the payment chain. In addition, such financial institutions should conduct enhanced scrutiny of, and monitor for suspicious activity funds transfers that do not contain complete originator information.

The implementation of this recommendation has proven somewhat complex and FATF has produced a rather lengthy Interpretative Note to clarify the requirements of Special Recommendation VII. There is no set of Best Practices applicable to this recommendation.

The objective of this recommendation is to obtain information on who is sending wire transfers so that funds sent for illegal purposes can be identified along with their senders. The information requirements depend upon whether the transfer is cross-border or domestic. Cross-border transfers need to be accompanied by the name, account number (or unique reference number where there is no account e.g. one-off transactions), and address. An identity number or customer identification number or date and place of birth can be substituted for the address if there are fears about revealing the address of a customer. Providing this information on the wire transfer will enable information about the sender to be obtained much more quickly and easily if there is an international money laundering or terrorist financing investigation than if it has to be the subject of lengthy inquiries.

Domestic transfers need only to be accompanied by the account number, provided there is the ability to trace the rest of the information about the organization within three days of the sender institution receiving a request, either from the beneficiary institution or the authorities. Countries may exempt transactions of up to EUR/USD 3,000 from those requirements.

Beneficiary financial institutions should be able to identify wire transfers that do not show meaningful information. This is not a requirement to examine every transaction and it is very unlikely that the beneficiary institutions would be able to carry out any investigation about the accuracy of the

61. Special Recommendations, Spec. Rec. VII.
62. Id.
64. Id. At paragraph 1.
65. Id., at paragraph 8 and 9.
information. The originator of the funds transfers are not their customers. However, institutions should have systems in place to examine a sample of wire transfers. Where there is incomplete information institutions should consider filing a suspicious transaction report. Where a financial institution sends messages that do not include the required originator information, the beneficiary institution should reconsider the business relationship with the originator.67

H. Non-Profit Organizations

According to the eighth Special Recommendation, each country should review the adequacy of its laws and regulations regarding non-profit organizations, in order to determine whether they can be used for terrorist financing purposes.68 In particular, a country should ensure that its non-profit organizations cannot be misused:

- By terrorist organizations posing as legitimate ones;
- To exploit legitimate entities as conduits for terrorist financing, including to avoid asset freezing measures; or
- To conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.69

There is no Interpretive Note on this recommendation, however, in an effort to help countries protect their non-profit institutions from abuse, FATF has issued a set of international best practices entitled, Combating the Abuse of Non-Profit Organizations.70 The goal of this recommendation is to prevent non-profit organizations (i.e., those organized for charitable, religious, educational, social or fraternal purposes), as well as other legal entities and arrangements, from being misused by terrorists.71 In this regard, the recommendation is rather general because the different entities categorized as non-profit organizations take

---

67. Id., at paragraphs 11–14.
68. Special Recommendations, Spec. Rec. VIII.
69. Id.
71. FATF, Guidance Notes, at Paragraph 39.
various legal forms and the nature of their operations varies from jurisdiction to jurisdiction.\textsuperscript{72}

In an effort not to require adherence to a rigid set of rules that may be of little or no meaning in certain jurisdictions, the recommendation consists of general guidance and goals to be achieved, rather than specific requirements. There are three areas for attention by countries under the recommendation:

- \textit{Ensure financial transparency.} Such organizations should have transparent financial records and conduct their activities in a way that can be audited and funds accounted for. Accounts should be published and disbursements of funds should be done through accounts with established financial institutions.
- \textit{Programmatic verification.} The organizations should know who receives funds and how they are spent and should take active steps to monitor these things. This is especially important when the recipients are in another country.
- \textit{Administration.} There should be good records kept for the activities of the organization and there should be clear governance structures and internal accountability.

I. Cash Couriers

The objective of the ninth \textit{Special Recommendation}, which was adopted in October of 2004, is to ensure that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the transportation of currency and monetary instruments from one country to another.\textsuperscript{73} Persons or entities that carry cash and cash equivalents across national borders are often referred to as “cash couriers.”

\textit{Special Recommendation IX} has essentially four specific requirements regarding cash courier activities. First, each country should have a system in place to detect the physical cross-border transportation of currency and bearer negotiable instruments.\textsuperscript{74} Second, each country should provide its compe-
tent authorities with legal authority to stop or restrain currency and bearer negotiable instruments that are either: (i) suspected of being related to terrorist financing or money laundering; or (ii) misrepresented in a required declaration or disclosure. Third, this Special Recommendation further requires that each country have effective, proportionate, and dissuasive sanctions in place for persons making a false declaration or disclosure regarding a cross-border transportation of currency or bearer negotiable instrument(s). Fourth and finally, there is the requirement for each country to adopt measures permitting it to confiscate currency and bearer negotiable instruments that are related to terrorist financing or money laundering.

FATF adopted a formal Interpretative Note to accompany Special Recommendation IX at the same time that it adopted this recommendation.\(^75\) The Interpretative Note provides a reasonably thorough definition of the terms used in the recommendation as well as a reasonably thorough description of how a country may implement the requirements of this recommendation. FATF also adopted an International Best Practices paper, entitled “Detecting and Preventing the Cross-Border Transportation of Cash by Terrorists and Other Criminals,” to accompany this recommendation.\(^76\) A country may also wish to consult the best practices paper, which was adopted in February of 2005, for purposes of how to implement the requirements of Special Recommendation IX.

According to the Interpretative Note, “bearer negotiable instruments” means:

- monetary instruments in bearer form, such as travelers’ checks;
- negotiable instruments (including checks, promissory notes and money orders) that are in bearer form, endorsed to a fictitious payee, or otherwise in such a form that title passes upon delivery; or
- incomplete instruments (including checks, promissory notes and money orders) that are signed, but do not include the payee’s name.\(^77\)

It should be noted that, for purposes of this Special Recommendation, gold, precious metals and precious stones are specifically excluded from the

\(^{75}\) Interpretative Note to Special Recommendation IX.
\(^{77}\) Interpretative Note to Special Recommendation IX, at Paragraph 3.
meaning of the term “bearer negotiable instruments.” 78 Disclosures, declarations or other representations regarding these items may, nonetheless, be covered under a country’s legal requirements, such as its customs laws or regulations, but it is not necessary to cover them in order to comply with this recommendation. 79

“Physical cross-border transportation” means any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another. It includes: physical transportation (i) by a natural person, or in that person’s luggage or vehicle; (ii) shipment through containerized cargo; or (iii) mailing by a natural or legal person. 80

Under the Interpretative Note, a country may satisfy the recommendation’s requirement to have detection measures in place through the use of one of two systems: a declaration system or a disclosure system. 81 With a “declaration system,” all persons making a physical cross-border transportation of currency or bearer negotiable instrument(s) having a specified threshold value (maximum value may not exceed EUR/USD 15,000) or more, would be required to submit a truthful declaration to designated competent authorities regarding the value of such transfer and other relevant information. The predetermined threshold should be set sufficiently low to meet the objectives of the recommendation. 82

With a “disclosure system,” all persons making a cross-border transportation of currency or bearer negotiable instrument(s) would be required to make a truthful disclosure to designated competent authorities upon request regarding the value of the transfer and other relevant information. 83 In this regard, a country should ensure that competent authorities are authorized to make their requests on a targeted basis, either upon intelligence or suspicion, or on a random basis.

It is important to note that a country needs to have a detection system in place for both in-coming and out-going transportations, but does not have to use the same type of system for in-coming and out-going transportations. 84

78. Id., at footnote 1.
79. Id.
80. Id., at Paragraph 5.
81. Id., at Paragraph 9.
82. Id., at Paragraph 9a.
83. Id., at Paragraph 9b.
84. Id., at Paragraphs 9 and 10a.
Thus, for example, a country could have a declaration system for in-coming transportations and a disclosure system for out-going transportations, and vice-versa.

A false declaration or disclosure is defined to mean:

• a misrepresentation of the value of the currency or bearer negotiable instrument(s) being transported,
• a misrepresentation of any relevant data that is asked for in the required declaration or disclosure or otherwise requested by competent authorities, or
• the failure to make a declaration or disclosure as required.85

Upon discovery of either a false declaration or false disclosure, the designated competent authority should have the legal authority to request and obtain additional information from the person with regard to the origin of the subject currency or bearer negotiable instrument(s) and the intended use of such currency or instruments.86

Regardless of which system is utilized, information obtained through the declaration and/or disclosure processes should be made available to the financial intelligence unit (FIU).87 In addition, the declaration and/or disclosure process should permit the greatest possible range of international cooperation and assistance in accordance with The Forty Recommendations, specifically Recommendations 35 through 40, and Special Recommendation V.88 In this regard, where declarations or disclosures above the maximum threshold are made, where false declarations or disclosures are discovered, or where there are suspicions of money laundering or terrorist financing, relevant information should be retained, including the amount of currency or bearer instrument(s) declared, disclosed or discovered, and the identification data of the persons.89

With regard to persons carrying out the physical transportation of currency or bearer negotiable instruments that are actually related to terrorist financing or money laundering, such currency or bearer negotiable

---

85. Id., at Paragraphs 6 and 7.
86. Id., at Paragraph 10b.
87. Id., at Paragraph 10c.
88. Id., at Paragraph 10f.
89. Id.
instruments should be subject to measures, including legislative ones, consistent with *The Forty Recommendations* (Recommendation 3) and *Special Recommendation III*, that would permit their confiscation.\(^9\) Prior to such a determination, where there is either a: (i) suspicion of terrorist financing or money laundering; or (ii) false declaration or disclosure, competent authorities should have the legal authority to stop or restrain the subject currency and/or bearer negotiable instrument(s) for a reasonable time to determine whether there is evidence of terrorist financing.\(^{10}\)

Finally, countries are encouraged to implement *Special Recommendation IX* subject to safeguards to ensure the proper use of information received and without restricting either trade payments between countries for goods and services or the freedom of capital movements in any way.\(^{11}\)

### J. Self-Assessment Questionnaire on Terrorist Financing

In order to focus on issues of interpretation and implementation with regard to the *Special Recommendations*, FATF issued a Self Assessment Questionnaire on Terrorist Financing (SAQFT).\(^{12}\) The SAQFT was initially used only by FATF members. Upon completion of the initial assessment of the SAQFT, FATF issued the Guidance Notes on the *Special Recommendations* and the SAQTF. The SAQTF is also available on the FATF website and may be used by any country for its own assessment purposes.\(^{13}\)

---

\(^9\) *Special Recommendation IX* and Interpretative Note to Special Recommendation IX, at paragraph 11.

\(^10\) Interpretative Note to Special Recommendation IX, at paragraph 10e.

\(^11\) Interpretative Note to Special Recommendation IX, at paragraph 10e.

\(^12\) [http://www.fatf-gafi.org/SAQTF_en.htm](http://www.fatf-gafi.org/SAQTF_en.htm).

\(^13\) Id.
Chapter X

World Bank and International Monetary Fund Initiatives to Fight Money Laundering and Terrorist Financing

A. Awareness Raising
1. The Global Dialogue Series
2. Country Assistance Strategy

B. Development of a Universal AML/CFT Assessment Methodology
1. Twelve-Month Pilot Program
2. Reports on the Observance of Standards and Codes
3. Revision of the Universal Methodology

C. Building Institutional Capacity
1. Organization of Training Conferences
2. Delivery of Technical Assistance to Individual Countries

D. Research and Analysis
1. Analysis of the Hawala System
2. Alternative Remittance System Studies
3. World Bank AML/CFT Website
4. FIU Handbook
5. Reference Guide

The missions of the World Bank (Bank) and the International Monetary Fund (IMF or Fund) are fundamentally different. Nonetheless, both organizations have identical goals with regard to anti-money laundering (AML) and combating the financing of terrorism (CFT). Moreover, the Bank and the Fund work jointly in all of their efforts to achieve those goals.

The basic mission of the Bank is to fight poverty throughout the world. The Bank helps countries strengthen their development efforts by providing loans and technical assistance for institutional capacity building, as well as loans for improvements in the infrastructure and environment of developing countries. The mission of the Bank includes providing resources, sharing knowledge and forging partnerships in the public and private sectors.¹

In essence, the mission of the IMF is macro-economic and involves financial stability surveillance throughout the world. IMF goals include:

Promoting international monetary cooperation;
• Facilitating the expansion and balanced growth of international trade;
• Promoting foreign currency exchange stability; and
• Assisting in the establishment of multilateral systems of payments.

In addition, the Fund promotes international monetary stability by making loans to countries to permit them to correct maladjustments in their balance of payments without resorting to measures that may destroy national or international prosperity.2

In April 2001, the two Boards of Executive Directors of the World Bank and the IMF recognized that money laundering is a problem of global concern that affects major financial markets and smaller ones.3 Taking into account that money laundering has potentially devastating economic, political and social consequences for countries that are in the process of developing domestic economies and building strong financial institutions, the Bank recognized that money laundering can impose important costs upon developing countries. The IMF recognized that money laundering has a full range of macroeconomic consequences, including unpredictable changes in money demand, risks to the soundness of financial institutions and financial systems, and increased volatility on international capital flows and exchange rates due to unanticipated cross border transfers.

Following the events of September 11, 2001, the World Bank and IMF Boards of Executive Directors adopted action plans to enhance efforts for AML/CFT. Furthermore, the Boards recognized, in July and August 2002, The Forty Recommendations on Money Laundering (The Forty Recommendations) and the eight Special Recommendations on Terrorist Financing (Special Recommendations), issued by the Financial Action Task Force on Money Laundering (FATF), as the relevant international standards for AML/CFT. The Boards added AML and CFT to the list of areas that are useful for their operational work and started a 12-month pilot program using

a universal, comprehensive AML/CFT assessment methodology in November 2002.

Over the course of the pilot program, the Fund and the Bank conducted assessments in 33 jurisdictions and FATF and the FATF-style regional bodies (FSRBs) conducted assessments in an additional eight jurisdictions. The Boards of the Fund and the Bank reviewed the outcome of the pilot program in March 2004. They concluded that the pilot had been successful and welcomed the deepening of international attention that it had led to on AML/CFT issues and the good collaboration that had taken place with FATF and the FATF-style regional bodies (FSRBs). At that time, the Boards resolved to make AML/CFT work a permanent part of their activities; to continue their collaboration with the FATF; to endorse the revised FATF recommendations as the new standard for which Reports on the Observance of Standards and Codes (ROSCs) are prepared and the revised Methodology to assess that standard; and to devote additional resources to this work in the future. The Fund and Bank expect to conduct approximately 20 assessments per year using the same Methodology used by FATF and the FSRBs.

A. Awareness Raising

1. The Global Dialogue Series
The first step in establishing or improving a country’s institutional framework for AML and CFT is to raise the awareness level within the country’s leadership about the issues, to demonstrate the implications for the country’s future, to share the experiences that other countries have had, and to inform the country about available resources and assistance. Toward that goal, the World Bank and IMF have established a series of Regional Policy Global Dialogues on AML/CFT. These are organized through interactive videoconferences for member countries within a given geographic region enabling government officials from those countries, staff of the Bank and Fund, FATF-Style Regional Bodies (FSRBs), regional development banks and other international organizations to discuss and exchange information. The issues discussed center upon:

- Identifying the challenges faced by countries in the struggle against illicit money flows;
• Sharing the lessons of success;
• Identifying specific problems for countries in that region; and
• Understanding the types of assistance countries need to combat money laundering and terrorist financing.

Some of the key questions addressed in the Global Dialogue Series are:

• How can the World Bank and IMF help countries strengthen their response to money laundering and terrorist financing?
• How does money laundering and terrorist financing fit into the broader context of corruption and poor governance?
• What has been the response of governments?
• What are the current challenges for regulators?
• What is the appropriate institutional structure for each country in implementing an effective program to fight money laundering and terrorist fighting?
• What are the future challenges in combating money laundering and terrorist financing in participating countries?

To answer those questions, senior policymakers in the participating countries offer their views on the economic costs of criminal abuse of financial systems, particularly money laundering and the financing of terrorism. Other points for discussion include practical means of sustaining economic development and financial market integrity in the face of such threats. The dialogue helps countries to learn from each other by drawing on their particular experiences as well as the broader experience of international experts.

2. Country Assistance Strategy

The Bank is integrating the results of the Financial Sector Assessment Program (FSAP) into the broader range of development measures considered in the Country Assistance Strategy (CAS), which sets out the priorities for the Bank’s program for a given country on a three-year basis in consultation with the government of that country. Following systematic reviews of FSAP findings, AML/CFT assistance has already been included in more than 30
CASs prepared since March 2002. Technical assistance is given high priority in countries where weaknesses in the integrity of the AML/CFT regime may pose significant governance and development risks. CASs also address AML/CFT issues in greater detail in countries that have been deficient in meeting international standards and best practices.

The Fund has integrated AML/CFT components into its Article IV surveillance. In addition to Financial System Stability Assessment (FSSA) reports to the Executive Board (which summarize the outcome of FSAPs, including the AML/CFT assessments), results from the AML/CFT questionnaire have been incorporated in more than 70 Article IV discussions since January 2002.

B. Development of a Universal AML/CFT Assessment Methodology

Over the course of 2002, the Bank and IMF worked in close collaboration with FATF and other international standard setters, i.e., the Basel Committee on Banking Supervision (Basel Committee), International Association of Securities Commissioners (IOSCO), International Association of Insurance Supervisors (IAIS) and the Egmont Group, to produce a single, comprehensive AML/CFT assessment methodology. This methodology was agreed and endorsed by FATF at its October 2002 Plenary meeting. The methodology consisted of 120 criteria covering each of the FATF Forty and Special Recommendations, including implementation of criminal law enforcement. It covered the legal and institutional AML/CFT framework for a country, including the establishment of financial intelligence units (FIUs). The methodology also covered relevant United Nations (UN) Security Council Resolutions and international conventions and other measures of international standard setters. It provided an in-depth assessment of the preventive measures for financial institutions.

Following the revision of The Forty Recommendations in June 2003, the Bank and Fund worked with the FATF and FSRBs to produce a revised assessment methodology. This was endorsed by the FATF in February 2004.

---

and by the Bank and Fund Boards in March 2004. It incorporates over
200 “essential criteria” against which countries will be assessed for their
compliance with the FATF standards and some “additional criteria” which,
although not part of the standard against which compliance is rated, com-
prise international best practices and will be part of the assessment. There are
considerably more criteria than in the previous version of the methodology,
reflecting the extension of the standards agreed in 2003.

The methodology will be used by the international organizations in their
evaluations of AML/CFT controls carried out as part of their overall assess-
ments of a country’s compliance with international financial standards in the
FSAP and OFC processes. They will result in a ROSC for AML/CFT, which
will be reported to the Executive Boards of the Bank and the Fund. The
methodology will also be used by the FATF and FSRBs in their mutual evalu-
ations. FATF and the FSRBs will prepare a ROSC as part of their mutual evalua-
tions, which will be recognized by the Bank and the Fund.

The process is one in which the FATF, FSRBs, the Bank, and the Fund
each carry out assessments using the same methodology and agree to rec-
ocnize each others reports. The organizations work together to establish a
sensible schedule for assessments, which fits in with the FSAP/OFC schedule
of the international financial institutions and FATF/FSRB mutual evaluation
timetables. It is expected that the Fund and the Bank will conduct approxi-
mately 20 assessments per year, and that FATF and the FSRBs will conduct
about the same number. This schedule should allow every country to receive
a full assessment approximately once every five years.

C. Building Institutional Capacity

1. The Organization of Training Conferences

The Bank and Fund hold targeted training conferences on specific AML/CFT
issues, utilizing public officials involved in AML/CFT from a particular
region. For example, during 2002, two technical assistance conferences took
place: one in Montevideo, Uruguay, and one in Moscow, Russia.

The Moscow conference is illustrative of the type of information presented.
The focus of the conference was the creation of operational Financial Intelligence
World Bank and International Monetary Fund Initiatives

Sections:

1. World Bank and International Monetary Fund Initiatives
   - Units (FIUs): The conference was aimed at those countries that either do not have operational FIUs or that have just started operating them. The primary aim of the conference was to involve experts from Eastern European countries that have recently achieved AML/CFT compliance standards, and allow officials from those countries to present their experience and best practices.
   - The conference was also a useful mechanism to help countries and organizations that provide AML/CFT technical assistance understand where the most urgent needs are, and to enable them to make personal contacts with government officials of those countries so future assistance might be more readily and easily provided.
   - The conference was successful in demonstrating the importance of attention to AML/CFT issues, and presenting the various requirements of international standards in such a manner that officials from participating countries could understand. It also demonstrated the specific steps necessary to begin taking action in their respective countries. Additionally, government officials were able to make personal contacts with experts in the field as well as their counterparts in their own neighboring countries, which makes obtaining advice and assistance in implementing AML/CFT less burdensome.
   - A further workshop was held in South Africa in May 2004, involving the 14 member countries of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). It was organized by ESAAMLG with the participation of the Bank and Fund and included experts from several other international organizations and countries. The aim of the workshop was to inform policy makers from the ESAAMLG countries of the basic elements of a national strategy to counter money laundering and terrorist financing and work with them to develop their strategies to tackle the major AML/CFT issues in each country. The participants worked at the meeting to produce outline strategies which were then to be further developed in the country before being finalized and presented to the ESAAMLG plenary in August 2004.

2. Delivery of Technical Assistance to Individual Countries
   - The Bank and the Fund are providing various forms of technical assistance (TA) to countries that want to establish or improve their AML/CFT
regimes. Since April of 2001, these TA efforts have increased. The Bank and Fund use the findings from the FSAPs and separate AML/CFT reviews as a means of determining what TA is needed and prioritizing the TA.

For developing countries, AML/CFT TA is included in a jurisdiction’s CAS, which sets out the priorities for the Bank’s assistance program on a three-year basis in consultation with the government of the country. In particular, TA is given high priority in countries where weakness in the integrity of the AML/CFT may pose significant governance and developmental risks.

The focus of the Bank’s and the Fund’s TA for AML/CFT is on:

- Formulation of AML/CFT laws and regulations that meet international best practices;
- Implementation of laws, regulations, policies and procedures by financial sector supervisors and other similar competent authorities charged with responsibility for enforcement of AML/CFT measures;
- Establishment of legal frameworks for financial intelligence units (FIUs) that meet international best practices;
- Development of training and awareness programs to address AML/CFT concerns in the public and private sectors;
- Collaboration with other parties in multinational training programs; and development of computer-based training materials.

In the two-year period leading up to the March 2004 decision by the Bank and Fund boards to make AML/CFT a permanent part of their work programs, the Bank and Fund delivered 85 country-specific technical assistance projects reaching 63 countries and 32 regional projects reaching over 130 countries.

---

D. Research and Analysis

1. Analysis of the Hawala System

The Bank and the Fund conducted a study on the operational characteristics of informal funds transfer systems (IFTs), commonly referred to as Hawalas.7 The study examines the historical and socioeconomic context within which Hawalas have evolved. In this regard, their growth is rooted primarily in the facilitation of trade between distant geographic locations at a time when conventional banking instruments were either weak or nonexistent.

The study also analyzes the operational features of IFTs for both legitimate and illegitimate purposes. These operational features are mainly speed, lower transaction costs, ethnic and cultural convenience and familiarity, versatility and potential anonymity. In addition, IFTs have prospered in countries where financial institutions are inefficient and financial policies are restrictive. Finally, like any underground economic activity, IFTs have implications for monetary control; influencing exchange rate operations; distorting economic data, (and, thereby, statistical information available to policy makers); and reducing taxes on income and services.

The study further discusses the implications for regulatory and supervisory responses to this type of activity. Recommendation VI of FATF’s Special Recommendations recommends that countries treat Hawalas and other IFTs as part of the regulated system, subject to many of the same AML/CFT requirements as covered financial institutions.8 More countries are subjecting these entities to licensing or registration in accordance with the FATF recommendation.

2. Alternative Remittances Systems Studies

In September of 2002, the Asia-Pacific Economic Cooperation (APEC) Finance Ministers established a working group on alternative remittance systems (ARS) to examine the economic, structural and regulatory factors

---

that encourage the use of ARS in the APEC economies. In support of the project, the World Bank prepared a report that creates a framework for estimating the magnitude of remittances flows, analyzes incentives for formal versus informal channels, and examines the role of formal financial sectors in the provision of remittance services that are compliant with international AML/CFT standards.  

As part of the APEC ARS Initiative follow-up, and as part of an effort to increase the World Bank’s involvement in studying the important topic of ARSs for all of its clients, comparative case studies have been planned for specific economies. Research findings and conclusions of these case studies will be shared as part of the exchange of ideas and experiences. This is an ongoing project; the findings from different studies will be reported and available on the Bank’s AML/CFT website.

3. World Bank AML/CFT Website

The Bank operates a website specifically for AML/CFT purposes. This website contains up-to-date information about the Bank’s programs and efforts to combat money laundering and terrorist financing. It also contains reference materials and publications, such as this Reference Guide. The website may be accessed at www.amlcft.org. Those wishing to contact the Bank on AML/CFT matters should write aml@worldbank.org.

4. FIU Handbook

In 2004, the Fund and the Bank jointly published a handbook on virtually all aspects of the establishment and operation of financial intelligence units (FIUs). The handbook is entitled Financial Intelligence Unit, An Overview.  

11. The handbook is available for purchase from the IMF. It is also available for viewing (read-only) on the Bank’s AML/CFT website, http://www.amlcft.org.
The handbook covers a wide array of topics relating to FIU, including:

- Key steps for establishing an FIU,
- Basic models of operation,
- Core functions,
- Additional functions, and
- International assessments.

5. The Reference Guide

This Reference Guide on AML and CFT is a product of the Bank’s and Fund’s efforts to fight money laundering and terrorist financing. When policy makers looked at the AML/CFT material available to a country, particularly a developing country with limited experience in the area, it quickly became apparent that there was no single source that could be used to address all the issues. Hence, the Bank and Fund commissioned this Reference Guide as a means to make all relevant information available from a single and comprehensive source.

The first edition was published in 2003 and made available in five languages (English, French, Russian, Arabic and Spanish). This second edition has been prepared as an update, following the revision of The Forty Recommendations in June 2003,12 the revised Methodology for assessments in 2004,13 other changes in relevant materials, and subsequent developments in Fund and Bank AML/CFT programs and activities.

The Reference Guide is available on the Bank’s website, http://www.amlcft.org/, and will also be translated into other languages.

---

Annex I

Websites for Key Organizations, Legal Instruments, and Initiatives

**Basel Committee on Banking Supervision—Bank For International Settlements**

- http://www.bis.org/ (BIS Home Page)
- http://www.bis.org/bcbs/ (Basel Committee on Banking Supervision)
- http://www.bis.org/publ/bcbs30.pdf (Core Principles for Effective Banking Supervision)
- http://www.bis.org/publ/bcbs61.pdf (Core Principles Methodology)
- http://www.bis.org/publ/bcbs85.htm#pgrtop (Customer Due Diligence for Banks)

**Commonwealth Secretariat**

- http://www.thecommonwealth.org/ (Main site)
• http://www.thecommonwealth.org/dynamic/Country.asp (Commonwealth countries)

Council Of Europe
• http://www.coe.int/portalT.asp (Main page)

Egmont Group For Financial Intelligence Units (FIUs)
• http://www.egmontgroup.org/ (Main page)
• http://www.egmontgroup.org/list_of_fius_062304.pdf (Countries with operational Financial Intelligence Units)
• http://www.egmontgroup.org/procedure_for_being_recognised.pdf (Procedure for being recognized as member country)
• http://www.fincen.gov/fiuinaction.pdf (List of AML cases)

European Union
• http://europa.eu.int/ (Main page)

Financial Action Task Force on Money Laundering (FATF)
• http://www.fatf-gafi.org (Welcome page)
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives

- http://www.fatf-gafi.org/FATDocs_en.htm (Money Laundering Methods and Trends)
- http://www1.oecd.org/fatf/pdf/PR-20021220_en.pdf (FATF statements and documents on NCCT, Press Release, December 20, 2002, FATF decides to impose counter-measures on Ukraine; no counter-measures to apply to Nigeria at this time)

FATF-Style Regional Bodies

Asia/Pacific Group on Money Laundering
- http://www.apgml.org (Main site)
• http://www.apgml.org/content/member_jurisdiction.jsp (Member Jurisdictions)
• http://www.apgml.org/content/observer_jurisdiction.jsp (Observer Jurisdictions)
• http://www.apgml.org/content/organisations.jsp (Observer Organisations)

Caribbean Financial Action Task Force
• http://www.cfatf.org (Main site)
• http://www1.oecd.org/fatf/Ctry-orgpages/org-cfatf_en.htm (Co-operating and Supporting Nations and Observers)
• http://www.cfatf.org/about/about.asp?PageNumber=1 (Membership)
• http://www.cfatf.org/eng/kingdec/index.pdf (Kingston Declaration on Money Laundering—November 5–6, 1992)

MONEYVAL (Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV Committee), (Now known as MONEYVAL)
• http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/Money_laundering/ (Main site)
• http://www1.oecd.org/fatf/Ctry-orgpages/org-pcrev_en.htm (Members and Observers)

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
• http://www.esaamlg.org (Main site)
• http://www1.oecd.org/fatf/Ctry-orgpages/org-esaamlg_en.htm (Members and Observers)

Financial Action Task Force of South America (GAFISUD)
• http://www.gafisud.org (Main site)
• http://www.gafisud.org (See members and observers)
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives

**International Association of Insurance Supervisors**
- http://www.iaisweb.org/ (Main page)
- http://www.iaisweb.org/framesets/pas.html (Overview of IAIS principles, standards and guidance papers)
- http://www.iaisweb.org/132_176_ENU_HTML.asp (Member countries and jurisdictions)

**International Monetary Fund**
- http://www.imf.org/ (Main page)

**International Organization of Securities Commissioners**
- http://www.iosco.org/iosco.html (Main page)

**Organization of American States–CICAD**
- http://www.oas.org/main/english/ (Main page)
• http://www.cicad.oas.org/Desarrollo_Juridico/eng/legal-regulations-money.htm (Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses (1998)

United Nations

• http://www.un.org
• http://www.undcp.org/ (Office on Drugs Control and Crime)
• http://www.un.org/Overview/unmember.html (List of Member Sates)
• http://www.unodc.org/unodc/crime_cicp_signatures_convention.html (Signatories–Convention against Transnational Organized Crime)
• http://www.untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty11.asp (Status–Convention of the Suppression of the Financing of Terrorism)
• http://www.un.org/aboutun/charter/index.html (UN Charter)
• http://untreaty.un.org/English/Terrorism.asp (United Nations Treaty Collection Conventions on Terrorism)
• http://www.un.org/terrorism/ (UN Action against Terrorism)
• http://www.un.org/sc/ctc (Counter-Terrorism Committee)
• http://www.unodc.org/unodc/treaty_adherence.html (List of member countries)
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives


United Nations–International Money Laundering Information Network
• http://www.imolin.org/ (Main page)
• http://www.imolin.org/imolin/gpml.html (United Nations Global Program Against Money Laundering)
• http://www.imolin.org/conventi.htm (Standards, Conventions and Legal Instruments)
• http://www.imolin.org/model.htm (Model Laws/Regulation)
• http://www.imolin.org/map.htm (National legislation relating to money laundering (map))
• http://www.imolin.org/reference.htm (Reference)
• http://www.imolin.org/current.htm (Current Events in the Anti-Money Laundering Arena)
• http://www.imolin.org/calendar.htm (Calendar of Events)

United Nations–Security Council Resolutions
• http://www.un.org/documents/scres.htm

Wolfsberg Group of Banks
• http://www.wolfsberg-principles.com/index.html (The Wolfsberg Group of Banks)
• http://www.wolfsberg-principles.com/privat-banking.html (Global Anti-Money-Laundering Guidelines for Private Banking)
• http://www.wolfsberg-principles.com/wolfsberg_statement.html (The Suppression of the Financing of Terrorism)

The World Bank Group
• http://www.worldbank.org/
• http://www.amlcft.org (Financial Market Integrity website on anti-money laundering and terrorist financing)
Annex II

Other Useful Websites and Resources

Websites

European Central Bank

- http://www.ecb.int/

The Financial Crimes Enforcement Network (FinCEN)

- http://www.fincen.gov/af_main.html

Financial Stability Forum

- http://www.fsforum.org/

Interpol

- http://www.interpol.com/Public/Terrorism/default.asp (Interpol's involvement in the fight against international terrorism)
The Money Laundering Compliance Website


Organisation for Economic Co-operation and Development


U.S. Department of the Treasury, Comptroller of the Currency, Administrator of National Banks


U.S. State Department—Country Summaries


The World Customs Organization

- [http://www.wcoomd.org/ie/index.html](http://www.wcoomd.org/ie/index.html) (Main page)

Other Resources

Annex III

United Nations Anti-Terrorist Conventions Referred to in the International Convention for the Suppression of the Financing of Terrorism

A. Legal Systems

Scope of the criminal offence of money laundering


Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.
Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year’s imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences.1

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisional measures and confiscation

---

1. See the definition of “designated categories of offences” in the Glossary.
3. Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. Measures to Be Taken by Financial Institutions and Nonfinancial Businesses and Professions to Prevent Money Laundering and Terrorist Financing

4. Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer due diligence and record-keeping

5. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

• establishing business relations;

* Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.
• carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
• there is a suspicion of money laundering or terrorist financing; or
• the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.  

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

2. Reliable, independent source documents, data or information will hereafter be referred to as “identification data.”
Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

6.* Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

   a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
   b) Obtain senior management approval for establishing business relationships with such customers.
   c) Take reasonable measures to establish the source of wealth and source of funds.
   d) Conduct enhanced ongoing monitoring of the business relationship.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

   a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to
a money laundering or terrorist financing investigation or regulatory action.
b) Assess the respondent institution’s anti-money laundering and terrorist financing controls.
c) Obtain approval from senior management before establishing new correspondent relationships.
d) Document the respective responsibilities of each institution.
e) With respect to “payable-through accounts”, be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

8. Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with nonface to face business relationships or transactions.

9.* Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

10. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

11. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12. The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a) Casinos—when customers engage in financial transactions equal to or above the applicable designated threshold.
b) *Real estate agents*—when they are involved in transactions for their client concerning the buying and selling of real estate.

c) *Dealers in precious metals and dealers in precious stones*—when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) *Lawyers, notaries, other independent legal professionals and accountants* when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

13. If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14. Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they
did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15. Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:
   a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
   b) An ongoing employee training programme.
   c) An audit function to test the system.

16. The requirements set out in Recommendations 13 to 15, and 21 apply to all designated nonfinancial businesses and professions, subject to the following qualifications:
   a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
   b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
   c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk. Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to...
help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

23. Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.
24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

   a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

   - casinos should be licensed;
   - competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino
   - competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

   b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

25. The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.
C. Institutional and Other Measures Necessary in Systems for Combating Money Laundering and Terrorist Financing

Competent authorities, their powers and resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.
30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

33. Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

34. Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure
that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

**D. International Co-operation**

35. Countries should take immediate steps to become party to and implement fully the *Vienna Convention*, the *Palermo Convention*, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

**Mutual legal assistance and extradition**

36. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

   a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.
   b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.
   c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
   d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.
Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

37. Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

38. There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

39. Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.
Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrest or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

40. Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.
b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.
c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.
Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

**Glossary**

In these Recommendations the following abbreviations and references are used:

“**Beneficial owner**” refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

“**Core Principles**” refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

“**Designated categories of offences**” means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
• murder, grievous bodily injury;
• kidnapping, illegal restraint and hostage-taking;
• robbery or theft;
• smuggling;
• extortion;
• forgery;
• piracy; and
• insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

“Designated non-financial businesses and professions” means:

a) Casinos (which also includes internet casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants—this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
– providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
– acting as (or arranging for another person to act as) a trustee of an express trust;
– acting as (or arranging for another person to act as) a nominee shareholder for another person.

“Designated threshold” refers to the amount set out in the Interpretative Notes.

“Financial institutions” means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.³
2. Lending.⁴
3. Financial leasing.⁵
4. The transfer of money or value.⁶
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller’s cheques, money orders and bankers’ drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   a) money market instruments (cheques, bills, CDs, derivatives etc.);
   b) foreign exchange;
   c) exchange, interest rate and index instruments;
   d) transferable securities;
   e) commodity futures trading.

³ This also captures private banking.
⁴ This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).
⁵ This does not extend to financial leasing arrangements in relation to consumer products.
⁶ This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

Annex IV-20
8. Participation in securities issues and the provision of financial services related to such issues.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.\(^7\)

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

“FIU” means financial intelligence unit.

“Legal arrangements” refers to express trusts or other similar legal arrangements.

“Legal persons” refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

“Payable-through accounts” refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

---

\(^7\) This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).
“Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, 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. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

“Shell bank” means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

“STR” refers to suspicious transaction reports.

“Supervisors” refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

“the FATF Recommendations” refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

Interpretative Notes to the Forty Recommendations

General

1. Reference in this document to “countries” should be taken to apply equally to “territories” or “jurisdictions.”

2. Recommendations 5–16 and 21–22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations
under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.

4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

5. The Interpretative Notes that apply to financial institutions are also relevant to designated nonfinancial businesses and professions, where applicable.

Recommendations 5, 12 and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5)—USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12)—USD/EUR 3,000.
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16)—USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.
Recommendation 5

CUSTOMER DUE DILIGENCE AND TIPPING OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.
   
   b) Make a STR to the FIU in accordance with Recommendation 13.

2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer’s awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD FOR LEGAL PERSONS AND ARRANGEMENTS

4. When performing elements (a) and (b) of the CDD process in relation to legal persons or arrangements, financial institutions should:
a) Verify that any person purporting to act on behalf of the customer is so authorised, and identify that person.

b) Identify the customer and verify its identity—the types of measures that would be normally needed to satisfactorily perform this function would require obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer’s name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

The relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

**RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED**

5. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer’s account is operated which is not consistent with the customer’s business profile.
TIMING OF VERIFICATION

6. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
- Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.

7. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification.

These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. Financial institutions should refer to the Basel CDD paper \(^8\) (section 2.2.6.) for specific guidance on examples of risk management measures for non-face to face business.

---

**Requirement to identify existing customers**

8. The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant.

**Simplified or reduced CDD measures**

9. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

10. Examples of customers where simplified or reduced CDD measures could apply are:

   - Financial institutions—where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls.
   - Public companies that are subject to regulatory disclosure requirements.
   - Government administrations or enterprises.

11. Simplified or reduced CDD measures could also apply to the beneficial owners of pooled accounts held by designated non financial businesses or professions provided that those businesses or professions are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring their compliance with those requirements. Banks
should also refer to the Basel CDD paper (section 2.2.4.), which provides specific guidance concerning situations where an account holding institution may rely on a customer that is a professional financial intermediary to perform the customer due diligence on his or its own customers (i.e. the beneficial owners of the bank account). Where relevant, the CDD Paper could also provide guidance in relation to similar accounts held by other types of financial institutions.

12. Simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- Life insurance policies where the annual premium is no more than USD/EUR 1000 or a single premium of no more than USD/EUR 2500.
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member’s interest under the scheme.

13. Countries could also decide whether financial institutions could apply these simplified measures only to customers in its own jurisdiction or allow them to do for customers from any other jurisdiction that the original country is satisfied is in compliance with and has effectively implemented the FATF Recommendations.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Recommendation 6

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.
Recommendation 9

This Recommendation does not apply to outsourcing or agency relationships. This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.

Recommendations 10 and 11

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself, the premium payment and the benefits.

Recommendation 13

1. The reference to criminal activity in Recommendation 13 refers to:

   a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or
   b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

   Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.
Recommendation 14 (tipping off)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

Recommendation 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.
Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or “fit and proper”) tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.

Recommendation 25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

Recommendation 26

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

Recommendation 27

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use
of procedures such as controlled deliveries and undercover operations are precluded.

Recommendation 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Recommendation 40

1. For the purposes of this Recommendation:

   • “Counterparts” refers to authorities that exercise similar responsibilities and functions.
   • “Competent authority” refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the cooperation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.
3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.
I. Ratification and implementation of UN instruments
Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering
Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets
Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organis-
tions in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism
If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International co-operation
Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers
Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information
(name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organisations
Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

i. by terrorist organisations posing as legitimate entities;

ii. to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

iii. to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

IX. Cash couriers
Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.
Interpretative Note to Special Recommendation II: Criminalising the financing of terrorism and associated money laundering

OBJECTIVE

1. Special Recommendation II (SR II) was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and inter alia money laundering, another objective of SR II is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. The basis for criminalising terrorist financing should be the United Nations
DEFINITIONS

2. For the purposes of SR II and this Interpretative Note, the following definitions apply:

a) The term funds refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

b) The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

c) The term terrorist act includes:


---

1. Although the UN Convention had not yet come into force at the time that SR II was originally issued in October 2001—and thus is not cited in the SR itself—the intent of the FATF has been from the issuance of SR II to reiterate and reinforce the criminalisation standard as set forth in the Convention (in particular, Article 2). The Convention came into force in April 2003.

ii) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.

e) The term terrorist organisation refers to any group of terrorists that:
   (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

**Characteristics of the Terrorist Financing Offence**

3. Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.
4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.

5. Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. It should also be an offence to attempt to commit the offence of terrorist financing.

8. It should also be an offence to engage in any of the following types of conduct:

   a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
   b) Organising or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
   c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

9. Terrorist financing offences should be predicate offences for money laundering.

10. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.
11. The law should permit the intentional element of the terrorist financing offence to be inferred from objective factual circumstances.

12. Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.

13. Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

14. Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for terrorist financing.

Interpretative Note to Special Recommendation III: Freezing and Confiscating Terrorist Assets Objectives

1. FATF Special Recommendation III consists of two obligations. The first requires jurisdictions to implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant United Nations resolutions. The second obligation of Special Recommendation III is to have measures in place that permit a jurisdiction to seize or confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court.

2. The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative, while the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.
**Scope**

3. Special Recommendation III is intended, with regard to its first requirement, to complement the obligations in the context of the United Nations Security Council (UNSC) resolutions relating to the prevention and suppression of the financing of terrorist acts—S/RES/1267(1999) and its successor resolutions,\(^2\) S/RES/1373(2001) and any prospective resolutions related to the freezing, or if appropriate seizure, of terrorist assets. It should be stressed that none of the obligations in Special Recommendation III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding.\(^3\) The focus of Special Recommendation III instead is on the preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups.

4. S/RES/1267(1999) and S/RES/1373(2001) differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations.

5. S/RES/1267(1999) and its successor resolutions obligate jurisdictions to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267 (the Al-Qaida and Taliban Sanctions Committee), including funds derived from funds or other assets owned or controlled,

---


\(^3\) For instance, both the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) and UN Convention against Transnational Organised Crime (2000) contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Those obligations exist separately and apart from obligations that are set forth in S/RES/1267(1999), S/RES/1373(2001) and Special Recommendation III.
directly or indirectly, by them or by persons acting on their behalf or at their
direction, and ensure that neither these nor any other funds or other assets
are made available, directly or indirectly, for such persons’ benefit, by their
nationals or by any person within their territory. The Al-Qaida and Taliban
Sanctions Committee is the authority responsible for designating the per-
sons and entities that should have their funds or other assets frozen under
S/RES/1267(1999). All jurisdictions that are members of the United Nations
are obligated by S/RES/1267(1999) to freeze the assets of persons and entities
so designated by the Al-Qaida and Taliban Sanctions Committee.4

6. S/RES/1373(2001) obligates jurisdictions5 to freeze without delay the
funds or other assets of persons who commit, or attempt to commit, terrorist
acts or participate in or facilitate the commission of terrorist acts; of entities
owned or controlled directly or indirectly by such persons; and of persons
and entities acting on behalf of, or at the direction of such persons and
entities, including funds or other assets derived or generated from property
owned or controlled, directly or indirectly, by such persons and associated
persons and entities. Each individual jurisdiction has the authority to des-
ignate the persons and entities that should have their funds or other assets
frozen. Additionally, to ensure that effective co-operation is developed among
jurisdictions, jurisdictions should examine and give effect to, if appropriate,
the actions initiated under the freezing mechanisms of other jurisdictions.
When (i) a specific notification or communication is sent and (ii) the jurisdic-
tion receiving the request is satisfied, according to applicable legal principles,
that a requested designation is supported by reasonable grounds, or a reason-
able basis, to suspect or believe that the proposed designee is a terrorist, one
who finances terrorism or a terrorist organisation, the jurisdiction receiving
the request must ensure that the funds or other assets of the designated per-
son are frozen without delay.

4. When the UNSC acts under Chapter VII of the UN Charter, the resolutions it issues are manda-
tory for all UN members.
5. The UNSC was acting under Chapter VII of the UN Charter in issuing S/RES/1373(2001) (see
previous footnote).
DEFINITIONS

7. For the purposes of Special Recommendation III and this Interpretive Note, the following definitions apply:

a) The term freeze means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.

b) The term seize means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.

c) The term confiscate, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets.6

---

6. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court deci-
d) The term *funds* or *other assets* means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

e) The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts\(^7\) by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.

f) The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should

---


Annex VI-9
be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.

g) The term terrorist organisation refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s).

h) The term designated persons refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).

i) The phrase without delay, for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. The phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

**FREEZING WITHOUT DELAY TERRORIST-RELATED FUNDS OR OTHER ASSETS**

8. In order to fulfil the preventive intent of Special Recommendation III, jurisdictions should establish the necessary authority and adopt the following standards and procedures to freeze the funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with both S/RES/1267(1999) and S/RES/1373(2001):

a) **Authority to freeze, unfreeze and prohibit dealing in funds or other assets of designated persons.** Jurisdictions should prohibit by enforceable means the transfer, conversion, disposition or movement of funds or other assets. Options for providing the authority to freeze and unfreeze terrorist funds or other assets include:
i) empowering or designating a competent authority or a court to
issue, administer and enforce freezing and unfreezing actions under
relevant mechanisms, or

ii) enacting legislation that places responsibility for freezing the funds
or other assets of designated persons publicly identified by a com-
petent authority or a court on the person or entity holding the
funds or other assets and subjecting them to sanctions for non-com-
pliance.

The authority to freeze and unfreeze funds or other assets should
also extend to funds or other assets derived or generated from funds or
other assets owned or controlled directly or indirectly by such terror-
ists, those who finance terrorism, or terrorist organisations.

Whatever option is chosen there should be clearly identifiable com-
petent authorities responsible for enforcing the measures. The com-
petent authorities shall ensure that their nationals or any persons and
entities within their territories are prohibited from making any funds
or other assets, economic resources or financial or other related ser-
VICES available, directly or indirectly, wholly or jointly, for the benefit
of: designated persons, terrorists; those who finance terrorism; terrorist
organisations; entities owned or controlled, directly or indirectly, by
such persons or entities; and persons and entities acting on behalf of or
at the direction of such persons or entities.

b) **Freezing procedures.** Jurisdictions should develop and implement pro-
cedures to freeze the funds or other assets specified in paragraph (c)
below without delay and without giving prior notice to the persons
or entities concerned. Persons or entities holding such funds or other
assets should be required by law to freeze them and should further-
more be subject to sanctions for non-compliance with this require-
ment. Any delay between the official receipt of information provided
in support of a designation and the actual freezing of the funds or
other assets of designated persons undermines the effectiveness of
designation by affording designated persons time to remove funds or
other assets from identifiable accounts and places. Consequently, these
procedures must ensure (i) the prompt determination whether reason-
able grounds or a reasonable basis exists to initiate an action under a
freezing mechanism and (ii) the subsequent freezing of funds or other
assets without delay upon determination that such grounds or basis for freezing exist. Jurisdictions should develop efficient and effective systems for communicating actions taken under their freezing mechanisms to the financial sector immediately upon taking such action. As well, they should provide clear guidance, particularly financial institutions and other persons or entities that may be holding targeted funds or other assets on obligations in taking action under freezing mechanisms.

c) **Funds or other assets to be frozen or, if appropriate, seized.** Under Special Recommendation III, funds or other assets to be frozen include those subject to freezing under S/RES/1267(1999) and S/RES/1373(2001). Such funds or other assets would also include those wholly or jointly owned or controlled, directly or indirectly, by designated persons. In accordance with their obligations under the United Nations International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention (1999)), jurisdictions should be able to freeze or, if appropriate, seize any funds or other assets that they identify, detect, and verify, in accordance with applicable legal principles, as being used by, allocated for, or being made available to terrorists, those who finance terrorists or terrorist organisations. Freezing or seizing under the Terrorist Financing Convention (1999) may be conducted by freezing or seizing in the context of a criminal investigation or proceeding. Freezing action taken under Special Recommendation III shall be without prejudice to the rights of third parties acting in good faith.

d) **De-listing and unfreezing procedures.** Jurisdictions should develop and implement publicly known procedures to consider de-listing requests upon satisfaction of certain criteria consistent with international obligations and applicable legal principles, and to unfreeze the funds or other assets of de-listed persons or entities in a timely manner. For persons and entities designated under S/RES/1267(1999), such procedures and criteria should be in accordance with procedures adopted by the Al-Qaida and Taliban Sanctions Committee under S/RES/1267(1999).

e) **Unfreezing upon verification of identity.** For persons or entities with the same or similar name as designated persons, who are inadvertently affected by a freezing mechanism, jurisdictions should develop and
implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner upon verification that the person or entity involved is not a designated person.

f) **Providing access to frozen funds or other assets in certain circumstances.** Where jurisdictions have determined that funds or other assets, which are otherwise subject to freezing pursuant to the obligations under S/RES/1267(1999), are necessary for basic expenses; for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, jurisdictions should authorise access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and subject to approval of the Al-Qaida and Taliban Sanctions Committee. On the same grounds, jurisdictions may authorise access to funds or other assets, if freezing measures are applied pursuant to S/RES/1373(2001).

g) **Remedies.** Jurisdictions should provide for a mechanism through which a person or an entity that is the target of a freezing mechanism in the context of terrorist financing can challenge that measure with a view to having it reviewed by a competent authority or a court.

h) **Sanctions.** Jurisdictions should adopt appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing freezing mechanisms by financial institutions and other persons or entities that may be holding funds or other assets as indicated in paragraph 8(c) above. Failure to comply with such legislation, rules or regulations should be subject to civil, administrative or criminal sanctions.

**Seizure and Confiscation**


---

8. See Article 1, S/RES/1452(2002) for the specific types of expenses that are covered.
(1999), including legislative measures, to enable their courts or competent authorities to seize and confiscate terrorist funds or other assets.

Interpretative Note to Special Recommendation VI: Alternative Remittance

GENERAL

1. Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.

2. Special Recommendation VI consists of three core elements:

a) Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems;

b) Jurisdictions should ensure that money/value transmission services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (2003) (in particular, Recommendations 4–16 and 21–25)\(^9\) and the Eight Special Recommendations (in particular SR VII); and

c) Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without

---

9. When this Interpretative Note was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.
a license or registration and that fail to comply with relevant FATF Recommendations.

**Scope and Application**

3. For the purposes of this Recommendation, the following definitions are used.

4. *Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.

5. A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (or parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala, hundi, fei-chien*, and the *black market peso exchange.*

6. *Licensing* means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally.

---

10. The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.
7. Registration in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.

8. The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents which must be made available to the designated competent authority. An agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

**Applicability of Special Recommendation VI**

9. Special Recommendation VI should apply to all persons (natural or legal), which conduct for or on behalf of another person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.

10. Jurisdictions need not impose a separate licensing / registration system or designate another competent authority in respect to persons (natural or legal) already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations [2003]) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF Forty Recommendations (2003) (in particular, Recommendations 4–16 and 21–25) and the Eight Special Recommendations (in particular SR VII).

**Licensing or Registration and Compliance**

11. Jurisdictions should designate an authority to grant licences and/or carry out registration and ensure that the requirement is observed. There
should be an authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations (including the Eight Special Recommendations). There should also be effective systems in place for monitoring and ensuring such compliance. This interpretation of Special Recommendation VI (i.e., the need for designation of competent authorities) is consistent with FATF Recommendation 23.

SANCTIONS

12. Persons providing money/value transfer services without a license or registration should be subject to appropriate administrative, civil or criminal sanctions. Licensed or registered money/value transfer services which fail to comply fully with the relevant measures called for in the FATF Forty Recommendations (2003) or the Eight Special Recommendations should also be subject to appropriate sanctions.

Interpretative Note to Special Recommendation VII: Wire Transfers

OBJECTIVE

1. Special Recommendation VII (SR VII) was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (2) to financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary, and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious

11. The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.

12. It is recognised that jurisdictions will need time to make relevant legislative or regulatory changes and to allow financial institutions to make necessary adaptations to their systems and procedures. This period should not be longer than two years after the adoption of this Interpretative Note.
transactions. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

DEFINITIONS

2. For the purposes of this interpretative note, the following definitions apply.

a) The terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

b) *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.

c) *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction.

d) The term *financial institution* is as defined by the FATF Forty Recommendations (2003). The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.

---

13. When this Interpretative Note was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.

14. However, these systems do have a role in providing the necessary means for the financial institutions to fulfil their obligations under SR VII and, in particular, in preserving the integrity of the information transmitted with a wire transfer.
e) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

**SCOPE**

3. SR VII applies, under the conditions set out below, to cross-border and domestic transfers between financial institutions.

**CROSS-BORDER WIRE TRANSFERS**

4. Cross-border wire transfers should be accompanied by accurate and meaningful originator information.15

5. Information accompanying cross-border wire transfers must always contain the name of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included.

6. Information accompanying the wire transfer should also contain the address of the originator. However, jurisdictions may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.

7. Cross-border wire transfers that are contained within batch transfers, except for those sent by money remitters, will be treated as domestic wire transfers. In such cases, the ordering institutions must retain the information necessary to identify all originators and make it available on request to the authorities and to the beneficiary financial institution. Financial institutions

---

15. Jurisdictions may have a de minimis threshold (no higher than USD 3,000) for a one-year period from publication of this Interpretative Note. At the end of this period, the FATF will undertake a review of this issue to determine whether the use of a de minimis threshold is acceptable. Notwithstanding any thresholds, accurate and meaningful originator information must be retained and made available by the ordering financing institution as set forth in paragraph 9.
should ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

**DOMESTIC WIRE TRANSFERS**

8. Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, financial institutions need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator.

9. The information must be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate authorities. Law enforcement authorities should be able to compel immediate production of such information.

**EXEMPTIONS FROM SR VII**

10. SR VII is not intended to cover the following types of payments:

   a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, and the necessary information should be included in the message.

   b) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.
ROLE OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

ORDERING FINANCIAL INSTITUTION

11. The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the standards set out in the FATF Forty Recommendations (2003).16

INTERMEDIARY FINANCIAL INSTITUTION

12. For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

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

BENEFICIARY FINANCIAL INSTITUTION

14. Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminat-

16. See footnote 2.
ing its business relationship with financial institutions that fail to meet SRVII standards.

ENFORCEMENT MECHANISMS FOR FINANCIAL INSTITUTIONS THAT DO NOT COMPLY WITH WIRE TRANSFER RULES AND REGULATIONS

15. Jurisdictions should adopt appropriate measures to monitor effectively the compliance of financial institutions with rules and regulations governing wire transfers. Financial institutions that fail to comply with such rules and regulations should be subject to civil, administrative or criminal sanctions.

Guidance Notes

1. The Eight Special Recommendations on terrorist financing were adopted by the FATF in October 2001. Immediately following their adoption, the FATF undertook to assess the level of implementation of the Special Recommendations through a self-assessment exercise. A self-assessment questionnaire on terrorist financing (SAQTF) was developed with a series of questions for each Special Recommendation. The questions were designed to elicit details that would help determine whether a particular jurisdiction has in fact implemented a particular Special Recommendation.

2. Since the adoption of the Special Recommendations, the FATF has had little time to develop interpretations based on the experience of implementing these measures. Upon completion of the initial phase of this exercise by FATF members, it was therefore decided that additional guidance would be drafted and published to assist non-FATF members in understanding some of the concepts contained in the Special Recommendations on terrorist financing and to clarify certain parts of the SAQTF. This document therefore contains additional clarification of the Eight Special Recommendations and the SAQTF.

3. It should be emphasised at the start that the information presented here is meant primarily to serve as a guide to jurisdictions attempting to fill in and
submit the SAQTF. For this reason, they should not be considered exhaustive or definitive. Any questions on particular interpretations or implications of the Special Recommendations should be directed to the FATF Secretariat at contact@fatf-gafi.org.

SR I: Ratification and implementation of UN instruments

4. This Recommendation contains six elements:

- Jurisdictions should ratify and fully implement the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism, and

5. For the purposes of this Special Recommendation, **ratification** means having carried out any necessary national legislative or executive procedures to approve the UN Convention and having delivered appropriate ratification instruments to the United Nations. **Implementation** as used here means having put measures in place to bring the requirements indicated in the UN Convention and UNSC Resolutions into effect. The measures may be established by law, regulation, directive, decree, or any other appropriate legislative or executive act according to national law.

6. The UN Convention was open for signature from 10 January 2000 to 31 December 2001, and upon signature is subject to ratification, acceptance or approval. Ratification, acceptance or approval instruments must be deposited with the Secretary-General of the United Nations in New York. Those countries that have not signed the Convention may accede to it (see Article 25 of the Convention). The full text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism/conv12.pdf. As of 19 March 2002, 132 countries have signed, and 24 have deposited ratification instruments. On 10 March 2002, the UN Convention reached the minimum number of ratifications (22) stipulated as necessary for it to come into effect. The effec-
SR II: Criminalising the financing of terrorism and associated money laundering

7. This Recommendation contains two elements:

- Jurisdictions should criminalise “the financing of terrorism, of terrorist acts and of terrorist organisations”; and
- Jurisdictions should establish terrorist financing offences as predicate offences for money laundering.

8. In implementing SR II, jurisdictions must either establish specific criminal offences for terrorist financing activities, or they must be able to cite existing criminal offences that may be directly applied to such cases. The terms financing of terrorism or financing of terrorist acts refer to the activities described in the UN Convention (Article 2) and S/RES/1373(2001), paragraph 1b (see the UN website at http://www.un.org/documents/scres.htm for text of this Resolution). It should be noted that each jurisdiction should also ensure that terrorist financing offences apply as predicate offences even when carried out in another State. This corollary interpretation of SR II is then consistent with FATF Recommendation 4.

9. FATF Recommendation 4 already calls for jurisdictions to designate “serious offences” as predicates for the offence of money laundering. SR II builds on Recommendation 4 by requiring that, given the gravity of terrorist financing offences, terrorism financing offences should be specifically included among the predicates for money laundering. For the full text of the FATF
Forty Recommendations, along with their Interpretative Notes, see the FATF website at http://www.fatf-gafi.org/40Recs_en.htm.

10. Finally, as in general with other predicates for money laundering, jurisdictions should ensure that terrorist financing offences are predicate offences even if they are committed in a jurisdiction different from the one in which the money laundering offence is being applied.

SR III: Freezing and confiscating terrorist assets

11. This Recommendation contains three major elements:

- Jurisdictions should have the authority to freeze funds or assets of (a) terrorists and terrorist organisations and (b) those who finance terrorist acts or terrorist organisations;
- They should have the authority to seize (a) the proceeds of terrorism or of terrorist acts, (b) the property used in terrorism, in terrorist acts or by terrorist organisations and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organisations; and
- They should have the authority to confiscate (a) the proceeds of terrorism or of terrorist acts, (b) the property used in terrorism, in terrorist acts or by terrorist organisations and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organisations.

12. The term measures, as used in SR III, refers to explicit (legislative or regulatory) provisions or “executive powers” that permit the three types of action. As with the preceding Recommendation, it is not necessary that the texts authorising these powers mention terrorist financing in particular. However, jurisdictions with already existing laws must be able to cite specific provisions that permit them to freeze, to seize or to confiscate terrorist related funds and assets within the national legal/judicial context.

13. The definitions of the concepts of freezing, seizure and confiscation vary from one jurisdiction to another. For the purposes of general guidance, the following descriptions of these terms are provided:
14. **Freezing**: In the context of this Recommendation, a competent government or judicial authority must be able to freeze, to block or to restrain specific funds or assets and thus prevent them from being moved or disposed of. The assets/funds remain the property of the original owner and may continue to be administered by the financial institution or other management arrangement designated by the owner.

15. **Seizure**: As with freezing, competent government or judicial authorities must be able to take action or to issue an order that allows them to take control of specified funds or assets. The assets/funds remain the property of the original owner, although the competent authority will often take over possession, administration or management of the assets/funds.

16. **Confiscation (or forfeiture)**: Confiscation or forfeiture takes place when competent government or judicial authorities order that the ownership of specified funds or assets be transferred to the State. In this case, the original owner loses all rights to the property. Confiscation or forfeiture orders are usually linked to a criminal conviction and a court decision whereby the property is determined to have been derived from or intended for use in a violation of the law.

17. With regard to freezing in the context of SR III, the terms **terrorists**, **those who finance terrorism** and **terrorist organisations** refer to individuals and entities identified pursuant to S/RES/1267 (1999) and S/RES/1390 (2002), as well as to any other individuals and entities designated as such by individual national governments.

**SR IV: Reporting suspicious transactions related to terrorism**

18. This Recommendation contains two major elements:

- Jurisdictions should establish a requirement for making a report to competent authorities when there is a **suspicion** that funds are linked to terrorist financing; or
• Jurisdictions should establish a requirement for making a report to competent authorities when there are *reasonable grounds* to suspect that funds are linked to terrorist financing.

19. For SR IV, the term *financial institutions* refers to both banks and non-bank financial institutions (NBFIs). In the context of assessing implementation of FATF Recommendations, NBFIs include, as a minimum, the following types of financial services: bureaux de change, stockbrokers, insurance companies and money remittance/transfer services. This definition of *financial institutions* is also understood to apply to SR IV in order to be consistent with the interpretation of the FATF Forty Recommendations. With regard specifically to SR IV, if other types of professions, businesses or business activities currently fall under anti-money laundering reporting obligations, jurisdictions should also extend terrorist financing reporting requirements to those entities or activities.

20. The term *competent authority*, for the purposes of SR IV, is understood to be either the jurisdiction’s financial intelligence unit (FIU) or another central authority that has been designated by the jurisdiction for receiving disclosures related to money laundering.

21. With regard to the terms *suspect* and *have reasonable grounds to suspect*, the distinction is being made between levels of mental certainty that could form the basis for reporting a transaction. The first term—that is, a requirement to report to competent authorities when a financial institution suspects that funds are derived from or intended for use in terrorist activity—is a subjective standard and transposes the reporting obligation called for in FATF Recommendation 15 to SR IV. The requirement to report transactions when there are reasonable grounds to suspect that the funds are derived from or intended for use in terrorist activity is an objective standard, which is consistent with the intent of Recommendation 15 although somewhat broader. In the context of SR IV, jurisdictions should establish a reporting obligation that may be based either on suspicion or on having reasonable grounds to suspect.
SR V: International Co-operation

22. This Recommendation contains five elements:

- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions through mutual legal assistance mechanisms;
- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions by means other than through mutual legal assistance mechanisms;
- Jurisdictions should have specific measures to permit the denial of “safe haven” to individuals involved in terrorist financing;
- Jurisdictions should have procedures that permit the extradition of individuals involved in terrorist financing; and
- Jurisdictions should have provisions or procedures to ensure that “claims of political motivation are not recognised as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing.”

23. To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made for some questions in the SAQTF between international co-operation through mutual legal assistance mechanisms on the one hand and information exchange through means other than through mutual legal assistance.

24. For the purposes of SR V, the term mutual legal assistance means the power to provide a full range of both non-coercive legal assistance, including the taking of evidence, the production of documents for investigation or as evidence, the search and seizure of documents or things relevant to criminal proceedings or to a criminal investigation, the ability to enforce a foreign restraint, seizure, forfeiture or confiscation order in a criminal matter. In this instance, mutual legal assistance would also include information exchange through rogatory commissions (that is, from the judicial authorities in one jurisdiction to those in another).
25. Exchange of information by means *other than through mutual legal assistance* includes any arrangement other than those described in the preceding paragraph. Under this category should be included exchanges that take place between FIUs or other agencies that communicate bilaterally on the basis of memoranda of understanding (MOUs), exchanges of letters, etc.

26. With regard to the last three elements of SR V, these concepts should be understood as referred to in the relevant UN documents. These are S/RES/1373 (2001), paragraph 2c (for denial of safe haven); the UN Convention, Article 11 (for extradition); and the UN Convention, Article 14 (for rejection of claims of political motivation as related to extradition). The text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism.asp; the text of S/RES/1373 (2001) may be accessed at http://www.un.org/documents.scres.htm.

27. The term *civil enforcement* as used in SR V is intended to refer only to the type of investigations, inquiries or procedures conducted by regulatory or administrative authorities that have been empowered in certain jurisdictions to carry out such activities in relation to terrorist financing. *Civil enforcement is not meant to include civil procedures and related actions as understood in civil law jurisdictions.*

SR VI: Alternative Remittance

28. This Recommendation consists of three major elements:

- Jurisdictions should require licensing or registration of persons or legal entities providing money/value transmission services, including through informal systems or networks;
- Jurisdictions should ensure that money/value transmission services, including informal systems or networks, are subject to FATF Recommendations 10–12 and 15; and
- Jurisdictions should be able to impose sanctions on money/value transmission services, including informal systems or networks, that fail to
obtain a license/register and that fail to comply with relevant FATF Recommendations.

29. Money or value transfer systems have shown themselves vulnerable to misuse for money laundering or terrorist financing purposes. The intention of SR VI is to ensure that jurisdictions impose anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems. To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made between formal and informal transfer systems in some questions.

30. The term money remittance or transfer service refers to a financial service—often provided by a distinct category of non-bank financial institutions—whereby funds are moved for individuals or entities through a dedicated network or through the regulated banking system. For the purposes of assessing compliance with the FATF Recommendations, money remitter/transfer services are included as a distinct category of NBFI and are thus considered part of the regulated financial sector. Nevertheless, such services are used in some laundering or terrorist financing operations, often as part of a larger alternate remittance or underground banking scheme.

31. The term informal money or value transfer system also refers to a financial service whereby funds or value are moved from one geographic location to another. However, in some jurisdictions, these informal systems have traditionally operated outside the regulated financial sector in contrast to the “formal” money remittance/transfer services described in the preceding paragraph. Some examples of informal systems include the parallel banking system found in the Americas (often referred to as the “Black Market Peso Exchange”), the hawala or hundi system of South Asia, and the Chinese or East Asian systems. For more information on this topic, see the FATF-XI Typologies Report (3 February 2000), available through the FATF website at http://www.fatfgafi.org/FATDocs_en.htm#Trends, or the Asia Pacific Group Report on Underground Banking and Alternate Remittance Systems (18 October 2001), available through the APG website at http://www.apgml.org/.
32. Where licensing or registration are indicated in the questionnaire, either licensing or registration is considered sufficient to meet the requirements of the Recommendation. Licensing in this Recommendation means a requirement to obtain permission from a designated government authority in order to operate a money/value transmission service. Registration in this Recommendation means a requirement to register or declare the existence of a money/value transmission service in order for the business to operate. It should be noted that the logical consequence of the requirements of SR VI is that jurisdictions should designate a licensing or registration authority and an authority to ensure compliance with FATF Recommendations for money/value transmission services, including informal systems or networks. This corollary interpretation of SR VI (i.e., the need for designation of competent authorities) is consistent with FATF Recommendation 26. 33. The reference to “all FATF Recommendations that apply to banks and non-bank financial institutions” includes as a minimum Recommendations 10, 11, 12, and 15. Other applicable Recommendations include Recommendations 13, 14, 16–21 and 26–29. The full text of these and all other FATF Recommendations may be consulted on the FATF website http://www.fatf-gafi.org/40Recs_en.htm.

SR VII: Wire transfers

34. This Recommendation consists of three elements:

- Jurisdictions should require financial institutions to include originator information on funds transfers sent within or from the jurisdiction;
- Jurisdictions should require financial institutions to retain information on the originator of funds transfers, including at each stage of the transfer process; and
- Jurisdictions should require financial institutions to examine more closely or to monitor funds transfers when complete originator information is not available.

35. For the purpose of SR VII, three categories of financial institution are specifically concerned (banks, bureaux de change, and money remittance/transfer
services), although other financial services (for example, stockbrokers, insurance companies, etc.) may be subject to such requirements in certain jurisdictions.

36. The list of types of accurate and meaningful originator information indicated in the Special Recommendation (that is, name, address and account number) is not intended to be exhaustive. In some instances—in the case of an occasional customer, for example—there may not be an account number. In certain jurisdictions, a national identity number or a date and place of birth could also be designated as required originator information.

37. The term enhanced scrutiny for the purposes of SR VII means examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (origin in a country known to provide safe haven to terrorists or terrorist organisations, for example) and thus warrant eventual reporting to the competent authority.

SR VIII: Non-profit organisations

38. The intent of SR VIII is to ensure that legal entities (juridical persons), other relevant legal arrangements, and in particular non-profit organisations may not be used by terrorists as a cover for or a means of facilitating the financing of their activities. This Recommendation consists of two elements:

- Jurisdictions should review the legal regime of entities, in particular non-profit organisations, to prevent their misuse for terrorist financing purposes; and
- With respect specifically to non-profit organisations, jurisdictions should ensure that such entities may not be used to disguise or facilitate terrorist financing activities, to escape asset freezing measures or to conceal diversions of legitimate funds to terrorist organisations.

39. As stated above, the intent of SR VIII is to ensure that legal entities, other relevant legal arrangements, and non-profit organisations may not be misused by terrorists. Legal entities have a variety of forms that differ from one jurisdiction to another. The degree to which a particular type of entity may be vulnerable to misuse in terrorist financing may also vary from one
jurisdiction to another. For this reason, a selection of types of legal entities and other legal arrangements has been presented in the SAQTF in an attempt to obtain a clear picture of the situation in individual jurisdictions. The selection is based on types of entities that have been observed as being involved in money laundering and/or terrorist financing activities in the past. Individual categories may overlap, and in some instances, a jurisdiction may not have all the categories indicated in the SAQTF.

40. Similarly it should be pointed out that non-profit organisations, a particular focus of SR VIII, may exist in legal forms that vary from one jurisdiction to another. Again, the selection of entity types in the SAQTF has been made with the intention of permitting jurisdictions to find entities or arrangements that correspond to their individual situation. The term non-profit organisation can be generally understood to include those types of entities that are organised for charitable, religious, educational, social or fraternal purposes, or for the carrying out of other types of “good works”. In addition, the earnings of such entities or activities should normally not benefit any private shareholder or individual, and they may be restricted from direct or substantial involvement in political activities. In many jurisdictions, non-profit organizations are exempt from fiscal obligations.

41. In the SAQTF, the term offshore companies refers to what are usually established as limited liability juridical persons in certain jurisdictions and which often fall under a separate or privileged regulatory regime. Such entities may be used to own and operate businesses (a shell or holding company), issue shares or bonds, or raise capital in other manners. They are generally exempt from local taxes or subject to a preferential rate and may be prohibited from doing business in the jurisdiction in which they are incorporated. The International Business Corporation (IBC) is an example of such an entity. In the SAQTF, jurisdictions should only respond to relevant offshore questions if they have an offshore sector within their jurisdiction.

42. The SAQTF also includes a category “Trusts and/or foundations” under SR VIII. Trusts are legal arrangements available in certain jurisdictions. Although they are not strictly speaking legal entities, they are used as a means for holding or transmitting assets and may, as with certain legal entities, be
misused as a means for hiding or disguising true ownership of an asset. The term foundations refers primarily to “private foundations or establishments” that exist in some civil law jurisdictions and which may engage in commercial and/or non-profit activities. Some examples of these include Stiftung, stichting, Anstalt, etc.

**Interpretative Note to Special Recommendation IX: Cash Couriers**

**Objectives**

1. FATF Special Recommendation IX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures 1) to detect the physical cross-border transportation of currency and bearer negotiable instruments, 2) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, 3) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, 4) to apply appropriate sanctions for making a false declaration or disclosure, and 5) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. Countries should implement Special Recommendation IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.

**Definitions**

2. For the purposes of Special Recommendation IX and this Interpretative Note, the following definitions apply.

3. The term *bearer negotiable instrument* includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including
cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted.\footnote{For the purposes of this Interpretative Note, gold, precious metals and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should co-operate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.}

4. The term \textit{currency} refers to banknotes and coins that are in circulation as a medium of exchange.

5. The term \textit{physical cross-border transportation} refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person’s accompanying luggage or vehicle; (2) shipment of currency through containerized cargo or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

6. The term \textit{false declaration} refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

7. The term \textit{false disclosure} refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked.

8. When the term \textit{related to terrorist financing or money laundering} is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or
intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

The types of systems that may be implemented to address the issue of cash couriers

9. Countries may meet their obligations under Special Recommendation IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

a. **Declaration system**: The key characteristics of a declaration system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a pre-set, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the pre-set threshold is sufficiently low to meet the objectives of Special Recommendation IX.

b. **Disclosure system**: The key characteristics of a disclosure system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.
10. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

a. The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.
b. Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.
c. Information obtained through the declaration/disclosure process should be available to the financial intelligence unit (FIU) either through a system whereby the FIU is notified about suspicious cross-border transportation incidents or by making the declaration/disclosure information directly available to the FIU in some other way.
d. At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Special Recommendation IX.
e. In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.
f. The declaration/disclosure system should allow for the greatest possible measure of international co-operation and assistance in accordance with Special Recommendation V and Recommendations 35 to 40. To facilitate such co-operation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of EUR/USD 15,000 is made, or (ii) where there is a false declaration or false disclosure, or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by the appropriate authorities. At a minimum, this information will cover: (i) the amount
of currency or bearer negotiable instruments declared / disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

Sanctions

11. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or bearer negotiable instruments.
Annex VII

Cross-Reference of The Forty Recommendations to Reference Guide

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Reference Guide</th>
</tr>
</thead>
</table>
| 1              | Chapter I, footnote 8  
Chapter V, footnotes 4, 20–22, 25–27  
Chapter VIII, footnote 7 |
| 2              | Chapter V, footnotes 38, 39 |
| 3              | Chapter V, footnotes 51, 53, 55, 58–60 |
| 4              | Chapter V, footnotes 57, 80  
Chapter VI, footnotes 75  
Chapter VII, footnotes 14–20, 33  
Chapter IX, footnote 58 |

Annex VII-1
5  Chapter V, footnotes 67–68  
Chapter VI, footnotes 5, 17–19, 21–22, 41  
Chapter IX, footnote 58

6  Chapter V, footnote 67–68  
Chapter VI, footnote 41  
Chapter IX, footnote 58

7  Chapter V, footnotes 67–68  
Chapter VI, footnote 32  
Chapter IX, footnote 58

8  Chapter V, footnotes 67–68  
Chapter VI, footnotes 35, 41  
Chapter IX, footnote 58

9  Chapter V, footnotes 67–68  
Chapter VI, footnotes 36, 41  
Chapter IX, footnote 58

10  Chapter V, footnote 67–68  
Chapter VI, footnotes 41, 46–48, 59  
Chapter VII, footnote 5  
Chapter IX, footnote 58

11  Chapter V, footnotes 67–68  
Chapter VI, footnotes 37, 41, 60  
Chapter VII, footnote 4  
Chapter IX, footnote 58

12  Chapter V, footnotes 67–68  
Chapter VI, footnotes 42–45, 55  
Chapter VII, footnote 4  
Chapter IX, footnote 58

Annex VII-2
| 13 | Chapter V, footnotes 67–68, 79  
Chapter VI, footnote 56  
Chapter VII, footnotes 4, 12  
Chapter IX, footnotes 39, 58 |
|---|---|
| 14 | Chapter V, footnotes 67–68  
Chapter VI, footnotes 58, 62  
Chapter VII, footnote 4  
Chapter IX, footnote 58 |
| 15 | Chapter V, footnotes 67–68  
Chapter VI, footnotes 76, 77, 79  
Chapter VII, footnote 4  
Chapter IX, footnote 58 |
| 16 | Chapter V, footnotes 67–68  
Chapter VI, footnotes 65, 66, 68, 69  
Chapter VII, footnote 4  
Chapter IX, footnote 58 |
| 17 | Chapter V, footnotes 67–68  
Chapter VII, footnote 4  
Chapter IX, footnote 58 |
| 18 | Chapter V, footnotes 67–68  
Chapter VI, footnote 34  
Chapter VII, footnotes 4, 12  
Chapter IX, footnote 58 |
| 19 | Chapter V, footnotes 67–68  
Chapter VI, footnotes 70, 73  
Chapter VII, footnotes 4, 12  
Chapter IX, footnote 58 |
<table>
<thead>
<tr>
<th></th>
<th>Chapter V, footnotes 67–68, 74</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Chapter VI, footnote 74</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 4</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 58</td>
</tr>
<tr>
<td>21</td>
<td>Chapter V, footnotes 67–68</td>
</tr>
<tr>
<td></td>
<td>Chapter VI, footnote 38</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 4</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 58</td>
</tr>
<tr>
<td>22</td>
<td>Chapter V, footnotes 67–68</td>
</tr>
<tr>
<td></td>
<td>Chapter VI, footnotes 9, 10</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 4</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 58</td>
</tr>
<tr>
<td>23</td>
<td>Chapter V, footnotes 67–68, 76–78</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnotes 58, 59, 60</td>
</tr>
<tr>
<td>24</td>
<td>Chapter V, footnotes 67–68</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 58</td>
</tr>
<tr>
<td>25</td>
<td>Chapter V, footnotes 67–68</td>
</tr>
<tr>
<td></td>
<td>Chapter VI, footnote 61</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 38</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 58</td>
</tr>
<tr>
<td>26</td>
<td>Chapter VII, footnotes 3, 9</td>
</tr>
<tr>
<td>27</td>
<td>Chapter V, footnote 82</td>
</tr>
<tr>
<td></td>
<td>Chapter VIII, footnotes 27, 29</td>
</tr>
<tr>
<td>28</td>
<td>Chapter VI, footnotes 59, 74, 75</td>
</tr>
<tr>
<td>29</td>
<td>Chapter V, footnotes 76, 77</td>
</tr>
<tr>
<td>30</td>
<td>Chapter V, footnote 84</td>
</tr>
<tr>
<td></td>
<td>Chapter</td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
</tr>
<tr>
<td>31</td>
<td>V, footnote 81</td>
</tr>
<tr>
<td>32</td>
<td>V, footnote 85</td>
</tr>
<tr>
<td>33</td>
<td>VI, footnotes 80, 81</td>
</tr>
<tr>
<td>34</td>
<td>VI, footnotes 82, 83</td>
</tr>
<tr>
<td>35</td>
<td>VIII, footnote 3, 8</td>
</tr>
<tr>
<td>36</td>
<td>VII, footnote 8</td>
</tr>
<tr>
<td>37</td>
<td>V, footnote 28</td>
</tr>
<tr>
<td>38</td>
<td>VIII, footnotes 26, 30</td>
</tr>
<tr>
<td>39</td>
<td>VIII, footnote 31</td>
</tr>
<tr>
<td>40</td>
<td>VII, footnote 8</td>
</tr>
</tbody>
</table>
Annex VIII

Cross-Reference of the Special Recommendations to Reference Guide

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Reference Guide</th>
</tr>
</thead>
</table>
| I              | Chapter I, footnote 12  
Chapter VIII, footnote 7  
Chapter IX, footnotes 8, 10, 21 |
| II             | Chapter I, footnotes 13, 14, 15  
Chapter V, footnotes 24, 48, 49  
Chapter IX, footnotes 23–26, 35 |
| III            | Chapter IX, footnotes 6, 27, 28, 29, 30, 31, 32, 33 |
| IV             | Chapter IX, footnote 36 |
| V              | Chapter IX, footnotes 41, 42 |

Annex VIII-1
VI  Chapter I, footnote 17  
Chapter V, footnote 69  
Chapter IX, footnotes 6, 51, 52, 53

VII  Chapter V, footnote 69  
Chapter IX, footnotes 61, 62–67

VIII  Chapter I, footnote 16  
Chapter IX, footnotes 6, 68, 69, 70

IX  Chapter IX, footnotes 72–92
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Design and layout by James Quigley
Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism
Second Edition and Supplement on Special Recommendation IX

www.amlcft.org

THE WORLD BANK

International Monetary Fund

ISBN 0-8213-6513-4
지금세탁방지 및
테러자금조달 금지 제도 해설

인쇄 2010년 12월 일
발행 2010년 12월 일

발행인 금융정보분석원장 최수현
발행처 금융위원회 금융정보분석원
서울특별시 영등포구 여의대로 97
전화 : 02.2156.9941
www.kofiu.go.kr

인쇄 서울기업
02-3673-0412

자금세탁방지/테러자금조달 금지 안내서에 대한 저작권 © [2006]는
국제부흥개발은행/세계은행에 있습니다.

Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism
Copyright © 2006 by

The International Bank for Reconstruction and Development/The World Bank
자금세탁방지 및 테러자금조달방지 제도 해설

특별권고 IX 관련 내용 수록 개정판

www.amlcft.org