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

Paul Allan Schott

THE WORLD BANK
Reference Guide to
Anti-Money Laundering and
Combating the Financing of Terrorism
Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism
Contents

Preface ................................................................. ix
Foreword ............................................................. xi
Acknowledgments ............................................... xiii
Abbreviations and Acronyms .............................. xv

Introduction: How to Use this Reference Guide ....... xvii

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-12
D. International Association of Insurance Supervisors .............. III-15
E. International Organization of Securities Commissioners ........ III-17
F. The Egmont Group .................................................... III-18

Chapter IV: Regional Bodies and Relevant Groups ......................... IV-1
A. FATF-Style Regional Bodies ........................................ IV-1
B. Wolfsberg Group of Banks .......................................... IV-4
C. The Commonwealth Secretariat ..................................... IV-6
D. Organization of American States—CICAD .......................... IV-7

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

Chapter V: Legal System Requirements ....................................... V-1
A. Ratification and Implementation of the Vienna Convention .... V-2
B. Criminalization of Money Laundering and Terrorist Financing . V-4
C. Seizure, Confiscation, and Forfeiture ............................... V-11
D. Scope of Covered Financial Institutions ............................ V-15
E. Integrity Standards ...................................................... V-17

Chapter VI: Financial Institution Requirements .......................... VI-1
A. Customer Identification and Due Diligence ........................ VI-2
B. Suspicious Transaction Reporting ................................... VI-10
C. Record Keeping Requirements ....................................... VI-13
D. Cash Transaction Reporting ......................................... VI-15
E. Privacy Laws Versus Reporting and Disclosure .................... VI-18
F. Internal Controls, Compliance and Audit ........................... VI-18

Chapter VII: The Financial Intelligence Unit .............................. VII-1
A. Definition of a Financial Intelligence Unit ........................ VII-3
B. Core Functions ....................................................... VII-4
C. Possible Additional Functions ...................................... VII-7
Chapter VIII: International Cooperation

A. Prerequisites for Effective International Cooperation
B. General Principles of International Cooperation Against Money Laundering
C. International Cooperation Between FIUs
D. International Cooperation Between Financial Supervisory Authorities
E. International Cooperation Between Law Enforcement and Judicial Authorities

Chapter IX: Combating the Financing of Terrorism

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
F. Alternative Remittance Systems
G. Wire Transfers
H. Non-Profit Organizations
I. Self Assessment Questionnaire on Terrorist Financing

Part C: The Role of the World Bank and International Monetary Fund

Chapter X: World Bank and International Monetary Fund Initiatives to Fight Money Laundering and Terrorist Financing

A. Awareness Raising
B. Development of a Universal AML/CFT Assessment Methodology
C. Building Institutional Capacity
D. Research and Analysis
Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

Annexes

I. Websites for Key Organizations, Legal Instruments and Initiatives .............................................. Annex I-1
II. Other Useful Websites and Resources ................................................. Annex II-1
III. List of United Nations Anti-Terrorist Conventions .............................................. Annex III-1
IV. The Forty Recommendations on Money Laundering and Interpretative Notes .............................................. Annex IV-1
V. Eight Special Recommendations on Terrorist Financing .............................................. Annex V-1
VI. Guidance Notes for the Special Recommendations on Terrorist Financing and the Self-Assessment Questionnaire .............................................. Annex VI-1
VIII. Cross Reference of Special Recommendations to Reference Guide .............................................. Annex VIII-1

Diagrams

The Processes of Money Laundering and Financing of Terrorism .............. I-7
Preface

Money laundering and terrorist financing are global problems. For developed and developing countries alike, these activities compromise the stability, transparency and efficiency of financial systems. Thus, these activities merit the complete attention of all countries. Moreover, the events of September 11, 2001, have heightened the international concern.

Criminals and those who finance terrorism are aided by lax or corrupt institutional frameworks for fighting money laundering and terrorist financing. Such regimes permit criminals and terrorists to operate freely, using their financial gains to expand their criminal pursuits and to foster illegal activities such as corruption, drug trafficking, arms trafficking, smuggling, and financing terrorist activities. The economy, society and ultimately the security of countries used as money laundering platforms are all imperiled.

The global agenda to curb money laundering and the financing of terrorism requires a cooperative approach among many different international bodies. The International Monetary Fund and the World Bank are integral parts of this international effort. Working with the Financial Action Task Force and other international standard-setters, we have intensified our work in these areas. This Reference Guide to Money Laundering and the Financing of Terrorism is a significant contribution toward solving these global problems because it provides a comprehensive source of practical information about the issues, the specific actions countries need to take to address these issues according to internationally accepted standards, and the role the Fund and the Bank play to help in the process.

Cesare Colari
Vice President
Financial Sector
World Bank

Stefan Ingves
Director
Monetary and Exchange Affairs Department
International Monetary Fund
The World Bank and International Monetary Fund developed this unique Reference Guide to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in an effort to provide practical steps for countries implementing an AML/CFT regime in accordance with international standards. The Guide describes the global problem of money laundering and terrorist financing on the development agenda of individual countries and across regions. It explains the basic elements required to build an effective AML/CFT legal and institutional framework and summarizes the role of the World Bank and the International Monetary Fund in fighting money laundering and terrorist financing.

The primary objective of this joint Bank-Fund project is to ensure that the information contained in the Reference Guide is useful and easily accessible by developing countries that are working to establish and strengthen their policies against money laundering and the financing of terrorism. Additionally, this Guide is intended to contribute to global understanding of the devastating consequences of money laundering and terrorist financing on development growth, and political stability and to expand the international dialogue on crafting practical solutions to implement effective AML/CFT regimes.

Because we recognize that those who seek to launder money or finance terrorism are continuously evolving new ways to accomplish their illicit purposes, we expect to continuously update the Reference Guide with the latest information on practices that have proved to be most effective in fighting these financial crimes. We welcome your feedback and recommendations on how this Guide can better equip countries with the necessary tools to counter money laundering and terrorist financing.

Margery Waxman
Director
Financial Market Integrity
World Bank

Barry Johnston
Assistant Director
Monetary and Exchange Affairs 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 this Reference Guide.

The author is grateful to his Bank and Fund colleagues for their willingness to read multiple drafts 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 the terrorist financing: John Abbott, Maud Julie Bokkerink, Pierre-Laurent Chatain, Alain Damais, Ross Delston, Edil Dushenaliyev, Gabriella Ferencz, Richard Gordon, 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, Cari Votava, and Richard Zechter.

Most importantly, the author could not have produced this comprehensive document without the hours/weeks/months of work by Bank staff members who helped organize the material carefully, checked all references and made this publication a reality: Oriana Bolvaran, Nicolas de la Riva, Martin Josefson, Maria Orellano, Ana Pazos, James Quigley, Michaela Schott, Dafna Tapiero, Emiko Todoroki, Tracy Tucker, Paolo Ugolini, and Brett Webster.
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
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
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAIS</td>
<td>International Association of Insurance Supervisors</td>
</tr>
<tr>
<td>IFTs</td>
<td>informal funds transfer systems</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>IOSCO</td>
<td>International Organization of Securities Commissions</td>
</tr>
<tr>
<td>KYC</td>
<td>“know-your-customer”</td>
</tr>
<tr>
<td>MONEYVAL</td>
<td>Council of Europe the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures</td>
</tr>
<tr>
<td>MOU</td>
<td>memorandum of understanding</td>
</tr>
<tr>
<td>NCCT</td>
<td>Non-Cooperative Countries and Territories</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
<tr>
<td>PC-R-EV</td>
<td>Now known as MONEYVAL</td>
</tr>
<tr>
<td>STR</td>
<td>suspicious transaction reports</td>
</tr>
<tr>
<td>TA</td>
<td>Technical Assistance</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNSCCTC</td>
<td>United Nations Security Council Counter Terrorism Committee</td>
</tr>
<tr>
<td>Wolfsberg Group</td>
<td>Wolfsberg Group of Banks</td>
</tr>
</tbody>
</table>
Introduction:
How to Use this Reference Guide

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

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 and the eight Special Recommendations on Terrorist Financing. Annex VI is FATF's 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. Placement
   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 many different types of financial institutions; many different financial transactions using multiple financial institutions and other entities, such as financial advisers, shell corporations and service providers as intermediaries; transfers to, through, and from different countries; and the use of many 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 it. 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 so as 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 are rewarded with disguised and apparently legitimate proceeds. Similarly, those who finance terrorism are rewarded by providing the financial support to carry out terrorist stratagems and attacks.

A. What Is Money Laundering?

Money laundering can be defined in a number of ways. Most countries subscribe to the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention):  

1. 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 allY person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

2. 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.

2. The Vienna Convention, Article 3(b).
The Vienna Convention adds that money laundering also involves:

- 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.¹

By its terms, the Vienna Convention limits predicate offenses (which is to say, the criminal activity whose illicit proceeds are laundered) to drug trafficking offenses. As a consequence, crimes unrelated to drug trafficking, such as tax evasion, fraud, kidnapping and theft, for example, are not defined as money laundering offenses under the Vienna Convention. Over the years, however, the international community has come to the view that predicate offenses for money laundering should go beyond drug trafficking. Thus, other international instruments have expanded the Vienna Convention’s definition of predicate offenses to include other serious crimes.⁴ For example, the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention) requires all participant countries to apply that convention’s money laundering offenses to “the widest range of predicate 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,⁵ 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.¹ However, in its 40 recommendations for fighting money laundering (The Forty Recommendations), FATF specifically incorporates the Vienna Convention’s technical and legal definition of money laundering⁶ and recommends expanding the predicate offenses of that definition to include all serious crimes.⁷

---

1. Id., Article 3(cl).
2. See discussion at Chapter V, A., Predicate Offenses.
4. See Chapter III, B., FATF.
7. Id., at Rec. 4.
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).**

   The difficult issue for some countries is defining terrorism. Not all countries that have adopted the convention agree on 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...
Money Laundering and Terrorist Financing: Definitions and Explanations

define the term financing of terrorism in its eight Special Recommendations on Terrorist Financing (Special Recommendations)\textsuperscript{12} 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.\textsuperscript{13} 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,\textsuperscript{14} and designate such offenses as money laundering predicate offenses.\textsuperscript{15} Finally, FATF has stated that the eight Special Recommendations combined with The Forty Recommendations on money laundering\textsuperscript{16} 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 used, directly or indirectly, to finance or support terrorism.\textsuperscript{17} CFT efforts also

\textsuperscript{13} \textit{id.}, at Spec. Rec. I.
\textsuperscript{14} \textit{id.}, at Spec. Rec. II.
\textsuperscript{15} \textit{id.}, at introductory paragraph.
\textsuperscript{16} Special Recommendations, Spec. Rec. VIII.
require examination of alternative money transmission or remittance systems, such as *hawalas*. This effort includes consideration of what measures should be taken to preclude the use of such entities by money launderers and terrorists.  

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 the predicate offenses for money laundering.

**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 problem on a global basis is 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 US $590 billion and US $1.5 trillion.  

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 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 one, 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 purchases 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, security or insurance contract are converted or moved to other institutions further separating them from their criminal source. Such funds could 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 transferred electronically 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, securities 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
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 them 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 purchase 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 are 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. 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. 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. See Chapter IV for a discussion of the FATF-style regional bodies.
Chapter II

Money Laundering Impacts Development

A. The Adverse Implications for Developing Countries
   1. Increased Crime and Corruption
   2. Weakened Financial Institutions
   3. Damaged Economy and Private Sector
   4. Damaged Financial Intermediaries
   5. Increased Financial Disruptiveness

B. The Benefits of an Effective AML/CFT Framework
   1. Fighting Crime and Corruption
   2. Enhancing Stability of Financial Institutions
   3. Encouraging Economic Development

Criminal enterprises and terrorist financing operations succeed largely to the extent that they are able to sanitize and conceal their 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 financing 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. The economy, society, and ultimately the security of countries used as money-laundering 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 or for a specific 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 impact 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. 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 the AML/CFT framework;
- little, weak or selective enforcement of AML/CFT;
- ineffective penalties, including difficult confiscation provisions; and
- a limited number of predicate crimes for money laundering.

Money Laundering Impacts Development

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

- employees and management of financial institutions,
- lawyers and accountants,
- the legislature,
- enforcement agencies,
- supervisory authorities,
- police authorities,
- prosecutors, and
- the courts.

A comprehensive and effective AML/CFT framework, together with timely implementation and effective enforcement, on the other hand, reduce the profitable aspects of 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 AML/CFT framework.

2. Damaged Reputation and International Consequences

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
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.11 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 helps fight crime and corruption. When money laundering itself is made a crime, it provides another avenue to prosecute criminals, both those who commit criminal acts and those who assist them through laundering illegally obtained funds. Similarly, an AML/CFT framework that 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 eliminates certain profits altogether, thereby reducing the incentive to commit criminal acts. Thus, it should go without saying that the broad scope of predicate offenses for money laundering, the greater the potential benefit.

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 finan-
cial 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.13

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.
Chapter III
International Standard Setters

A. The United Nations
   1. The Vienna Convention
   2. The Palermo Convention
   3. International Convention for the Suppression of the Financing of Terrorism
   5. Global Programme against Money Laundering
   6. The Counter-Terrorism Committee

B. The Financial Action Task Force on Money Laundering
   1. The Four Recommendations on Money Laundering
   2. Monitoring Members’ Progress
   3. Revising Money Laundering Trends and Techniques
   4. The FATF list
   5. Special Recommendations on Terrorist Financing
   6. Methodology for AML/CFT Assessments

C. The Basel Committee on Banking Supervision
   1. Statement of Principles on Money Laundering
   2. Core Principles for Banking
   3. Counter-Terrorism

D. International Association of Insurance Supervisors

E. International Organization of Securities Commissions

F. The Egmont Group

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. 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. Second, the UN actively operates a program to fight money laundering; the Global Programme Against Money Laundering which is headquartered in Vienna, Austria, and is part of the UN Office of Drugs and Crime. 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 a country through a Security Council Resolution regardless of other action.

1. The Vienna Convention

As a result of growing concern with 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 the money

---

1. There were other international efforts, e.g., “Measures Against the Transfer and Safekeeping of Funds of Criminal Origin,” adopted by the Committee of the Council of Europe on June 27, 1980. It is beyond the purpose of this Reference Guide, however, to discuss in detail the history of the international effort to fight money laundering.
4. The UNDCP was renamed the Office of Drug Control and Crime Prevention (ODCCP) in 1997, and renamed the Office of Drugs and Crime (ODC) in October of 2002.
laundering resulting from it. 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). The Vienna Convention, named for the city in which it was signed, and 166 countries are party to the convention, and deals primarily with provisions to fight the illicit drug trade and related law enforcement issues. Although it does not use the term *money laundering*, the convention defines the concept and calls upon countries to criminalize the activity. The Vienna Convention is limited, however, to drug trafficking 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). 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;
- establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;  

---

7. *The Vienna Convention*, Article 3 (b) and (c) (i).
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; and
• promote international cooperation.

According to the UN, this convention is not yet in force; it has been
signed by 147 countries and ratified by 32 countries. Forty countries need
to ratify this convention before it can enter into force. The Palermo
Convention is important because its AML provisions adopt the same
approach previously adopted by the Financial Action Task Force on Money
Laundering in its Forty Recommendations.

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). This convention came into force on April
10, 2002, and 132 countries have signed the convention and 76 countries
have ratified it.

This convention requires ratifying states to criminalize terrorism, terrorist
organizations and terrorist acts. Under the convention, it is unlawful for any per­
son 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).
14. Id.
treatyI.asp.
4. Security Council Resolution 1373

Unlike an international convention, which requires 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 terrorist, including freeing 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. Global Programme against Money Laundering

The UN Global Programme against Money Laundering (GPML) is within the UN Office of Drugs and Crime (ODC). 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.

6. 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, 2001.20 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, nor is it a sanctions committee, 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.

20. UN Security Council Resolution 1373.
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 laundering. 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 29 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.

1. The Forty Recommendations on Money Laundering

FATF has adopted a set of 40 recommendations, *The Forty Recommendations*, which constitute a comprehensive framework for AML and are designed for universal application by countries throughout the world. *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 in Chapter V, VI, VII, VIII of the Reference Guide.

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 mem-
ber 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 countries 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.

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 to their financial institutions and

---

businesses with respect to international transactions, as well as their reputation internationally.

5. Special Recommendations on Terrorist Financing

FATF also focuses its expertise on the world-wide effort to combat terrorist financing. To accomplish this expanded mission FATF has adopted eight 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

Throughout 2002, FATF, the International Monetary Fund (IMF), the World Bank, and other standard setters, in consultation with the FSRBs, worked on a methodology to assess The Forty Recommendations and the Special Recommendations, and completed a comprehensive assessment methodology. At its plenary session in October of 2002, FATF adopted this single, comprehensive methodology to be used in making its mutual assessments.

The development of the comprehensive methodology is intended to fill a gap in assessment procedures. First, it is intended to facilitate a more uniform approach worldwide in conducting assessments based on The Forty Recommendations and Special Recommendations. Second, it provides a framework to integrate the work of the different standard setters, as it pertains to AML/CFT, and there has been extraordinary international cooperation and agreement in this regard among the standard setters. Third, the

---

development of the methodology provides a framework for acceptance of The Forty Recommendations and Special Recommendations as the twelfth standard recognized by the IMF and Bank as useful to their operational work, and where Reports on Standards and Codes (ROSCs) would be prepared.

The methodology has now been approved by all of the relevant parties that will be making assessments. The methodology consists of 120 criteria covering each of The Forty Recommendations and Special Recommendations. 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. It also addresses implementation of the AML/CFT regime in the non-prudentially regulated financial sector.

C. The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 countries. Individual countries are represented by their central bank and also 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.

36. See 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.
38. 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, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States.
Three of the Basel Committee's supervisory standards and guidelines concern money laundering issues.

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 becoming associated with criminals or being used as a channel for money laundering." 39

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. 40 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. 41 Here, banks should not offer services or provide

40. Id., at Preamble paragraph 6.
41. Id., at Customers identification.
42. Id., at Compliance with laws.
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 customer confidentiality. 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 Statement on Prevention. Furthermore, banks should ensure 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 Core Principles for Effective Banking Supervision (Core Principles), 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 being used; intentionally or unintentionally, by criminal elements.

43. Id., at Cooperation with law enforcement authorities.
44. Id., at Adherence to the Statement.
46. Id., Core Principle 15.
These “know your customer” or “KYC” policies and procedures are a crucial part of an effective AML/CFT institutional framework for every country.

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 use assess the adequacy of KYC policies and procedures. These, additional criteria include specific reference to compliance with The Forty Recommendations.

3. Customer Due Diligence

In October of 2001, the Basel Committee issued an extensive paper on KYC principles entitled, Customer due diligence for banks (Customer Due Diligence). 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 standard are set out in detail in this document.

It is worth noting that these KYC standards set out in 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 Customer Due Diligence “be consistent with the FATF recommendations."

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.  
49. Id.
50. Id., at paragraph 3.
51. For a list of member countries and jurisdictions, see Members at http://www.iaisweb.org/fr/members/about.html. The listing of members contains hyperlinks to individual member websites.
Its primary objectives are to:

- promote cooperation among insurance regulators,
- set international standard for insurance supervision,
- provide training to members, and
- coordinate work with regulators in the other financial sectors and international financial institutions.\(^2\)

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.\(^3\)

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,\(^4\) 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.

The four principles parallel the four principles in the Basel Committee's *Statement on Prevention.* The *AML Guidance Notes* are entirely consistent

---

\(^2\) Id., at Home page.
\(^3\) 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)\(^5\) 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 91 countries.\(^6\) 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 type 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.\(^7\)

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 recommenda-
tions 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

---

tion.pdf.
enhancing the ability of relevant authorities to identify and prosecute money launderers;
2. The extent and adequacy of record-keeping requirements, from the perspective 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 transactions, 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."

F. The Egmont Group

As part of the effort to fight money laundering, governments have created agencies to analyze information submitted by financial institutions 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."

59. See discussion in Chapter VII of this Reference Guide.
In 1995, a number of governmental units known today as FIUs began working together and formed the Egmont Group (named for the location of its first meeting at the Egmont-Arenberg Palace in Brussels). The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

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, or (ii) required by national regulation, in order to counter money laundering.” 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 is currently comprised of 69 jurisdictions. Members of the Egmont Group have access to a secure website, which is not available to the public, to exchange information.

Finally, the Egmont Group has produced a compilation of one hundred sanitized cases about the fight against money laundering from its member financial intelligence units.

---

Chapter IV

Regional Bodies and Relevant Groups

A. FATF-Style Regional Bodies

1. Asia-Pacific Groups on Money Laundering
2. Caribbean Financial Action Task Force
3. Council of Europe—MIFID AML
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-
ment of FATF's *The Forty Recommendations on Money Laundering (The Forty Recommendations)* and the eight *Special Recommendations on Terrorist Financing (Special Recommendations).* They also administer mutual evaluations of their members, which are intended to identify weaknesses so that the member may take remedial action. Finally, the FSRBs provide information to their members about trends, techniques and other developments for money laundering in their Typology Reports, which are usually produced on an annual basis.

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 are:

1. Asia/Pacific Groups on Money Laundering (APG)
2. Caribbean Financial Action Task Force (CFATF)

---

2. Member jurisdictions are: Australia, Bangladesh, Brunei Darussalam, Chinese Taipei, Cook Islands, Fiji, Hong Kong China, India, Indonesia, Japan, Macau-China, Malaysia, Marshall Islands, Nepal, New Zealand, Nine, Pakistan, Republic of Korea, Palau, Philippines, Samoa, Singapore, Sri Lanka, Thailand, United States and Vanuatu.

   Observer jurisdictions are: Cambodia, Canada, France, Lan People's Democratic Republic, Mongolia, Papua New Guinea, Republic of Kiribati, Republic of the Maldives, Republic of Nauru, Tonga, Union of Myanmar, United Kingdom and Vietnam.

   Observer organizations are: Asian Development Bank (ADB), Asia Pacific Economic Cooperation (APEC), Association of South East Asian nations (ASEAN), Caribbean Financial Action Task Force (CFATF), Commonwealth Secretariat, Egmont Group, FATF, International Monetary Fund (IMF), INTERPOL, Offshore Group of Banking Supervisors (OGBS), Pacific Financial Technical Assistance Centre (PFTAC), Pacific Islands Forum Secretariat (PIFS), The World Bank, World Customs Organization (WCO) and United Nations (UN) International Drug Control Programme (UNDCP) and UN Office on Drugs and Crime (UNODC), [http://www.apgml.org](http://www.apgml.org).

3. Member countries are: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, Grenada, 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. (continued)
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 their 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

---


4. Members are: Albania, Andorra, Armenia, Azerbaijan, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Liechtenstein, Lithuania, Malta, Moldova, Poland, Romania, Russian Federation, San Marino, Slovakia, Slovenia, Former Yugoslav Republic of Macedonia and Ukraine.

Observers are: Commission of the European Communities, Commonwealth Secretariat, European Bank for Reconstruction and Development (EBRD), FATF (Secretariat and Member Countries), International Monetary Fund (IMF), Interpol, Offshore Group of Banking Supervisors (OGBS), Secretariat General of the Council of the European Union, United Nations Crime Prevention and Criminal Justice Division, United Nations Office on Drugs and Crime (UNODC), World Bank and World Customs Organisation (WCO), http://www.coe.int/EN/Legal_affairs/Legal_cooperation/Combating_economic Crime/Money laundering/.

5. Members are: Kenya, Malawi, Mauritius, Mozambique, Namibia, Seychelles, Swaziland, Tanzania, Uganda, Botswana, Lesotho, South Africa, Zambia, and Zimbabwe have joined ESAAMLG, but have not yet signed its memorandum of understanding.

Observers are: Commonwealth Secretariat, FATF Secretariat, United Kingdom, United States and World Bank, http://www.esaamlg.org.

6. Members are: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru and Uruguay. Observers are: France IDB, Mexico, Portugal, Spain, and United States, http://www.gafisud.org/english/index.html.

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


B. Wolfsberg Group of Banks

The Wolfsberg Group of Banks, named after the town in Switzerland where the group was formed, represents a group of international private banks. The group has established three 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.

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 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. “Know your customer” (KYC) policies and procedures should be enhanced with searches of lists of known or suspected terrorists. In addition, banks should apply extra due diligence whenever they see suspicious or irregular activities, especially 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.

3. Anti-Money Laundering Principles for Correspondent Banking

The Wolfsberg Group has adopted a set of principles to govern the establishment and maintenance of correspondent banking relationships on a global basis. The principles prohibit international banks from doing business with “shell banks.” 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 bank to consider the client bank’s:

- domicile;
- ownership and management structure;
- business portfolio, and
- client base.

13. Id., principles 4 and 5.
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.

C. The Commonwealth Secretariat

The Commonwealth Secretariat is a voluntary association of 54 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 and the CFATF, APG and ESAAMLG.


16. 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, Zambia, and Zimbabwe, http://www.thecommomwealth.org/.

17. The manual is only available directly from the Commonwealth Secretariat; it is not currently available online.


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.

18. 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.


Chapter V

Legal System Requirements

<table>
<thead>
<tr>
<th>A. Ratification and Implementation of the Vienna Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Criminalization of Money Laundering and Terrorist Financing</td>
</tr>
<tr>
<td>1. Proceeds of Crime</td>
</tr>
<tr>
<td>2. Terrorist Financing</td>
</tr>
<tr>
<td>3. State of Mind</td>
</tr>
<tr>
<td>4. Corporate Liability</td>
</tr>
<tr>
<td>5. Reporting Liability for Laundering</td>
</tr>
<tr>
<td>6. Launderers' Fees</td>
</tr>
<tr>
<td>C. Seizure, Confiscation and Forfeiture</td>
</tr>
<tr>
<td>1. Confiscation of Free and Related Proceeds of Crime</td>
</tr>
<tr>
<td>2. Enforced Confiscation of Property</td>
</tr>
<tr>
<td>3. Third Party Liability</td>
</tr>
<tr>
<td>4. International Aspects of Confiscation</td>
</tr>
<tr>
<td>D. Scope of Covered Financial Institutions</td>
</tr>
<tr>
<td>E. Integrity Standards</td>
</tr>
</tbody>
</table>

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. Other specific requirements for combating the financing of terrorism (CFT) are discussed in Chapter IX. Consequently, this chapter discusses five legal system requirements that are principles primarily for AML. These principles permit each country to adopt laws that are consistent with both its own cultural circumstances, legal precepts and constitution, as well as international standards. They are:

- ratification and implementation of the Vienna Convention;
- criminalization of money laundering and terrorist financing;

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

- laws for seizure, confiscation and forfeiture of illegal proceeds;
- the types of financial institutions to be covered; and
- integrity standards for financial institutions.

The legal system requirements for AML, as well as others 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). 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 complying with international standards. Thus, each FATF recommendation should be considered very carefully by a country as it establishes or improves its institutional AML framework.

### A. Ratification and Implementation of the Vienna Convention

The starting place for implementing an AML institutional framework is the ratification and implementation of the *Vienna Convention*. This is the first recommendation of FATF. Many countries have ratified this convention; the issue, however, is whether the country has taken sufficient steps to implement fully its requirements. The *Vienna Convention* serves as a basis for a number of other FATF recommendations on preventing, detecting, and prosecuting money laundering, which are discussed in detail in this and other chapters of the Reference Guide.

The United Nations (UN) took the first step toward criminalizing international money laundering in 1988, when it instituted the *Vienna Convention*. The convention created three categories of criminal offenses related to money laundering, although it did not use the term “money laundering” in any of the three categories.

The first type of money-laundering crime identified in the convention involves either (a) the transfer or conversion of property with the knowledge

---

3. *Id.*, Rec. 1.
that such property is derived from a drug-trafficking offense for the purpose of concealing or disguising its illicit origin, or (b) helping another to evade the legal consequences of his or her other actions.  

The second type of money laundering offense is defined as an effort to conceal or disguise 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. The third type of offense involves acquiring, possessing, or using property with the knowledge that it is derived from a drug-trafficking offense.  

Under the Vienna Convention, countries are obligated to enact the first two types of offenses into domestic law; the third offense is not mandatory. Rather, the third offense is specifically subject to each country’s “constitutional principles and basic concepts of legal principles.”

The Vienna Convention’s definitions of criminal money laundering are the most widely accepted definitions of the concept and the ones used in all of the current international legal instruments on this topic. The Vienna Convention’s definitions are incorporated in The Forty Recommendations by FATF, which state, among other things, that “each country should take such measures as may be necessary, including legislative ones, to enable it to criminalize money laundering as set forth in the Vienna Convention.”

B. Criminalization of Money Laundering and of Terrorist Financing

If the international community is to have any hope of preventing the criminal activities related to the laundering of money and the financing of terrorism, each country must have a legal framework that criminalizes these activities. Criminalization serves three principal objectives. First, it compels compliance with AML preventive 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. Predicate Offenses

A predicate offense for money laundering is the underlying criminal activity that generates proceeds, which when laundered, lead to the offense of money laundering. Designating certain criminal activities as predicate offenses for money laundering is necessary to comply with international standards. Because the Vienna Convention was drafted as an international drug-control instrument, the predicate offenses for money laundering relate only to drug-trafficking offenses. Subsequent instruments that adopted the Vienna Convention language with respect to the definition money laundering have

invariably expanded the scope of the predicate offense to include other substantial profit-generating crimes.

In fact, FATF encourages countries to extend the scope of the predicate offense to include all serious offenses, including those that are not necessarily drug-related.14 The Council of Europe adopted a very broad definition of predicate offenses in its Anti-Money Laundering Convention, a definition that is not confined to the laundering of drug money.15 The United Nations Convention against Transnational Organized Crime (2000) (Palermo Convention) imposes an obligation on all State parties to apply the convention’s money-laundering offenses to “the widest range of predicate offenses.”16

Similarly, the UN adopted a broad definition of the predicate offense in the UN Model Legislation, permitting each country either to define the predicate offense by category, by a sanction-based assessment of seriousness, or by a list of specific offenses.17 Although the UN Model Legislation is nearly silent on the scope of the predicate offense, it does envision a broad definition of predicate offenses. The UN Model Crime Bill, on the other hand, defines the predicate offense as any “serious offense.”18 The definition of “serious” is determined by a sanction of imprisonment not less than a certain duration; the UN Model Crime Bill proposes a 12-month duration, although alternative durations are permissible.19 Countries may choose to extend the list of predicate offenses to a pre-set list of crimes. For example, a listing of crimes could include smuggling (arms, people, goods, etc.), fraud, theft, embezzlement, racketeering, prostitution and kidnapping. In short, the profit-generating character of a given criminal activity becomes the criterion in deciding whether that activity is a predicate offense for money laundering.

With regard to the UN Model Legislation, or other model legislation, such instruments should be treated as suggested approaches and language for drafting legislation; they should not be merely copied. In the drafting process, model laws should be adapted to take into account the particular country’s circumstances, constitution and legal principles.

15. Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 1(e) & article 6(4) and Explanatory Report para. 16.
17. Article 1, 1.2 (a).
18. Section 2(n) and (s) and Section 17.
19. Id.
Because criminalization is a matter of domestic jurisdiction, different countries will make different determinations about what constitutes a predicate offense for money laundering. To prevent these inevitable national variations from undermining the effectiveness of mutual legal assistance and extradition matters, each country needs to be constructive in applying its criminality and territoriality principles so as not to thwart the law's overall intent; this applies to all money laundering offenses, regardless of the predicate offense. In order to facilitate international legal assistance and extradition arrangements, it may be necessary to ensure that the predicate offense is a crime in all countries involved; the country where the crime was committed, the country requesting assistance, and the country whose assistance is requested.

The extension of the predicate offense to cover all serious offenses, regardless of jurisdiction, is more conducive to international cooperation and more consistent with the transnational character of money laundering activities. There would be a significant international limitation if a country were to require that, in order for a money-laundering offense to occur, the proceeds should derive only from a predicate offense committed within its jurisdiction. Countries should especially consider exempting from the territoriality principle those predicate offenses that generate large proceeds and which typically result in complex transnational laundering operations, such as drug trafficking and corruption.

2. Terrorist Financing

Those who finance terrorism, like criminals, use the international financial system to hide the funds they need to support their activities, even if these funds have legitimate sources. A practical way to undermine the capacity of these organizations is to help prevent their funds from entering the global financial system, in the first place. Failing that, a country needs legislation to detect when terrorist funds have entered its borders so that the funds can be confiscated and forfeited.

In its eight Special Recommendations on Terrorist Financing (Special Recommendations), ATF urges countries to criminalize the financing of terrorism, terrorist acts and terrorist organizations and to designate these as predi-
cate offenses of money laundering. This issue is discussed in greater depth in Chapter IX.

3. State of Mind

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 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 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; this language was adopted by the UN Model Crime Bill. The Model Bill also envisages some money-laundering offenses with specific intent such as concealing or disguising the origin, nature, location, disposition, movement, or ownership of the property. Also, some money-laundering offenses could require proving the specific

---

21. The Vienna Convention, article 3(b)(i).
24. Id., at subparagraph (a).
25. UN Model Crime Bill, at Section 17(a).
intent of an individual to assist another in evading the legal consequences of his or her actions.²⁶

A broad definition of the "state of mind" was adopted in the OAS-Model Regulations.²⁷ These model regulations address three different states of mind: that (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.²⁸ 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 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 Model Regulations further provide that these three culpable states of mind can be inferred from objective and factual circumstances.²⁹

Because of the difficulty inherent in proving the state of mind of a person who is engaging in an activity that is ordinary on its face, the Vienna Convention, FATF and many the other legal instruments provide that the law should permit the inference of the required state of mind from objective factual circumstances.³⁰

4. Corporate Liability

Money laundering often takes place through corporate entities. The concept of corporate criminal liability, however, varies greatly among different coun-

²⁶ Id., at subparagraph (b).
²⁷ OAS-Model Regulations.
²⁸ OAS-Model Regulations, Article 2.
²⁹ Id., at subparagraph (5).
³⁰ The Vienna Convention, article 3(3); The Evity Recommendations, Rec. 5; Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 6(2)(c); United Nations Convention against Transnational Organized Crime (2000), article 6(2)(b).
tries. 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 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.

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.” In the UN Model Crime Bill, the UN defines “person” for the purposes of the Model Bill as including both natural and legal persons. While this language defines “person” more narrowly than that of the OAS, it still acknowledges the principle of criminal liability for corporations.

31. The Forty Recommendations, Rec. 6; OAS-Model Regulations, article 15.
32. UN Model Legislation, Article 4.2.3.
33. Id.
34. Id.
35. OAS-Model Regulations, Article 1(6).
36. Section 2(1).
5. 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 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.

The general international standard in this area is a broad laundering offense that permits for the perpetrator to be held 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.

6. Lawyers’ Fees

The offenses of 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

37. 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 3.1.1; UN Model Crime Bill, Sec. 17; OAS-Model Regulations, Article 2.
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. 38

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 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.

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 laws, whereby authorities may permanently deprive criminals and terrorists of their ill-gotten proceeds. 39

1. Confiscation of Direct and Indirect Proceeds of Crime

International instruments encourage countries to adopt laws that permit the confiscation of the proceeds of crime. In the past under most legal systems, confiscation has largely been confined to the instruments used in the commission of the crime. The 1990 Vienna Convention, however, has provided a framework for the international community to consider the confiscation of the proceeds of crime. This Convention has been adopted by several countries, including the United States. The Convention defines the scope of confiscation and sets out the procedural requirements for such actions. The Convention also contains provisions to prevent the recurrence of the crime and to ensure the effective enforcement of the law.

38. 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.

39. The 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).
sion 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 defines the proceeds of crime as “any property derived from or obtained, directly or indirectly, through the commission of an offense.”40 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 they 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 the instrumentalities used, or intended for use, in laundering.41 Criminals are likely to convert property to some other form if specifically-named property is subject to confiscation prior to the issuance of the confiscation order or its enforcement. They 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 unexecutable, 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.42

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.43 This in turn requires that such authorities have the power to require disclosure or to seize commercial and financial records.44 FATF specifically recommends that banking secrecy laws,

40. Article 11(p).
41. The Forty Recommendations, Rec. 7.
42. The Vienna Convention, article 5; Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 2.
43. The Forty Recommendations, Rec. 7.
44. The Vienna Convention, article 5(3); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 4(1).
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."

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. (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, various international agreements qualify the permissibility of such action by requiring countries to take measures to protect the rights of *bona fide* third parties. 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."

According to the OAS-Model Regulations, the relevant authority is required to give notification of the proceedings. 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

---

47. *The Forty Recommendations*, Rec. 7; The Vienna Convention, article 5(8); Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990), article 8; The Palermo Convention, article 12(3).
49. OAS Model Regulations, Article 6.4.
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 offenses; (2) acquired the property for insufficient consideration; or (3) acquired the property knowing its illicit origin. 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.

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 international 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.

50. Section 36. This is a model law designed for common law jurisdictions.
51. See UN Model Legislation, Article 4.2.9. This is a model law designed for civil law jurisdictions.
52. The 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).
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. Scope of Covered Financial Institutions

An important policy consideration to be made with regard to financial institution requirements is to determine which financial institutions are to be covered by the country’s AML framework. The starting point is, of course, commercial banks and similar institutions. International standards, however, include different types of institutions, many of which may not be thought of as financial institutions. FATF recommends that most of The Forty Recommendations apply to both banks and non-bank financial institutions (NBFIs).

The following are entities that should be considered by a country, depending upon the unique characteristics of NBFIs in that country.

- commercial bank or institution with similar powers;
- trust company;
- private banker;
- branch of a foreign bank located outside of the country;
- broker or dealer in securities or commodities;
- investment banker;
- investment company;
- insurance company;
- currency exchange;
- issuer, redeemer, or cashier of travelers’ checks, checks, money orders or similar instruments;
- dealer in precious metals, stones, or jewels;
- pawnbroker;
- loan or finance company;

53. The Vienna Convention, article 5(b); The Palermo Convention, article 14(3)(b); OAS-Model Regulations, article 7(d); V.
54. The Vienna Convention, article 5(b)(i); The Palermo Convention (2000), article 14(3)(a); OAS-Model Regulations, article 7(e).
55. The Forty Recommendations, Recs. 8 and 9.
travel agency;
licensed sender of money;
telegraph company;
merchant, commodity-trading advisor, or commodity pool operator.

FATF also recommends that countries consider applying certain financial institution requirements to businesses or individuals that conduct certain financial activities. These activities are as follows:

- acceptance of deposits and other repayable funds from the public;
- consumer credit;
- mortgage credit;
- factoring, with or without recourse;
- finance of commercial transactions (including forfeiting);
- financial leasing;
- money transmission services;
- issuing and managing means of payment (e.g., credit and debit cards, cheques, traveler’s cheques, and bankers’ drafts);
- financial guarantees and commitments;
- trading for account of customers (e.g., spot, forward, swaps, futures, options) in:
  - money market instruments (cheques, bills, CDs, etc.);
  - foreign exchange;
  - exchange, interest rate and index instruments;
  - transferable securities;
  - commodity futures trading.
- participation in securities issues and the provision of financial services related to such issues;
- individual and collective portfolio management;
- safekeeping and administration of cash or liquid securities on behalf of clients;
- life insurance and other investment related insurance;
- money changing.
Legal System Requirements

FATF recommends that, at a minimum, the NBFIs that should be included are: bureaux de change, stock brokers, insurance companies, and money transmitter/transfer services.\(^{56}\)

Once the scope of financial institutions to be covered has been determined, it is important that competent authorities be designated to ensure effective implementation of the financial institution's requirements.\(^{57}\) The designation of competent authorities for the implementation purposes also applies to all of The Forty Recommendations.\(^{58}\)

E. Integrity Standards

Money cannot be laundered, nor terrorism financed, without the assistance of financial institutions. When criminals control financial institutions or hold senior management positions, countries find it exceedingly difficult to prevent and detect money laundering. The laws and regulatory measures of a country should be written so that convicted criminals cannot hold or control significant investments in any of a country's covered financial institutions. Similarly, convicted criminals should be prevented from holding any significant management position with such financial institutions, including positions on the boards of directors, executive or supervisory boards, or comparable positions.\(^{59}\)

In this regard, laws or regulations should be in place requiring the registration, authorization, and/or licensing of financial institutions so that such criminal involvement is precluded. These provisions should also require that directors, senior managers and persons holding similar positions are evaluated with regard to expertise and integrity. Such persons should possess the appropriate qualifications, including the skills and experience relevant to the position held in the financial institution. Such persons should have no criminal record for violations of fiduciary duty or similar crimes, and there should be no record of adverse regulatory judgments ren-


\(^{57}\) The Forty Recommendations, Rec. 27.

\(^{58}\) Id.

\(^{59}\) Id., Recs. 25 and 29.
dering that person unfit to hold a position as senior manager, director, or a comparable position.

Country laws or regulations should also provide an effective mechanism to withdraw the license of a financial institution on the basis of substantial irregularities relating to money laundering and the financing of terrorism. The withdrawal of the license should also occur if the financial institution fails to maintain standards of integrity when its large investors or management officials change.\(^6\)

Finally, an effective AML/CFT institutional framework applies certain requirements to financial institutions. These requirements involve customer identification, record keeping, reporting of suspicious transactions and others. Failure to abide by these requirements results in penalties that could include loss of the license to engage in business.\(^7\)

\(^6\) Id., Rec. 29

\(^7\) See Chapter VI for a detailed discussion of these requirements.
Chapter VI

Financial Institution Requirements

A. Customer Identification and Due Diligence
1. Scope of Customer Identification and Due Diligence
2. Who is a Customer?
3. Customer Acceptance and Notification Procedures
4. Monitoring and Minimizing of High Risk Accounts
5. Cases Calling for Increased Due Diligence
6. Extending Due Diligence to Vendor and Others
7. Insurance Sector Measures
8. Security Sector Measures

B. Suspicious Transaction Reporting
1. Suspicious Transactions: What is known
2. "Safe Harbor" Provisions for Reporting
3. Insurance Sector Reporting
4. Securities Sector Reporting

C. Record Keeping Requirements
1. Financial Institution Record Keeping Requirements
2. Insurance Sector Record Keeping Requirements
3. Securities Sector Record Keeping Requirements

D. Cash Transaction Reporting
1. Multiple Cash Transactions
2. Cross-Border Movements
3. Modern Money Management Techniques

E. Privacy Laws Versus Reporting and Disclosure

F. Internal Controls, Compliance, and Audit

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 transfers 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. Thus, it is necessary for a country to make policy decisions about financial institution requirements based upon the unique features of that country’s financial institutions, financial markets, and economy in general. All such decisions, however, should be made with reference to international standards.
A. Customer Identification and Due Diligence

In accordance with international standards set by the Basel Committee on Banking Supervision (Basel Committee) and by the Financial Action Task Force on Money Laundering (FATF), countries must ensure 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 identification requirements are also known as “Know your customer” (KYC), 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.

3. Basel Committee, Core Principle for Effective Banking Supervision, Principle 13 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.”
4. 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/bchb85.pdf.
5. Derived from Basel Customer Due Diligence for Banks (provision 9).
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 regulatory standards exist between the home and host country, the higher or more comprehensive, of the two standards should be applied.

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.

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.

---

7. Id.
9. Id. (provision 21).
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.

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.

10. Id. (provision 20).
11. Id.
12. Id.
13. Id.
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, 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. 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. 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).

14. Id. (provision 22).
15. The Forty Recommendations, Rec.10, and Basel Customer Due Diligence for Banks (provision 30).
17. The Forty Recommendations, Rec. 11.
18. Id., Rec. 10.
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.

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 (see part E of this chapter), or when there is any doubt of that customer’s actual identity. The same would apply in the event of the occasional corporate customer.

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. National supervisors are strongly encouraged to assist financial institutions in developing their own customer acceptance and identification procedures.

4. Maintaining and Monitoring of High Risk Accounts

Financial institutions should avoid accounts kept through correspondent financial institutions located in high-risk jurisdictions with lax legal safeguards against money laundering and terrorist financing. The FATF classifies certain jurisdictions as “noncooperative countries and territories” (NCCT). These jurisdictions pose special high risk issues for financial institutions.

Similarly, transactions with certain types of “shell banks” should also be avoided. In general, the shell banks to be avoided are those incorporated in a jurisdiction having no physical presence or no affiliation with a regulated financial group.

19. See FATF, Spec. Rec. VII.
22. For the complete list of FATF’s “noncooperative” jurisdictions, see http://www1.oecd.org/fatf/NCCT_en.htm.
23. See Basel Customer Due Diligence for Banks (Provision 51).
Financial institutions are strongly encouraged to employ software programs to assist in their management of information. Such programs aid in gathering, analyzing, screening, and communicating data that identify high-risk customers and high-risk activities. They should screen out unusual or suspicious activities. These programs play a key role in detecting potentially suspicious activity amid the vast number of legitimate daily transactions.

In addition, financial institutions should fine-tune their monitoring capabilities to adjust for multiple international accounts, which are sometimes known vehicles for subtle system abuse conducted on a cross-border basis. Financial institutions should account for this potential for abuse by aggregating and monitoring significant balances and activity in accounts on a "worldwide consolidated basis."

5. Cases Calling for Increased Due Diligence

As a general rule, due diligence should be commensurate with an account's perceived risk level. Higher-risk customers and accounts should receive greater scrutiny. Increased diligence should be exercised in the instances identified below:

- transactions in any way suspected to be related to terrorism or organizations that sponsor or assist terrorism;
- fund transfers that do not offer complete originator information (i.e., name, address, and account number);
- new technology that permits customer or transactional anonymity;
- complex, large, or unusual patterns of transactions with no apparent economic or lawful purpose;
- account activity in jurisdictions known for lax legislation on money laundering and terrorist financing;

25. Id.
27. Id., (provision 6).
28. Special Recommendations, Spec. Recs. IV and VII; The Forty Recommendations, Recs. 9, 13, 14, and 21; and Basel Customer Due Diligence for Banks (provisions 23, 29, 35–36, 44, 45, and 52). This list is illustrative and is not exhaustive of all circumstances calling for increased due diligence.
• foreign nationals maintaining accounts in another sovereign absent a clearly expressed reason;
• instances where a financial institution believes another financial institution has refused service to a potential customer;
• business referrals through correspondent banking services (i.e., wire transfers and third-party use of correspondent accounts);
• private banking and high-risk customers, particularly politically exposed individuals and their affiliates; and
• customers who do not present themselves for face-to-face interviews or transactions (e.g., electronic banking via Internet or third-party introduction).

Steps should be taken to mitigate the higher degree of risk posed by such cases. This means obtaining more information about the customer, the account, the institution, the transaction, or the jurisdiction involved. It is standard, for example, for financial institutions to require more information from customers who do not present themselves for face-to-face interviews; such unconventional transactions can be cleared once that additional information is provided. The customer can provide such additional information in the form of certified documents, additional forms of identification, an independent and verifiable customer contact, third-party or institutional referrals that meet KYC standards, or a customer first payment under his or her name at another bank adhering to similar standards.

If the customer is not able to supply sufficient information to address the diligence concerns of a financial institution or if suspicions persist, the institutions should retain the authority not to accept the customer. In this regard, care must be taken to establish the specific reasons for denying service so as not to subject the institutions to potential legal liability. However, the authority to deny service for failure to furnish appropriate customer identification information should be available as an option to institutions.

30. Id.
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 national supervisor may wish to consider implementing policies that incorporate these trends in due diligence.

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 guidelines 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 nonpolicyholders (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.\footnote{See IAIS, Anti-Money Laundering Guidance Notes, http://www.iaiswcb.org/framesets/pas, h/mL.}
B. 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 Methodology) do apply to the securities sector.

B. Suspicious Transactions Reporting

"Employees should be required to report suspicious or unusual behavior to a superior or to internal security." Financial institutions have an obligation, in other words, according to this international mandate, to report suspicious transactions. "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." Institutions reporting suspicious activity should not in any case notify their customers that their behavior has been reported as suspect to authorities. From that point on—which is to say, upon notification—financial institutions must fully comply with instructions from government authorities.


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 financial institu-

32. Id.
34. The Forty Recommendations, Rec.17.
35. Id., Rec.18.
tion 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.
  - 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.

---

36. *Id.*, Rec.34.
37. *Id.*, Rec.28. See also Basel Customer Due Diligence for Banks, (provision 53).
• Signs Regarding Transactions on Deposit Accounts
  - Closing of an account followed 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 guaranties (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 amount 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 so long as the suspicious report was filed in good faith (i.e., it was not frivolous nor malicious)."  

3. Insurance Sector Reporting

The IAIS has established its own set of guidelines for reporting suspicious transactions. The insurance industry should follow these, in addition to the relevant guidelines noted above. Insurance companies should report suspicious activity to the financial intelligence unit or other national centralized

38. The Forty Recommendations, Rec. 16.
authority. The following are 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."

4. Securities Sector Reporting

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.

C. Record Keeping Requirements

1. Financial Institutions Recording Keeping Requirements

Financial institutions should keep customer identity and transaction records for a minimum of five years following the termination of an account. Institutions may be required to retain records for longer than five years if required by regulators. Contents of the records should be made readily available to authorities upon request and, further, be sufficient to permit the prosecution of criminal behavior.

Maintaining records is important for both prevention and detection of money laundering and terrorist financing purposes. If a potential customer

41. Id.
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.\(^\text{45}\)

2. Insurance Sector Record Keeping Requirements

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:

- 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 “discharge documentation”).\(^\text{44}\)

Financial institution supervisors must verify that all representatives for insurance companies are licensed under appropriate insurance law and juris-

\(^{42}\) Id.

\(^{43}\) See IAIS Anti-Money Laundering Guidance Notes.
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 Record Keeping Requirements

The IOSCO has established its own set of record keeping requirements, which securities firms should follow in addition to adhering to the applicable general guidelines listed 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.

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. Such thresholds may be established by statute, or by regulation under the authority of the appropriate...
ate government supervisory agency. Depending on circumstances in a country, such requirements may also apply to certain businesses such as casinos, antique or automobile dealers, or when 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 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.

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 circum-

51. Basel Customer Due Diligence for Banks, provision 16.
stnces, 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.

Finance ministers and customs officials 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.53

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.54

52. The Forty Recommendations, Rec. 22.
53. Id., Rec. 24.
E. Privacy Laws Versus Reporting and Disclosure

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 recommends that financial institution privacy laws should be drafted so as not to inhibit the implementation of any of its recommendations.54

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.55 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.56

54. The Forty Recommendations, Rec. 2.
55. Id.
56. Id., Recs. 19 and 26.
The designation of an AML/CFT compliance officer at the management level, by each financial institution, is the third internal policy recommended. Such a compliance officer helps to ensure that appropriate management attention is devoted to the institution’s compliance efforts.

An audit function is the fourth 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.  

57. Id.  
58. Id.  

VI-19
Chapter VII

The Financial Intelligence Unit

A. Definition of a Financial Intelligence Unit

B. Core Functions
1. Custodial Repository Function
2. Analytical Function
3. Domestic Information Sharing
4. International Information Sharing

C. Possible Additional Functions
1. Regulatory Supervisory Function
2. Law Enforcement Function
3. Prosecution Function
4. Consulting and Training Function

D. Organizational Structure
1. The Various Types of FIUs
2. Choosing the Right Model
3. Capacity Considerations
4. Staffing Considerations

E. Privacy Safeguards
1. The Main Policy Issues: Privacy versus Efficiency
2. Confidentiality Guidelines
3. Speciality Principle
4. Intervisitance and Accountability

If the international community is to fight money laundering and terrorist financing, it 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. Launderers and those who finance terrorism 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.\(^1\) Financial investigations are greatly assisted by a country's comprehensive regime (a) requiring the reporting of certain information and record keeping, and (b) facilitating information sharing among competent authorities, both domestically and internationally. The primary goals of financial investigations are to identify,

\(^1\) United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention), art. 3(b)(i) & (ii), http://www.incb.org/e/conv/1988/
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), recommends that financial institutions be required to report certain information and keep certain records. In general, in its The Forty Recommendations on Money Laundering (The Forty Recommendations), FATF urges countries to impose measures on financial institutions requiring them to maintain records on the identities of their clients and their transactions, as well as to report any suspicious activity. Information generated by these reporting and record keeping requirements is used to reconstruct transactions, to establish the link between individual clients and a particular business, to prove the "state of mind" of an offense (see Chapter V, Criminalizing Money Laundering and Terrorist Financing, and State of Mind), and, finally, to identify the role of an individual in a criminal or terrorist financing enterprise.

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 data. Without such a system in place, investigators have a much more difficult time detecting criminal or terrorist financial dealings. The pressing need for effective data analysis explains the proliferation of FIUs and the growing impor-

3. Id., at Rec. 12.
The Financial Intelligence Unit

tance of their roles in the international effort to prevent, detect and prosecute money laundering and the financing of terrorism.

A. Definition of a Financial Intelligence Unit

All FIUs possess a number of basic functions, consistent with concepts utilized by FATF in The Forty Recommendations, even though FATF does not use the name FIU in describing these financial intelligence authorities. The Egmont Group 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.


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.

Thus, an FIU has four essential functions related specifically to detecting and countering the laundering of money: the "repository" function, data analysis, domestic information sharing, and international information sharing to the proper authorities. These functions are performed by a centralized unit—the FIU.


5. 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.oecd.org/fatf/pdf/EGinfo_web_en.pdf. See also Chapter III, the Egmont Group.

6. The Palermo Convention, Article 7(1)(b).
B. Core Functions

The role of an FIU varies from country to country; most of them, however, share four core functions. For a candidate FIU to qualify for membership in the Egmont Group, it must be able to satisfy these core function. Because money laundering is largely a cross-border activity, however, it is important for FIUs to join forces with other national intelligence units. Money laundering often involves cross-border channels for funds transfers. 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.

1. Centralized Repository Function

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 by other national regulatory or investigative authorities. FIUs must analyze the data they receive because so many suspicious transaction reports 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.

FIU staff members perform three specialized analytical functions. In general, they (1) screen the reported cases in order to identify those that are truly suspect as a step toward directing them to the competent investigative or prosecutorial authorities; (2) provide investigative support by conducting financial analysis upon request in support of an ongoing criminal or regulatory investigation; and (3) conduct “strategic analysis” both to advance the understanding of money-laundering mechanisms and to help invent new ways to prevent and detect them.

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 advanced intelligence techniques and apparatus, such as wire tapping and covert operations, subject to domestic legal principles.

In doing so, each country must balance very real privacy concerns against the FIU’s need for an effective analytical function. While resorting to publicly available commercial databases does not raise privacy concerns, increasing the power of these centralized intelligence units to request additional information does. The same caution applies to FIU surveillance and other intelligence techniques. In this regard, financial institution privacy laws should be drafted so as not to interfere with the functions of the FIU.

The analytical function makes the FIU a buffer between the financial community and the criminal justice system and serves to help protect innocent customers. This kind of buffer is generally enhanced in cases where the FIU is not acting as an investigative authority with criminal justice powers. Furthermore, its intermediary role could be undermined if investigative and criminal justice agencies have direct and unregulated access to the FIU’s

---

8. Id.
financial information databases. Thus, FIUs must be vigilant to ensure that sensitive financial information is never used inappropriately to damage the reputation of innocent persons.

3. Domestic Information Sharing

If it suspects money laundering and 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. It should also be authorized to cooperate and coordinate its actions with the other domestic authorities devoted to the prevention and detection of money laundering.

The importance of timely information sharing with the proper authorities cannot be overstated. Effective measures against money laundering rely on getting the information available to the appropriate authority. For some 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, they make the financial disclosures available to law enforcement authorities immediately; these FIUs conduct analysis on financial disclosures and other financial information upon request or as needed at a later time. In either case, the key is for the FIU to provide competent authorities with financial intelligence as quickly as possible so that they can pursue the leads provided by the FIUs.

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 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.

4. International Information Sharing

Because so much of money laundering and the financing of terrorism 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."

C. Possible Additional Functions

1. Regulatory/Supervisory Function

The FIU or another competent authority should be granted the power to supervise financial institutions and to control their compliance with the record keeping and reporting requirements. The FIU or another competent authority should also be authorized to impose sanctions or penalties against financial institutions for failing to comply with their reporting or record-keeping obligations—for example, meaningful fines and/or license suspensions. The FIU could be authorized to issue financial sector regulations as necessary for the implementation of laws against money laundering.

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. 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 anti-money laundering obligations. Some countries have opted to give the compliance-control responsibility to the FIU. In certain countries, some reporting institutions are not subject to any supervision other than that of the FIU, which makes it the most suitable body to address the cross-disciplinary issues raised in this context.

In addition, the FIU could be authorized to issue financial sector regulations for the implementation of laws against money laundering. Giving such responsibilities to the FIU, however, should take into account issues of capacity, funding and of prioritization. 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 limited, additional supervisory or regulatory function could undermine its core functions.

2. Law Enforcement Function

Even though most of the FIUs have no law enforcement powers, an FIU could be given some enforcement functions based on its direct access to financial information and its ability to deal efficiently with cases where urgent and/or provisional enforcement action is needed.

Countries may grant their FIU 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 will be expected to share information with investigative authorities upon request.

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, one could make the case for granting 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 identify any assets vulnerable to confiscation under the laws against money laundering and terrorist financing. 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 for the purpose of identifying such assets. 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.

3. Prosecution Function

If FIUs were given prosecutorial duties in addition to their core functions of data collecting, data storing, analysis, and information sharing and routing—
which is to say, the authority to conduct criminal investigations and to prosecute money-laundering, terrorist financing, and other related crimes, this authority might pose problems the FIU's vital intelligence function. It could also undermine the FIU's capacity to cooperate at the international level, especially with FIUs that do not prosecute those they are investigating. The added prosecutorial responsibility could also impact the FIU's role as a buffer between financial institutions (and other reporting parties) and the criminal justice system. In this regard, the FIU would not be able to serve as strong an intermediary between the two systems.

4. Consulting and Training Functions

Because of focused and multidisciplinary expertise of an FIU, it could easily serve as the best governmental unit to advise and train personnel from financial institutions in measures to fight money laundering and combat terrorist financing.

Again, countries must consider resource limitations in deciding whether to attach this function to the FIU.

D. Organizational Structure

1. The Various Types of FIUs

Countries generally choose one of three basic models in establishing an FIU:

a. the administrative agency 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 force, whether general or specialized; or

c. the prosecutorial model, where the agency is affiliated with the prosecutor's office as a judicial authority.
With regard to these three different organizational models, the following general conclusions can be drawn. The administrative model creates a less-independent FIU, but it tends to enjoy the trust of the financial sector, possess greater expertise about the financial system itself, and is better able to exchange information with its counterparts around the world (most of whom are administrative-model financial intelligence units). The law enforcement model, too, lacks certain independence. Add to this the drawback that its financial expertise—and thus the trust of the financial sector—is not as great as that enjoyed by FIUs based on the administrative model. Financial institutions are more reluctant to report suspicious activity to a police-based FIU if they know their clients immediately become subject to police investigation.

The prosecutorial model, the third option, enjoys independence, but lacks trust as well as actual contact with the financial sector. In many instances, it also lacks the ability to exchange information with foreign counterparts through FIU communication channels because most of these are administrative. Purely prosecutorial FIUs may not be able to take part as effectively in the international exchange of information among FIUs because their duties and obligations as judicial authorities do not allow them to exchange intelligence information on an informal, flexible, rapid, and/or confidential manner, unless specific legal provisions permit otherwise.

Although these conclusions simplify discussion, they also run the risk of oversimplification. For instance, attaching an FIU to a certain agency does not necessarily determine its entire nature. Staffing, functions, powers, and governing procedures are very important in this regard. Indeed, most existing FIUs actually use a mixed model, with administrative as well as some law enforcement and/or prosecutorial functions.

In addition, assessments of the different models are based on psychological perceptions about a host of matters, such as the degree of trust between the financial industry and a given model. Such impressions may vary greatly depending on the country and its culture. Thus, each of these issues is an important consideration.

Moreover, there is the distinction, although not at all clear cut, between the law enforcement/prosecutorial and the administrative models. If the police unit is a law enforcement agency whose primary responsibility is to gather evidence for the purpose of criminal prosecution, such definition could apply equally to many administrative departments with law enforce-
ment responsibilities, such as customs. Furthermore, a number of existing police or judiciary-based FIUs are given purely administrative powers (for example, depository and analytical functions) without any law enforcement powers, which makes them function more like FIUs based on the administrative model.

Identifying the various options for creating FIUs should not proceed from simple categorizations. The appropriate institutional base is but one of many questions that needs to be addressed when countries set about to establish effective financial intelligence units.

2. Choosing the Right Model

Good decisions about the proper model to adopt when setting up 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; they are given below in the form of questions:

- Does the proposed FIU possess relevant capacity and expertise in financial operations?
- What is the relationship between this particular institution and the financial industry in the domestic context?
- Does the institution possess a culture conducive to protecting the confidentiality of financial information and to mitigating potential harm to individual privacy?
- 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 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?
3. Capacity Considerations

Financial investigations are only as good as the individual investigators and the technological infrastructure that supports their efforts. A country must make policy determinations on how the FIU can make the best use of the financial analysis 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.

4. 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 comprehension of reporting entities, to the extent that the entities are financial institutions. 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 investigators means that some countries might opt for staffing their units with experts seconded from other agencies. Although 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.
E. 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.¹⁰

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.¹¹ Cumbersome procedures also hamper investigative efforts to gather information and/or evidence abroad. With financial globalization, such concerns have become even more acute. Money laundering laws can be seen as an attempt to ensure efficient information exchange and evidence gathering, both nationally and internationally, as prerequisites for effective regulatory and criminal law enforcement in today's globalized economy.

The very sensitive and confidential nature of individual 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 the boundaries

¹⁰. 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 so as to inhibit the exchange of information, in accordance with these principles, between or among FIUs; see The Egmont Group, Principles for Information Exchange between Financial Intelligence Units for Money Laundering Cases, (June 13, 2001), Principle 7, http://www.oecd.org/fatf/pdf/EGstat-200106_en.pdf.

¹¹. The Forty Recommendations, Rec. 2
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 the most important protection against abuse of private financial information. This principle will also enable the FIU to exercise its functions as an intermediary between the reporting financial institutions 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. 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 institutions, 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. Confidentiality requirements should be drafted in a way that does not inhibit international cooperation among FIUs.

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 from financial institutions, or requested by the FIU from such institutions. If an FIU is prohibited from using information provided to it for any purpose other than fighting money laundering and terrorist financing, countries can develop a sense of trust between reporting institutions and the FIU.

The specialty limitation necessarily depends on what it means to be “fighting 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 unit’s duties, as described in the law that established 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. 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.15

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

15. Id., at Principles of Information Exchange between Financial Intelligence Units for Money Laundering Cases (June 13, 2001), Principles 11 and 12.
be subject to abuse or undue influence from other government authorities. This sense of independence also supports a sense of trust between the FIU and reporting financial institutions, which 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 independence should, however, be accompanied by proper accountability mechanisms, such as parliamentary reporting, audits, and/or judicial oversight.
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 looking for safe havens with lax, ineffective or corrupt AML and combating the financing of terrorism (CFT) regimes, or those with limited international-cooperation capabilities, countries will find that having a proper international 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 international cooperation, they need to meet several prerequisites, including: (1) building a comprehensive and efficient domestic capacity; (2) ratifying and implementing the international conventions regarding money laundering and terrorism financing; and (3) complying with the recommendations of the Financial Action Task Force on Money Laundering (FATF), i.e. The Forty Recommendations on Money Laundering (The Forty Recommendations) and the eight Special Recommendations on Terrorist Financing (Special Recommendations), 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

they can perform efficiently their duties is a prerequisite for a country to be able to cooperate at the international level with its partners.  

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, noncorrupt 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), the UN Convention for the Suppression of the Financing of Terrorism (1999), and the UN Convention Against Transnational Organized Crime (2000) (Palermo Convention). These actions are part of FATF’s recommendations.  

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 and Confiscation of the Proceeds from Crime (1990) (the Strasbourg Convention).

---

3. The Forty Recommendations, Rec. 3.
8. The Forty Recommendations, Rec. 35.
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.

3. Complying with the FATF 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 the 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.” 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. 3.
10. Id., at Rec. 32.
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). \(^\text{11}\)

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 authority, should be treated by the requesting authority according to the scope of its request (transparency);

\(^{11}\) Id., at Recs. 3, 34, 37.
• 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. 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.\(^{13}\) 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.\(^ {14}\)

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.\(^ {15}\)

---

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 nonjudicial FIUs. 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.

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 per-
International Cooperation

taining 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 review 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

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

---

17. Id.
18. Id.
19. Id.
20. International Organization of Securities Commissioners (IOSCO), Core Principle No. 11., http://www.ioscweb.org/forms/par.htm; see further the IOSCO Multilateral MOU (May 2012).
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{28}

Assistance should be provided in investigations and proceedings where persons have committed both laundering and the predicate offenses, as well

\begin{footnotes}
\item[26] \textit{Id.}, at Rec. 38.
\item[27] \textit{Id.}, at Rec 36.
\item[28] \textit{Id.}, at Rec 33.
\end{footnotes}
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

29. Id., at Rec 36.
30. Id., at Rec 39.
31. Id., at Rec 40.
Chapter IX

Combating the Financing of Terrorism

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
F. Alternative Remittance Systems
G. Wire Transfers
H. Non-Profit Organizations
I. Self-Assessment Questionnaire on Terrorist Financing

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 in the international community. In October of 2001, the Financial Action Task Force on Money Laundering (FATF) expanded its mission beyond money laundering to also focus on the worldwide effort to combat the financing of terrorism (CFT).

To achieve these goals, FATF adopted eight Special Recommendations on Terrorist Financing (Special Recommendations) at the same time that it amended its mission. Like its earlier efforts, The Forty Recommendations on Money Laundering (The Forty Recommendations), the 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 in combating the financing of terrorism (CFT). Moreover, FATF specifically invites all countries to adopt the Special Recommendations and participate in its self-assessment exercise. Implementation of these Special Recommendations, together with *The Forty Recommendations* on money laundering, set out the basic framework to detect, prevent and suppress terrorist financing and terrorist acts.

The *Special Recommendations* are relatively new. Thus, there is little experience with interpreting and implementing them, although they are not difficult concepts. As a result, FATF also adopted Guidance Notes to help explain the *Special Recommendations*.

### A. Ratification and Implementation of United Nations Instruments

FATF’s first recommendation 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)*.” This part of the recommendation is self-explanatory. As with other ratified conventions, the basic issue is whether, and to what extent, a country has fully implemented its requirements. This issue is compounded by the fact that many fewer countries have ratified this *Convention than the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention)*.

The second part of the first recommendation requires each country to implement fully United Nations (UN) Security Council Resolutions:

8. FATF, Guidance Notes.
Implementation means that a country has all appropriate and necessary measures in place to bring the requirements of the UN Convention and the UN Security Council Resolutions into effect. 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.

Of the five UN Security Council Resolutions, the one that is the most important for FATF compliance purposes 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 terrorist; and
- cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

9. [link]
10. [link]
11. [link]
12. [link]
13. [link]
14. FATF, Guidance Notes, Paragraph 5.
15. Id.
17. S/RES/1371 (2001), [link]
B. Criminalizing the Financing of Terrorism and Associated Money Laundering

The second recommendation contains two elements, which require each country to:

- criminalize the financing of terrorism, terrorist acts and terrorist organizations; and
- establish terrorist offenses as predicate offenses of money laundering. 18

A country can satisfy this second recommendation either by establishing new laws making specific offenses for terrorists financing activities, or by demonstrating how existing criminal offenses can be applied to terrorists financing activities. 19 In addition, terrorist financing offenses should constitute money laundering offenses, even when carried out in another country. 20

C. Freezing and Confiscating Terrorist Assets

Under the third CFT 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,” discussed above. 21 Furthermore, each country should take appropriate action to authorize competent authorities within the country “to seize and confiscate property that the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations.” 22

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. 23 The “frozen” funds or assets remain the property of the owner and

18. Special Recommendations, Spec. Rec. II.
22. Id.
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.

“Seizure” means that the competent government authority has the authorization to take control of the specified funds or assets. 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. Confiscation usually occurs when there is a criminal conviction or judicial decision that determined that the assets to funds were derived from criminal activity, or were intended to be used in violation of law.

D. Reporting Suspicious Transactions Related to Terrorism

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.

Under this fourth recommendation, the term financial institutions refers to both banks and nonbank financial institutions, consistent with the country’s implementation of The Forty Recommendations. At a minimum, financial institutions should include banks, bureaux de change, stockbrokers, insurance companies and money remittance/transmitter services. Also consistent with The Forty Recommendations, other types of professions, businesses and business activities that are subject to the country’s anti-money laundering (AML) laws should be covered by this reporting requirement. The

24. Id., at Paragraph 15.
27. FATF, Guidance Notes, at Paragraph 19.
28. Id.
important point here is consistency in the definition of financial institutions between a 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.28 The “suspect” standard is a subjective standard and is the same as that used in FATF’s AML recommendations.29 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.30

E. International Cooperation

The fifth CFT recommendation, 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.”31 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.32

The first part of this measure 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

---

29. The Forty Recommendations, Rec. 15, which provides: “If financial institutions suspect that funds stem from a criminal activity,” they should promptly report their suspicions.
31. Special Recommendations, Spec. Rec. V.
32. Id.
Combating the Financing of Terrorism

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.18 Exchange of information by means “other than
through mutual legal assistance” means any other arrangement, including
exchange occurring through financial intelligence units (FIUs) or other govern­
mental agencies units that exchange information bilaterally pursuant to memo­
randa of understanding (MOUs), exchange of letter or otherwise.31

The second part of this measure concerns the concepts of “safe haven”
and “extradition.” These terms have the same meanings as the terms “safe
haven,”’ as used in UN Security Resolution 1373,” and “extradite,’” as
used in the UN International Convention for the Suppression of the
Financing of Terrorism.” With regard to extradition, countries should assure
that “claims of political motivation are not recognized as a ground for refusing
requests to extradite persons alleged to be involved in terrorist financing.”40 This concept and phrasing are from the UN Convention on
Suppression of the Financing of Terrorism.”

F. Alternative Remittance Systems

Each country should take actions to ensure that individuals and legal entities
that provide for “the transmission of money or value, including transmission
through an informal money value transfer system or network” are licensed or
registered and subject to the same standards, i.e. The Forty Recommendations,
that apply to banks.35 In addition, those that perform such services illegally
should be subject to administrative, civil or criminal sanctions.43

34. FATF, Guidance Notes, at Paragraph 24.
35. Id., at Paragraph 25.
37. UN Security Resolution 1373 (2001), at paragraph 2 (e).
38. Id.
39. UN Convention of Suppression of the Financing of Terrorism, at Article 11,
41. Article 14.
42. Special Recommendations, Spec. Rec. VI.
43. Id.
Formal money remittance or transfer services are often provided by a distinct category of non-bank financial institutions (NBFI's), 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 FATF Forty Recommendations, these money transmitters are included as a covered NBFI and considered subject to the regulated financial sector.44

The “informal 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.45 In many jurisdictions, these informal systems have traditionally operated outside the regulated financial sector, as described above. Such informal systems include the Black Market Peso Exchange, hundi or Hawala systems.46

The goal of Special Recommendation VI is to assure that countries impose AML and CFT requirements on all forms of money/value transfer systems.47 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.48 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.49 Such a requirement is consistent with The Forty Recommendations.50

44. The Forty Recommendations, Rec. 8.
45. FATF, Guidance Notes, at Paragraph 31.
47. FATF, Guidance Notes, at Paragraph 29.
49. FATF, Guidance Notes, at Paragraph 32.
Combating the Financing of Terrorism

G. Wire Transfers

Each country should take appropriate actions to require covered financial institutions, including money remitters, 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 of suspicious activity of, funds transfers that do not contain complete originator information.

The recommendation appears to be rather straightforward, although there have been issues with its interpretation. First, although the wording of the recommendation implies that it would apply to all covered financial institutions, the guidance notes provide that there are three categories of financial institutions of concern: (1) banks, (2) bureaux de change, and (3) money remitters or transfer services. Stockbrokers and insurance companies may be subject to this recommendation in certain jurisdictions, although no further clarification is currently provided.

A proposed interpretative note has been issued with regard to Special Recommendation VII. It would expand the definition of financial institution and provide more specific information about which transfers are to be covered and what information should be maintained for each type of transfer. The interpretative note also proposes to permit exemptions from these requirements for certain types of transfers. Thus, a country should consult the FATF website in order to obtain the latest information relating to the implementation of this recommendation.

---

51. Special Recommendations, Spec. Rec. VII.
52. Id.
53. FATF, Guidance Notes, at Paragraph 35.
54. Id.
56. Id.
H. Non-Profit Organizations

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. In particular, a country should ensure that its non-profit organizations cannot be misused:

- by terrorist organizing posing as legitimate ones;
- to exploit legitimate entities as conduits for terrorist financing, including to avoid asset freezing measures; and
- to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

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 terrorist. In this regard, the recommendation is rather general because the different entities categorized as non-profit organizations take various legal forms and the nature of their operations varies from jurisdiction to jurisdiction.

In an effort not to require adherence to a rigid set of rules that may be of little or no meaning in certain jurisdictions, this measure consists of general guidance and goals to be achieved, rather than specific requirements. Also, 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.*

---

58. *Id.*
60. *Id.*
I. 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). The SAQFT was initially used only by FATF members. Upon completion of the initial assessment of the SAQFT, FATF determined to issue guidance notes on the Special Recommendations and the SAQFT. The SAQFT is also available on the FATF website and may be used by any country for its own assessment purposes.

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 Strategies

B. Development of a Universal AMJ/CFT Assessment Methodology
   1. Twelve-Month Pilot Program
   2. Reports on the Observance of Standards and Codes

C. Building Institutional Capacity
   1. Organization of Training Conferences
   2. Delivery of Technical Assistance to Individual Countries
   3. Coordination of Technical Assistance

D. Research and Analysis
   1. Analysis of the Hawala System
   2. 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.

Essentially, the overall 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


X-1
The overall mission of the IMF is macro-economic and involves financial 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 a 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.7

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.7 Taking into account that money laundering has potentially devastating economic, political and social consequences for countries that are in the process of developing their domestic economies, their financial systems and building strong financial institutions, the Bank recognized that money laundering has potential important costs for 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 anti-money laundering (AML) and combating the financing of terrorism (CFT). Furthermore, the Boards recognized, in July and August 2002, the FATF The Forty Recommendations on Money Laundering (The Forty Recommendations) and the eight Special Recommendations on Terrorist Financing (Special Recommendations) as the relevant international stan-

---

World Bank and International Monetary Fund Initiatives

dards for AML/CFT. The Boards added the 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 in November 2002.

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, their implications for the country, share the experiences that other countries have had, and 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:

- the challenges faced by countries in the struggle against illicit money flows;
- sharing the lessons of success;
- identification 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 struc-
ture 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 ter­
rorist 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 finan­
cial 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 partic­
ular experiences as well as the broader experience of international experts.

2. Country Assistance Strategy

The Bank is integrating the results of the Financial Sector Assistance 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 find­
ings, AML/CFT assistance has already been included in ten 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 signifi­
cant 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.

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, comprehen­
World Bank and International Monetary Fund Initiatives

sive AML/CFT assessment methodology. This methodology has been agreed upon and endorsed by FATF at its October 2002 Plenary meeting. The methodology consists of 120 criteria covering each of the FATF Forty and Special Recommendations, including implementation of criminal law enforcement. It covers the legal and institutional AML/CFT framework for a country, including the establishment of financial intelligence units (FIUs). The methodology also covers relevant United Nations (UN) Security Council Resolutions and international conventions and other measures of international standard setters. It provides an in-depth assessment of the preventive measures for financial institutions.

1. Twelve-Month Pilot Program

This assessment program has been adopted for a 12-month pilot period, which started on November 15, 2002. The Boards of Executive Directors of the Bank and the Fund have underlined the crucial importance for the assessments to be conducted in conjunction with the delivery of appropriate technical assistance (at the request of the countries) to help countries build their institutional capacity to fight money laundering and terrorist financing, to remedy their vulnerabilities and to bring their AML/CFT regime into compliance with the FATF’s The Forty Recommendations and Special Recommendations.

2. Reports on the Observance of Standards and Codes

The Bank and the Fund have adopted an AML/CFT assessment program designed to produce Reports on Observance and Standards and Codes (ROSCs) in this area. The assessments leading to a ROSC will be conducted following two methods, one using the reports made in the context of mutual evaluations by FATF and by the participating FSRBs, the other (applicable to countries that are not members of FATF nor of an FSRB) using a report

5. Id.
made by a Bank/Fund-led mission. Since they are part of the ROSC process, which is a voluntary, cooperative, and uniform process, the AML/CFT assessments conducted by the Bank and the Fund will be undertaken only at the request of a country.  

C. Building Institutional Capacity

1. 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. These conferences were sponsored by the FIRST Initiative with the organizational support of the Bank and the Fund.

The Moscow conference is illustrative of the type of information presented. The focus of the conference was the creation of operational Financial Intelligence 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 a manner officials from participating countries could understand. It also demonstrated the specific steps necessary to begin taking

6. Id.
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.

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. 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.

---

8. Intensified Work on AML/CFT, paragraphs 39 and 40.
3. Coordination of Technical Assistance

In collaboration with donor agencies and international organizations, the World Bank and IMF have developed a database and mechanism for the coordinating AML/CFT TA request.9

The strategic objectives of the AML/CFT TA coordination initiative are to identify high priority TA needs and fill gaps in the delivery of TA, strengthen the roles of the FATF-style regional bodies (FSRBs) in TA coordination at the regional level and enhance information flow on TA needs.

Countries looking for TA normally pursue such assistance through multiple channels: bilateral donors, regional agencies, and directly through the Bank and the Fund. Requests for assistance cover the full range of AML/CFT activities, from establishing a complete regime without any previous statutory base, to funding specialist staff for specific functions, to organizing training programs for the private sector. This existing ad hoc approach can result in delays as multiple sources sort out which entity will provide what TA. In addition, some needs may go unmet, because a willing donor was under the impression that a request was addressed by another donor.

The Bank and the Fund have organized a network of contacts among participating organizations to facilitate coordination and communication of TA activities, to identify providers of TA, and identify potential sources of funding and other resources. A consensus has developed on the following points:

- coordination of TA should be organized on a regional basis through the FSRBs;
- immediate country needs for AML/CFT TA should be identified and responded to by donors and providers
- donors should consider additional for the FSRB secretariats to play an enhanced role in coordinating TA within their regions.

The Bank has taken primary responsibility in maintaining the database and working individually with the FSRB secretariats on the above objectives. As the TA priorities are collected by the FSRBs, the Bank, and the Fund transmit these requests to, and coordinate with, the various donors and TA providers.

---

9. Id., at paragraph 44 through 50.
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. 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; influence exchange rate operations; distort economic data, and thereby, statistical information available to policy makers; and reduce 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 on Terrorist Financing 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. More countries are subjecting these entities to licensing or registration in accordance with the FATF recommendation.

2. The Reference Guide

This Reference Guide on AML and CFT is a product of the Bank and Fund effort 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

10. The citation to this document to be determined in the future.
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 access to all relevant information available from a single and comprehensive source.
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#pgtop (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://www1.oecd.org/fatf/Cty-organpages/org-egmont_en.htm (Countries with operational Financial Intelligence Units)

European Union

- http://europa.eu.int/ (Main page)

Annex I-2
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives

Financial Action Task Force on Money Laundering (FATF)

- http://www1.oecd.org/fatf/ (Welcome page)
- http://www1.oecd.org/fatf/FATDocs_en.htm#Trends (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)
- http://www1.oecd.org/fatf/NCCT_en.htm (Non-Cooperative Countries and Territories)
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://www.cfatf.org/about/about.asp?PageNumber=1 (Membership)

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)
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

- http://www.esaamlg.org (Main site)
- http://wwwl.oecd.org/lfatf/Ctry-orgpages/org-esamlg_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)

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)

International Monetary Fund

- http://www.imf.org/ (Main page)

International Organization of Securities Commissioners

- http://www.iosco.org/iosco.html (Main page)
• http://www.iosco.org/resolutions/index.html (A Directory of Resolutions Passed by the International Organisation of Securities Commissions)
• http://www.iosco.org/docs (Principles for the Supervision of Operators of Collective Investment Schemes (September, 1997))

Organization of American States—CICAD

• http://www.oas.org/ (Main page)
• http://www.cicad.oas.org/Desarrollo_luridico/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 States)
• http://www.incb.org/e/conv11988/ (United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention))

Annex 1-6
Annex I: Websites for Key Organizations, Legal Instruments, and Initiatives

- http://www.un.org/terrorism/ (UN Action against Terrorism)
- http://www.un.org/sc/ctc (Counter-Terrorism Committee)

United Nations–International Money Laundering Information Network

- http://www.imolin.org/ (Main page)
- 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)
Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

**United Nations–Security Council Resolutions**


**Wolfsberg Group of Banks**


**The World Bank Group**


Annex I-8
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/

Annex II-1
Interpol

- http://www.interpol.com/Public/Terrorism/default.asp (Interpol's involvement in the fight against international terrorism)

The Money Laundering Compliance Website

- http://www.countermoneylaundering.com/

Organization of Economic Cooperation and Development

- http://www.oecd.org/ (Home page)

U.S. Department of the Treasury, Comptroller of the Currency Administrator of National Banks


US State Department–Country Summaries


The World Customs Organization

- http://www.wcoomd.org/e/index.html (Main page)

Annex II-2
Resources

Annex III

List of United Nations Anti-Terrorist Conventions


Annex III-1


Annex IV

The Forty Recommendations on Money Laundering and Interpretive Notes

The Forty Recommendations on Money Laundering

General Framework of the Recommendations

• Recommendation 1
  Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention)

• Recommendation 2
  Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

• Recommendation 3
  An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money

Annex IV-1
laundering investigations and prosecutions and extradition in money laundering cases, where possible.

Role of National Legal Systems in Combating Money Laundering

**SCOPE OF THE CRIMINAL OFFENCE OF MONEY LAUNDERING**

- **Recommendation 4**
  Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalise money laundering as set forth in the Vienna Convention. Each country should extend the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences. (See Interpretative Note.)

- **Recommendation 5**
  As provided in the Vienna Convention, the offence of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

- **Recommendation 6**
  Where possible, corporations themselves—not only their employees—should be subject to criminal liability.

**PROVISIONAL MEASURES AND CONFISCATION**

- **Recommendation 7**
  Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offence, or property of corresponding value, without prejudicing the rights of *bona fide* third parties.
Such measures should include the authority to: 1) identify, trace and evaluate property which is subject to confiscation; 2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and 3) take any appropriate investigative measures.

In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

Role of the Financial System in Combating Money Laundering

**Recommendation 8**
Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively. (See Interpretative Notes: Recommendation 8 and Recommendations 8 and 9.)

**Recommendation 9**
The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis. (See Interpretative Note.)
CUSTOMER IDENTIFICATION AND RECORD-KEEPING RULES

• Recommendation 10
Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

i. to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

ii. to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

• Recommendation 11
Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located). (See Interpretative Notes: Recommendation 11 and Recommendations 11 and 15 through 18.)
• **Recommendation 12**
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 behaviour.

Financial institutions should keep records on customer identification (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 account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

• **Recommendation 13**
Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

**Increased Diligence of Financial Institutions**

• **Recommendation 14**
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 supervisors, auditors and law enforcement agencies. (See Interpretative Note.)

• **Recommendation 15**
If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities. (See Interpretative Notes: Recommendation 15 and Recommendations 11 & 15 through 18.)
**Recommendation 16**
Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or 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 competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. (See Interpretative Note.)

**Recommendation 17**
Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities. (See Interpretative Note.)

**Recommendation 18**
Financial institutions reporting their suspicions should comply with instructions from the competent authorities. (See Interpretative Note.)

**Recommendation 19**
Financial institutions should develop programs against money laundering. These programs should include, as a minimum:

- the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;
- an ongoing employee training programme;
- an audit function to test the system.

**Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures**

**Recommendation 20**
Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, espe-
cially in countries which do not or insufficiently apply these 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 mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

**Recommendation 21**
Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these 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 supervisors, auditors and law enforcement agencies.

**Other Measures to Avoid Money Laundering**

**Recommendation 22**
Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements. (See Interpretative Note.)

**Recommendation 23**
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 cases, subject to strict safeguards to ensure proper use of the information.

**Recommendation 24**
Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book
entry recording of securities, as a means to encourage the replacement of cash transfers.

• **Recommendation 25**
  Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

**IMPLEMENTATION AND ROLE OF REGULATORY AND OTHER ADMINISTRATIVE AUTHORITIES**

• **Recommendation 26**
  The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions. (See Interpretative Note.)

• **Recommendation 27**
  Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

• **Recommendation 28**
  The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

• **Recommendation 29**
  The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates. (See Interpretative Note.)
Strengthening of International Cooperation

ADMINISTRATIVE CO-OPERATION

EXCHANGE OF GENERAL INFORMATION

• **Recommendation 30**
  National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

• **Recommendation 31**
  International competent authorities, perhaps Interpol and the World Customs Organisation, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

EXCHANGE OF INFORMATION RELATING TO SUSPICIOUS TRANSACTIONS

• **Recommendation 32**
  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. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.
OTHER FORMS OF CO-OPERATION

BASIS AND MEANS FOR CO-OPERATION IN CONFISCATION, MUTUAL ASSISTANCE AND EXTRADITION

• **Recommendation 33**
Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions—i.e. different standards concerning the intentional element of the infraction—do not affect the ability or willingness of countries to provide each other with mutual legal assistance. (See Interpretative Note.)

• **Recommendation 34**
International co-operation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

• **Recommendation 35**
Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

FOCUS OF IMPROVED MUTUAL ASSISTANCE ON MONEY LAUNDERING ISSUES

• **Recommendation 36**
Co-operative investigations among countries’ appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible. (See Interpretative Note.)

• **Recommendation 37**
There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by
financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

- **Recommendation 38**
  There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets. (See Interpretative Note.)

- **Recommendation 39**
  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. Similarly, there should be arrangements for coordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

- **Recommendation 40**
  Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offence or related offences. With respect to its national legal system, each country should recognise money laundering as an extraditable offence. 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 arrests or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.
ANNEX TO RECOMMENDATION 9: LIST OF FINANCIAL ACTIVITIES undertaken by business or professions which are not financial institutions

- Acceptance of deposits and other repayable funds from the public.
- Lending
- Financial leasing.
- Money transmission services.
- Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts...)
- Financial guarantees and commitments.
- Trading for account of customers (spot, forward, swaps, futures, options...) in:
  - money market instruments (cheques, bills, CDs, etc.);
  - foreign exchange;
  - exchange, interest rate and index instruments;
  - transferable securities;
  - commodity futures trading.
- Participation in securities issues and the provision of financial services related to such issues.
- Individual and collective portfolio management.
- Safekeeping and administration of cash or liquid securities on behalf of clients.
- Life insurance and other investment related insurance.
- Money changing.

Interpretative Notes to The Forty Recommendations

Interpretative Note to Recommendation 4

Countries should consider introducing an offence of money laundering based on all serious offences and/or on all offences that generate a significant amount of proceeds.

1. Including *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).
Interpretative Note to Recommendation 8

The FATF Recommendations should be applied in particular to life insurance and other investment products offered by insurance companies, whereas Recommendation 29 applies to the whole of the insurance sector.

Interpretative Note to Recommendations 8 and 9 (Bureaux de Change)

INTRODUCTION

Bureaux de change are an important link in the money laundering chain since it is difficult to trace the origin of the money once it has been exchanged. Typologies exercises conducted by the FATF have indicated increasing use of bureaux de change in laundering operations. Hence it is important that there should be effective counter-measures in this area. This Interpretative Note clarifies the application of FATF Recommendations concerning the financial sector in relation to bureaux de change and, where appropriate, sets out options for their implementation.

DEFINITION OF BUREAUX DE CHANGE

For the purpose of this Note, bureaux de change are defined as institutions which carry out retail foreign exchange operations (in cash, by cheque or credit card). Money changing operations which are conducted only as an ancillary to the main activity of a business have already been covered in Recommendation 9. Such operations are therefore excluded from the scope of this Note.

NECESSARY COUNTER-MEASURES APPLICABLE TO BUREAUX DE CHANGE

To counter the use of bureaux de change for money laundering purposes, the relevant authorities should take measures to know the existence of all natural and legal persons who, in a professional capacity, perform foreign exchange transactions.
As a minimum requirement, FATF members should have an effective system whereby the bureaux de change are known or declared to the relevant authorities (whether regulatory or law enforcement). One method by which this could be achieved would be a requirement on bureaux de change to submit to a designated authority, a simple declaration containing adequate information on the institution itself and its management. The authority could either issue a receipt or give a tacit authorisation; failure to voice an objection being considered as approval.

FATF members could also consider the introduction of a formal authorisation procedure. Those wishing to establish bureaux de change would have to submit an application to a designated authority empowered to grant authorisation on a case-by-case basis. The request for authorisation would need to contain such information as laid down by the authorities but should at least provide details of the applicant institution and its management. Authorisation would be granted, subject to the bureau de change meeting the specified conditions relating to its management and the shareholders, including the application of a “fit and proper test.”

Another option which could be considered would be a combination of declaration and authorisation procedures. Bureaux de change would have to notify their existence to a designated authority but would not need to be authorised before they could start business. It would be open to the authority to apply a ‘fit and proper’ test to the management of bureaux de change after the bureau had commenced its activity, and to prohibit the bureau de change from continuing its business, if appropriate.

Where bureaux are required to submit a declaration of activity or an application for registration, the designated authority (which could be either a public body or a self-regulatory organisation) could be empowered to publish the list of registered bureaux de change. As a minimum, it should maintain a (computerised) file of bureaux de change. There should also be powers to take action against bureaux de change conducting business without having made a declaration of activity or having been registered.

As envisaged under FATF Recommendations 8 and 9, *bureaux de change should be subject to the same anti-money laundering regulations as any other financial institution*. The FATF Recommendations on financial matters should therefore be applied to bureaux de change. Of particular importance are those on identification requirements, suspicious transactions reporting, due diligence and record-keeping.
To ensure effective implementation of anti-money laundering requirements by bureaux de change, *compliance monitoring mechanisms should be established and maintained*. Where there is a registration authority for bureaux de change or a body which receives declarations of activity by bureaux de change, it could carry out this function. But the monitoring could also be done by other designated authorities (whether directly or through the agency of third parties such as private audit firms). Appropriate steps would need to be taken against bureaux de change which failed to comply with the anti-laundering requirements.

The bureaux de change sector tends to be an unstructured one without (unlike banks) national representative bodies which can act as a channel of communication with the authorities. Hence it is important that *FATF members should establish effective means to ensure that bureaux de change are aware of their anti-money laundering responsibilities and to relay information, such as guidelines on suspicious transactions, to the profession. In this respect it would be useful to encourage the development of professional associations.*

**Interpretative Note to Recommendations 11, 15 through 18**

Whenever it is necessary in order to know the true identity of the customer and to ensure that legal entities cannot be used by natural persons as a method of operating in reality anonymous accounts, financial institutions should, if the information is not otherwise available through public registers or other reliable sources, request information—and update that information—from the customer concerning principal owners and beneficiaries. If the customer does not have such information, the financial institution should request information from the customer on whoever has actual control.

If adequate information is not obtainable, financial institutions should give special attention to business relations and transactions with the customer.

If, based on information supplied from the customer or from other sources, the financial institution has reason to believe that the customer’s account is being utilised in money laundering transactions, the financial institution must comply with the relevant legislation, regulations, directives or agreements concerning reporting of suspicious transactions or termination of business with such customers.
Interpretative Note to Recommendation 11
A bank or other financial institution should know the identity of its own customers, even if these are represented by lawyers, in order to detect and prevent suspicious transactions as well as to enable it to comply swiftly to information or seizure requests by the competent authorities. Accordingly Recommendation 11 also applies to the situation where an attorney is acting as an intermediary for financial services.

Interpretative Note to Recommendation 14

a. In the interpretation of this requirement, special attention is required not only to transactions between financial institutions and their clients, but also to transactions and/or shipments especially of currency and equivalent instruments between financial institutions themselves or even to transactions within financial groups. As the wording of Recommendation 14 suggests that indeed “all” transactions are covered, it must be read to incorporate these interbank transactions.

b. The word “transactions” should be understood to refer to the insurance product itself, the premium payment and the benefits.

Interpretative Note to Recommendation 15

In implementing Recommendation 15, 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.

2. The FATF adopted this Interpretative Note on 2 July 1999.
Interpretative Note to Recommendation 22

a. To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, members could consider the feasibility of subjecting all cross-border transfers above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

b. If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

Interpretative Note to Recommendation 26

In respect of this requirement, it should be noted that it would be useful to actively detect money laundering if the competent authorities make relevant statistical information available to the investigative authorities, especially if this information contains specific indicators of money laundering activity. For instance, if the competent authorities’ statistics show an imbalance between the development of the financial services industry in a certain geographical area within a country and the development of the local economy, this imbalance might be indicative of money laundering activity in the region. Another example would be manifest changes in domestic currency flows without an apparent legitimate economic cause. However, prudent analysis of these statistical data is warranted, especially as there is not necessarily a direct relationship between financial flows and economic activity (e.g. the financial flows in an international financial centre with a high proportion of investment management services provided for foreign customers or a large inter-bank market not linked with local economic activity).
Interpretative Note to Recommendation 29

Recommendation 29 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.

Interpretative Note to Recommendation 33

Subject to principles of domestic law, countries should endeavour to ensure that differences in the national definitions of the money laundering offences—e.g., different standards concerning the intentional element of the infraction, differences in the predicate offences, differences with regard to charging the perpetrator of the underlying offence with money laundering—do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

Interpretative Note to Recommendation 36 (Controlled delivery)

The controlled delivery of funds known or suspected to be the proceeds of crime is a valid and effective law enforcement technique for obtaining information and evidence in particular on international money laundering operations. In certain countries, controlled delivery techniques may also include the monitoring of funds. It can be of great value in pursuing particular criminal investigations and can also help in obtaining more general intelligence on money laundering activities. The use of these techniques should be strongly encouraged. The appropriate steps should therefore be taken so that no obstacles exist in legal systems preventing the use of controlled delivery techniques, subject to any legal requisites, including judicial authorisation for the conduct of such operations. The FATF welcomes and supports the undertak-
ings by the World Customs Organisation and Interpol to encourage their members to take all appropriate steps to further the use of these techniques.

**Interpretative Note to Recommendation 38**

a. Each country shall consider, when possible, 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. Each country should consider, when possible, 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.

**Interpretative Note on Deferred Arrest and Seizure**

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.
Annex V

Eight Special Recommendations on Terrorist Financing

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 organisations 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.
VI. Alternative remittance

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.
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.
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 coun-

Annex VI-2
tries 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 . 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 effective date of the Convention is 10 April 2002. The web page containing information on the status of the Convention is located on the UN website at http://untreaty.un.org/ENGLISH/status/Chapter_xviii/treaty11.asp. For general information about UN treaties, see http://untreaty.un.org/english/guide.asp and the Treaty Handbook of the UN Office of Legal Affairs at http://untreaty.un.org/English/TreatyHandbook/hbframeset.htm. The texts of the relevant UN Security Council Resolutions may be consulted on the UN website at http://www.un.org/documents/scres.htm.

**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
Annex VI: Guidance Notes for the Special Recommendations on Terrorist Financing

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 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

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;
Annex VI: Guidance Notes for the Special Recommendations on Terrorist Financing

- 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 purposes 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.

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 organisations 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.

---

_FATF Secretariat_  
27 March 2002
### Annex VII

**Cross-Reference of The Forty Recommendations to Reference Guide**

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Reference Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chapter I, footnote 8</td>
</tr>
<tr>
<td></td>
<td>Chapter V, footnote 3</td>
</tr>
<tr>
<td>2</td>
<td>Chapter V, footnote 45</td>
</tr>
<tr>
<td></td>
<td>Chapter VI, footnotes 54, 55</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnotes 7, 8, 11</td>
</tr>
<tr>
<td>3</td>
<td>Chapter VIII, footnotes 3, 9, 11, 15, 24</td>
</tr>
<tr>
<td>4</td>
<td>Chapter I, footnote 9</td>
</tr>
<tr>
<td></td>
<td>Chapter V, footnotes 8, 14</td>
</tr>
<tr>
<td></td>
<td>Chapter VIII, footnote 7</td>
</tr>
</tbody>
</table>

Annex VII-1
<table>
<thead>
<tr>
<th>Page</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Chapter V, footnote 30</td>
</tr>
<tr>
<td>6</td>
<td>Chapter V, footnote 31</td>
</tr>
<tr>
<td>7</td>
<td>Chapter V, footnotes 41, 43, 46, 47, 48</td>
</tr>
</tbody>
</table>
| 8    | Chapter V, footnote 55  
|      | Chapter IX, footnote 44 |
| 9    | Chapter V, footnote 55  
|      | Chapter VI, footnote 28 |
| 10   | Chapter VI, footnotes 15, 18  
|      | Chapter IX, footnote 48 |
| 11   | Chapter VI, footnote 17  
|      | Chapter VII, footnote 2  
|      | Chapter IX, footnote 48 |
| 12   | Chapter VI, footnotes 40, 41, 42  
|      | Chapter VII, footnotes 2, 3  
|      | Chapter IX, footnote 48 |
| 13   | Chapter VI, footnote 28  
|      | Chapter VII, footnote 2 |
| 14   | Chapter VI, footnotes 20, 28, 36  
|      | Chapter VII, footnote 2 |
| 15   | Chapter VII, footnote 2  
|      | Chapter IX, footnotes 30, 48 |
| 16   | Chapter VI, footnote 38  
|      | Chapter VII, footnote 2 |

Annex VII-2
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Chapter VI, footnote 34</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>18</td>
<td>Chapter VI, footnote 35</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>19</td>
<td>Chapter VI, footnotes 56, 57, 58</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>20</td>
<td>Chapter VI, footnotes 6, 7</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>21</td>
<td>Chapter III, footnotes 28, 31</td>
</tr>
<tr>
<td></td>
<td>Chapter VI, footnote 28</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>22</td>
<td>Chapter VI, footnote 52</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>23</td>
<td>Chapter VI, footnote 49</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>24</td>
<td>Chapter VI, footnote 53</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>25</td>
<td>Chapter V, footnote 59</td>
</tr>
<tr>
<td></td>
<td>Chapter VII, footnote 2</td>
</tr>
<tr>
<td>26</td>
<td>Chapter VI, footnotes 56, 57, 58</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnote 50</td>
</tr>
<tr>
<td>27</td>
<td>Chapter V, footnotes 57, 58</td>
</tr>
<tr>
<td>28</td>
<td>Chapter VI, footnote 37</td>
</tr>
<tr>
<td>29</td>
<td>Chapter V, footnotes 59, 60</td>
</tr>
</tbody>
</table>
As a practical matter, FATF members do not implement this recommendation; nor is it part of the assessment Methodology. This recommendation is currently under review by FATF.
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Reference Guide</th>
</tr>
</thead>
</table>
| I              | Chapter I, footnote 13  
Chapter VIII, footnote 7  
Chapter IX, footnotes 5, 16 |
| II             | Chapter I, footnotes 14, 15  
Chapter V, footnote 20  
Chapter IX, footnote 18 |
| III            | Chapter IX, footnotes 21, 22 |
| IV             | Chapter VI, footnote 28  
Chapter IX, footnote 26 |

Annex VIII-1
<table>
<thead>
<tr>
<th>V</th>
<th>Chapter IX, footnotes 32, 33</th>
</tr>
</thead>
<tbody>
<tr>
<td>VI</td>
<td>Chapter I, footnote 18</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnotes 42, 43</td>
</tr>
<tr>
<td></td>
<td>Chapter X, footnote 11</td>
</tr>
<tr>
<td>VII</td>
<td>Chapter VI, footnotes 19, 28</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnotes 51, 52</td>
</tr>
<tr>
<td>VIII</td>
<td>Chapter I, footnote 17</td>
</tr>
<tr>
<td></td>
<td>Chapter IX, footnotes 57, 58</td>
</tr>
<tr>
<td>1.</td>
<td>2.</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Cambodia  
2. Bangladesh  
3. Singapore  
4. Chile  
5. New Zealand  
6. India  
7. Norway  
8. Tanzania  
9. Costa Rica  
10. Turkey  
11. Sri Lanka  
12. Ecuador  
13. Austria  
14. South Africa  
15. Zambia  
16. Thailand  
17. Brazil  
18. Timor and Timor  
19. United States  
20. Malawi  
21. Ethiopia  
22. Republic of Kenya  
23. Czech Republic  
24. Dominican Republic  
25. SQUAS  
26. European Union  
27. Euphrates  
28. Baghdad  
29. Roland  
30. Japan

Design and layout by James Quigley
Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism

work in progress for public discussion