

Combating Money Laundering and the Financing of Terrorism

A Comprehensive Training Guide



Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized



Combating Money Laundering and the Financing of Terrorism

A Comprehensive Training Guide

Workbook 1. Effect on Economic Development and International Standards	3
Workbook 2. Legal Requirements to Meet International Standards	71
Workbook 3a. Regulatory and Institutional Requirements for AML/CFT	151
Workbook 3b. Compliance Requirements for Financial Institutions	255
Workbook 4. Building an Effective Financial Intelligence Unit	347
Workbook 5. Domestic (Inter-Agency) and International Cooperation	439
Workbook 6. Combating the Financing of Terrorism	503
Workbook 7. Investigating Money Laundering and Terrorist Financing	605

6

Combating the Financing of Terrorism

Workbook



6

Combating the Financing of Terrorism

Workbook



THE WORLD BANK
Washington, D.C.

© 2009 The International Bank for Reconstruction and Development / The World Bank
1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org
E-mail: feedback@worldbank.org

All rights reserved

1 2 3 4 12 11 10 09

This volume is a product of the staff of the International Bank for Reconstruction and Development / The World Bank. The findings, interpretations, and conclusions expressed in this volume do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent.

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

Rights and Permissions

The material in this publication is copyrighted. Copying and/or transmitting portions or all of this work without permission may be a violation of applicable law. The International Bank for Reconstruction and Development / The World Bank encourages dissemination of its work and will normally grant permission to reproduce portions of the work promptly.

For permission to photocopy or reprint any part of this work, please send a request with complete information to the Copyright Clearance Center Inc., 222 Rosewood Drive, Danvers, MA 01923, USA; telephone: 978-750-8400; fax: 978-750-4470; Internet: www.copyright.com.

All other queries on rights and licenses, including subsidiary rights, should be addressed to the Office of the Publisher, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2422; e-mail: pubrights@worldbank.org.

ISBN: 978-0-8213-7569-3
eISBN: 978-0-8213-7570-9
DOI: 10.1596/978-0-8213-7569-3

Library of Congress Cataloging-in-Publication Data

Combating money laundering and the financing of terrorism : a comprehensive training guide.
p. cm.

“A World Bank and International Monetary Fund publication.”

Includes bibliographical references.

ISBN 978-0-8213-7569-3 -- ISBN 978-0-8213-7570-9 (electronic)

1. Money laundering. 2. Terrorism--Finance. 3. Terrorism--Prevention. I. World Bank.

II. International Monetary Fund.

HV8079.M64C56 2009

332.1068'4--dc22

2009009952



About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti-Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS

Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS

Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT

Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS

Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.

MODULE 4: BUILDING AN EFFECTIVE FINANCIAL INTELLIGENCE UNIT

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

MODULE 5: DOMESTIC (INTERAGENCY) AND INTERNATIONAL COOPERATION

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

MODULE 6: COMBATING THE FINANCING OF TERRORISM

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

MODULE 7: INVESTIGATING MONEY LAUNDERING AND TERRORIST FINANCING

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

The initial work for this training program was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 3a was further written and developed by Manuel Vasquez, International Monetary Fund. The draft was reviewed by John McDowell, the World Bank and Thomas Grahn, Financial Supervisory Authority of Sweden. Pedagogical guidance was provided by Sheila Jagannathan, and peer review was conducted by Emiko Todoroki, the World Bank. In 2007 and 2008, updates and review were provided by Klaudio Stroligo, Cedric Mousset, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations” (2003) and “Special Recommendations on Terrorist Financing” (2005); and Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second Edition*, the World Bank, 2004.

CAPACITY ENHANCEMENT PROGRAM ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

Program Director: Latifah Merican Cheong

Task Team Leader: Emiko Todoroki

Instructional Design: Sheila Jagannathan

Production: Miguel Nicolas De La Riva, Jr.

Illustrations: James Quigley

Design: Naylor Design, Washington, D.C.

Composition: Precision Graphics, Champaign, Illinois

Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The module starts with a brief review of the CFT issues raised in the previous modules, addresses some general questions related to CFT, and then discusses the Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing in combination with the international obligations of states. The Module covers the following issues:

- 1. What does terrorist financing mean? 4**
- 2. International norms and standards on CFT 8**
 - 2.1 The SFT Convention of 1999 8
 - 2.2 Resolutions of the UN Security Council 9
 - 2.3 The Nine FATF Special Recommendations on Terrorist Financing 9
 - 2.4 The UN Comprehensive Convention on International Terrorism 9
 - 2.5 Other international treaties on combating the financing of terrorism 10
 - 2.6 Human rights and financing of terrorism 10
- 3. Is combating terrorist financing mandatory? 11**
 - 3.1 Are UN Security Council Resolutions binding on UN member states? 11
 - 3.2 The FATF Special Recommendations are emerging standards 12
- 4. The targets of international policies on CFT 13**
 - 4.1 Individuals 13
 - 4.2 Groups and organizations 13
 - 4.3 Private sector 14
 - 4.4 States 14
- 5. Ratification and implementation of UN instruments 16**
 - 5.1 What steps should be taken? 16
 - 5.2 What more should be done? 17

6. Offenses to be criminalized	18
6.1 How is the offense of financing of terrorism defined?	18
7. Freezing, seizing, and confiscating terrorist assets	20
7.1 Freezing, seizing, and confiscation: what are the differences?	20
7.2 Taking the measures against terrorists' assets	21
7.3 Setting up the necessary national legal framework	22
7.4 Challenges	22
8. Reporting suspicious transactions related to terrorism	24
8.1 Under what circumstances should a transaction be reported?	24
8.2 Challenges	25
8.3 What types of institutions are expected to submit reports?	25
9. Enhancing international cooperation	27
9.1 Mutual legal assistance	27
9.2 Extradition of offenders and other forms of cooperation	28
9.3 Challenges: A good legal framework is meaningless if states are not proactive	28
10. Measures required for alternative remittance systems	30
11. Measures required for wire transfers	33
11.1 What is a wire transfer?	33
11.2 What is the FATF's standard on wire transfers?	34
11.3 Who is covered by the wire transfer standard?	34
12. Dealing with cash couriers	36
12.1 Why monitor cross-border transportation of cash?	36
12.2 What is targeted?	36
12.3 What sort of action is required?	37
12.4 Implementation of sanctions	38
12.5 Challenges to the implementation of FATF Special Recommendation IX	38
13. Supervising nonprofit organizations and other legal entities	40
13.1 What entities should be under scrutiny?	40
13.2 What kind of oversight is needed? By whom?	41

This module introduces

- the nine FATF Special Recommendations on Terrorist Financing.
- relevant resolutions of the United Nations Security Council (UNSC).
- the UN Convention for the Suppression of the Financing of Terrorism.

At the end of the module, you will be able to

- explain what countries must do to prevent, detect, and prosecute the financing of terrorism and terrorist acts;
- understand the rationale for combating the financing of terrorism;
- name the international conventions and resolutions that should be ratified and implemented;
- list the type of offenses that should be criminalized;
- clarify the meaning of freezing and confiscating terrorist assets;
- explain when to file suspicious transaction reports (STRs) related to the financing of terrorism;
- describe alternative remittance systems, wire transfers, cash couriers, and measures to prevent the financing of terrorism through such means; and
- discuss the relationship of nonprofit organizations to the financing of terrorism.

1

What does terrorist financing mean?

How much do you know?

Let us review what we discussed on the financing of terrorism in the previous modules. Please answer the following questions, using the space below each to jot down your thoughts if necessary.

QUESTION 1. What is the financing of terrorism?

QUESTION 2. What is the main difference between money laundering and terrorist financing? Select one.

- a) They are the same.
- b) Money laundering is done by criminals and noncriminals, whereas terrorist financing is done by terrorists only.
- c) Money laundering involves only ill-gotten money, whereas terrorist financing involves both ill-gotten money and legitimate money.

QUESTION 3. What are the implications of terrorist financing for developing economies?

QUESTION 4. What are the signs of a weak AML/CFT regime? Mark all that you believe apply.

- a) Limited legal scope of the criminal offenses often connected with money laundering and terrorist financing
- b) Difficult confiscation provisions
- c) Banks subject to AML/CFT compliance but not non-financial institutions
- d) Limited communication and coordination across countries

The importance of combating terrorist financing has grown apace with the incidence of terrorism around the world. Although the measures used to prevent terrorist financing are quite similar to those used to counter money laundering, keep in mind that terrorist financing may originate from a legal source. As explained in Module 1, the source of terrorist financing may be legitimate or illegitimate, whereas the source of laundered money is always criminal.

To combat terrorist financing, the FATF adopted eight Special Recommendations on Terrorist Financing in 2001. In 2004, the FATF adopted a ninth Special Recommendation. Together, they are the international standards in combating terrorist financing. Their objectives are to prevent, detect, and prosecute terrorists and their supporters.

Analysis

To understand the meaning of “terrorist financing,” let us analyze a simple case:

Valachia is a province of Rurithania. A group calling itself the Liberation Front of Valachia is fighting for independence. For many years, the group has bombed police stations and infrastructure. Free Valachia, a political party active in the province, also favors independence. It has condemned the police measures that the Rurithanian government has taken against members of the Liberation Front of Valachia. The government of Rurithania is considering sharing with foreign countries the names of members and representatives of both groups. Its goal is to seize their assets on the grounds that the Free Valachia party is supporting the Liberation Front of Valachia. To what extent could international norms on terrorist financing apply to such a situation?

To answer that question, one must understand what **terrorism** means.

Terrorist financing, you will recall, is providing financial support for terrorism or for those who encourage, plan, or engage in terrorism. Although that appears at first glance to be a very simple concept, the case of Valachia shows how complex the issues may be. Most of the difficulty lies in reaching agreement on what constitutes terrorism.

The financing of terrorism is defined by the UN Convention for the Suppression of the Financing of Terrorism (SFT Convention, 1999).

Financing of terrorism occurs when a person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that these should be used or in the knowledge that these will be used in full or in part, to carry out a terrorist act as defined in the above-mentioned convention.

But where can we find a definition of terrorism (as distinct from terrorist acts)?

- Not in the SFT Convention.
- Not in the UNSC resolutions on terrorism.
- Not in the UN's comprehensive convention on terrorism—because the negotiations on the draft convention have stalled on precisely this question.

Terrorist acts, by contrast, are well defined:

- The SFT Convention defines a terrorist act as an “act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.”

Keep in mind that specific international conventions deal with particular types of terrorist activities. The SFT Convention includes the offenses set forth in nine treaties among the crimes that must be considered as acts of terrorism.

The Annex to the SFT Convention sets out the list of the nine international treaties that pertain to terrorist crimes, as follows:

- 1) Convention for the Suppression of Unlawful Seizure of Aircraft, at The Hague on December 16, 1970
- 2) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, in Montreal on September 23, 1971
- 3) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the UN on December 14, 1973

- 4) International Convention against the Taking of Hostages, adopted by the General Assembly of the UN on December 17, 1979
- 5) Convention on the Physical Protection of Nuclear Material, adopted in Vienna on March 3, 1980
- 6) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, in Montreal on February 24, 1988
- 7) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, in Rome on March 10, 1988
- 8) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, in Rome on March 10, 1988
- 9) International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the UN on December 15, 1997

 **Knowledge check**

QUESTION 5. Is it legitimate to finance terrorist acts if the financier’s motives are political or religious?

- a) True b) False

QUESTION 6. Are political actions such as strikes and peaceful demonstration acts of terrorism?

- a) True b) False

QUESTION 7. Are the actions of people against foreign occupation considered acts of terrorism?

QUESTION 8. Now back to the question posed in the introductory story. Do international standards on the financing of terrorism apply to the situation in Valachia? Think about your solution and then look for the answer.

2

International norms and standards on CFT

Is international cooperation against terrorism:

- a) A new issue,
- b) A very old issue, or
- c) An issue since the terrorist attacks of September 11, 2001?

The answer is b. Terrorism is a very old phenomenon, but international cooperation against terrorism began only in the 1970s. Since then, international treaties have addressed specific types of terrorist threats, such as the unlawful seizure of aircraft. For more information, see the list of treaties. In addition, in the past 10 years, the UN has intensified its efforts to combat terrorism. The SFT Convention was negotiated in the UN General Assembly and adopted in 1999. In the UNSC, the system of sanctions adopted against the Taliban in 1999 was a turning point. The terrorist attacks of September 11 triggered a qualitative jump in the scope and specificity of the measures that states must take to combat terrorism.

2.1 The SFT Convention of 1999

The SFT Convention had been ratified by just a few states before September 11, 2001. After September 11, member states were pressed to ratify the convention by UNSC Resolution 1373 (2001) and the FATF Special Recommendations. As of March 2007, with 156 parties, the convention is the most comprehensive international instrument for combating the financing of terrorism.

States that ratify this convention must:

- Establish in their criminal legislation the offense of financing terrorism
- Cooperate with other state parties and provide them with legal assistance
- Enact legislation concerning the role of financial institutions in the detection and reporting of evidence of terrorist financing
- Take appropriate measures for the identification, detection, and freezing or seizure of any funds used or allocated for the purpose of committing the financing of terrorism criminal offense as well as the proceeds derived from such offense, for purposes of possible confiscation.

2.2 Resolutions of the UN Security Council

The UNSC has been a driving force in combating the financing of terrorism. It has adopted two major resolutions.

- 1) Resolution 1267 (1999) (as modified and adapted by resolutions 1333 (2000), 1390 (2002), 1452 (2002), 1455 (2003), and 1526 (2004))

What is the objective of Resolution 1267?

Resolution 1267 targets specific individuals, entities, or groups—among them Osama bin Laden, Al-Qaeda, and the Taliban—for the purpose of restoring peace and suppressing threats to international security. With respect to the financing of terrorism, its major application is to freeze the assets of the named individuals and entities. The legal regime set up by resolution 1267 (1999), and modified by the resolutions 1333 (2000) and 1390 (2002), has been adapted to new resolutions.

- 2) Resolution 1373 (2001)

What is the objective of Resolution 1373?

Resolution 1373 targets international terrorism in general. It was adopted after the attacks of September 11, 2001, but it is not aimed at identifying or punishing the perpetrators of the attacks. Instead, the resolution provides a set of measures (including the freezing of terrorist assets) aimed at combating terrorism and its financing. A Counter-Terrorism Committee set up under the resolution is responsible for monitoring its implementation by the members of the UN.

2.3 The Nine FATF Special Recommendations on Terrorist Financing

The FATF Special Recommendations were an immediate response to the events of September 11, 2001. Adopted in October 2001 and October 2004, they extend the FATF Forty Recommendations on money laundering to cover the particularities of terrorist financing. They also cover certain issues in greater detail than do the SFT Convention and UNSC Resolution 1373 (2001). The Special Recommendations also introduce new issues.

2.4 The UN Comprehensive Convention on International Terrorism

In 2002, the UN General Assembly began work on a comprehensive convention on international terrorism. When adopted, the convention will complement existing treaties by providing a universal convention that addresses globally the problems of terrorism. As noted above, negotiators are having trouble with the definition of terrorism and the scope of the convention.

2.5 Other international treaties on combating the financing of terrorism

Because combating the financing of terrorism is part of a broad international effort, other international instruments also can be used in this fight. Those instruments include the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988), the UN Convention against Transnational Organized Crime (the Palermo Convention, 2000), and the UN Convention against Corruption (the Merida Convention, 2003). At the regional level, one might cite the following Council of Europe conventions: the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime (the Strasbourg Convention, 1990); the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the Warsaw Convention, 2005); and the European Convention on the Suppression of Terrorism (1977) with the Amending Protocol (2003).

Examples of the possible connection between terrorism and other types of criminal activities

Italy

In April 2004, a top Italian anti-Mafia prosecutor announced evidence of links between the Italian Mafia and Muslim terrorist groups in Italy. According to the statement, the two groups had forged links in arms and drug trafficking.

United States

Criminal investigations into cigarette smuggling (leading so far to one conviction in North Carolina in 2002) revealed that cigarette trafficking may be used by terrorists to raise funds for terrorist organizations overseas. (Source: Bedi Rohand. *Money Laundering Controls and Prevention*. London: ISI Publications (2004): 321.)

2.6 Human rights and financing of terrorism

States' obligations to combat the financing of terrorism do not override their other international obligations, especially the observance of human rights. In other words, the necessity to combat terrorism efficiently cannot be used as justification for not applying human rights standards. The UNSC has recently affirmed this principle (see paragraph 6 of UNSC Resolution 1456).¹ With respect to the fight against terrorist financing, this means that countries must respect human rights and due process when designing and implementing procedures for freezing, seizing, and confiscating terrorists' assets.

¹ Paragraph 6 of UN Security Council Resolution 1456 (2003) states, "States must ensure that any measures taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee, and humanitarian law." For more information on this issue see the Council of Europe's "Guidelines on Human Rights and the Fight against Terrorism."

3

Is combating terrorist financing mandatory?

States are bound by international law to put in place certain policies and to ensure that their legislation complies with international norms and standards. Laws aside, the political cost of not acting against the financing of terrorism is clear. Few countries would wish to become known as havens for financial activities related to terrorism. As we have seen, money launderers are always looking for jurisdictions that are less stringent in their regulation of financial activities. The financiers of terrorism are likely to favor the same jurisdictions.

Concerns

The secretary general of the Pacific Islands Forum expressed his concern about the area becoming a weak link in the fight against terrorism and organized crime unless adequate measures were taken. Small island states are especially vulnerable to abuse because many lack strong uniform laws and have inadequate human, financial, and technical resources.

3.1 Are UN Security Council Resolutions binding on UN member states?

Not all UNSC Resolutions are binding. But when a resolution is adopted on the basis of Chapter VII of the UN Charter—because the situation is deemed a threat to international peace and security—the “decisions” reported in the resolution bind all member states. This is the case for the following resolutions on terrorism: 1267 (1999), 1333 (2000), 1373 (2001), and 1390 (2002). The “recommendations” presented in the same resolutions, however, are nonbinding.

However, states are bound to respect the terms and provisions of the treaties they sign and ratify. States that have ratified the SFT Convention have a legal obligation to incorporate the treaty into their domestic legislation. Those that have signed but not yet ratified the convention have at least a good faith obligation to refrain from taking actions incompatible with the legal framework of the treaty. Note that UNSC Resolution 1373 (2001) and the FATF Special Recommendations call upon the member states to become parties to the SFT Convention.

3.2 The FATF Special Recommendations are emerging standards

The FATF Special Recommendations are not a binding international convention; however, many countries have made a political commitment to combat terrorist financing by implementing the FATF Special Recommendations along with the FATF Forty Recommendations. In addition, the Boards of the World Bank and International Monetary Fund (IMF) have endorsed the FATF Special Recommendations and added the Special Recommendations to the list of standards and codes that are relevant to their operational work. As part of the evaluations conducted by the FATF, FATF-Style Regional Bodies (FSRBs), the World Bank, and the IMF, countries are now assessed on their CFT efforts based on the FATF Special Recommendations.

UN Security Council Resolution 1526 (2004)

Paragraph 4 of UNSC Resolution 1526 (2004) “calls upon States to move vigorously and decisively to cut the flows of funds and other financial assets and economic resources to individuals and entities associated with the Al-Qaeda organization, Osama bin Laden and/or the Taliban, *taking into account, as appropriate, international codes and standards for combating the financing of terrorism, including those designed to prevent the abuse of nonprofit organizations and informal/alternative remittance systems*” (emphasis added).

IS THAT ENOUGH?

The international standards established by the FATF describe minimum standards that states should meet. However, countries need not be satisfied with the minimum. It is important to look at best practices. For instance, in the case of the FATF Special Recommendations, “International Best Practices (SRIII, SRVI, SRVIII, and SRIX)” are providing practical and appropriate ways to implement the standards.

WHAT DID YOU LEARN?

- Combating the financing of terrorism is an inescapable obligation of all states.
- The formal obligations of individual states may vary slightly depending on whether they have ratified the SFT Convention.
- The international standards define the *minimum* acceptable conduct. States can always adopt a stricter regime.

4

The targets of international policies on CFT

Individuals, groups, organizations, and even states may be involved at different stages of terrorist activity. International standards deal with that involvement in different ways.

4.1 Individuals

Certain rules are directed against individuals. The UNSC has expressly mentioned Osama bin Laden as a person targeted by a regime of sanctions. Other individuals, without being named in the resolutions themselves, have been added to the list of persons (individuals or legal entities) targeted by the sanctions committee set up by under the UNSC Resolution 1267 (1999), (hereafter the “1267 Committee”), because of their presumed links with the Al-Qaeda organization or the Taliban. The 1267 Committee, an organ of the UNSC, reviews the list periodically, based on information provided by UN member states.

Individuals: Osama bin Laden

Resolution 1333 (2000) contains the decision “that all States shall [...] freeze without delay funds and other financial assets of Osama bin Laden and individuals and entities associated with him as designated by the Committee, including those in the Al-Qaeda organization, and including funds derived or generated from property owned or controlled directly or indirectly by Osama bin Laden and individuals and entities associated with him, and to ensure that neither they nor any other funds or financial resources are made available, by their nationals or by any persons within their territory, directly or indirectly for the benefit of Osama bin Laden, his associates or any entities owned or controlled, directly or indirectly, by Osama bin Laden or individuals and entities associated with him including the Al-Qaeda organization.” (paragraph 8,c)

4.2 Groups and organizations

Some UNSC resolutions have targeted groups and organizations, such as the Taliban and Al-Qaeda. The 1267 Committee has some 100 groups or entities, such as the Jemaah Islamiyah, connected to Al-Qaeda.

Groups and organizations: Entities belonging to or associated with the Al-Qaeda organization

Entity identifiers	Alias	Address	Listed on	Other information
Name: Jemaah Islamiyah	A.k.a.: a) Jema'ah Islamiyah b) Jemaah Islamiya c) Jemaah Islamiah d) Jamaah Islamiyah e) Jama'ah Islamiyah F.k.a.:	Address:	Oct. 25, 2002	The network in Southeast Asia. Founded by the late Abdullah Sungkar.

Source: United Nations. Consolidated list of the 1267 Committee.

4.3 Private sector

The private sector is not the immediate target of international rules and standards on combating terrorist financing. Bankers and money-transfer operators are called upon to implement policies to combat the financing of terrorism, but because the international standards are not immediately transferable to national systems of regulation and enforcement, individual states must ensure that private sector practice conforms with the goals set by the international standards. In practice, this usually means that states must adopt implementing legislation and regulations to guide enforcement of AML/CFT requirements.

Private sector compliance

FATF Special Recommendation VI states that “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 nonbank financial institutions.” (Emphasis added.)

4.4 States

States are the main target of international rules on combating terrorist financing—as set forth, for example, in the SFT Convention, UNSC resolutions, and the FATF Special Recommendations. Even when rules are directed against individuals or groups, states are bound to take certain actions.

State compliance

Resolution 1373 (2001) provides “that all *States* shall [...] prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens.” (Paragraph 2d, emphasis added.)

What have you learned?

- States are the main target of international rules and standards on combating terrorist financing.
- In the fight against terrorism, specific individuals and entities have been targeted for action at the international level.
- States are obliged to ensure that international standards and treaty obligations are implemented through their national legislation and that the legislation is enforceable and is enforced.

5

Ratification and implementation of UN instruments

Let us analyze a hypothetical scenario to understand these issues.

Case study: Rurithania

For many years, the state of Rurithania has had antiterrorist legislation aimed at combating terrorism at the domestic level. However, it has passed no law regarding international cooperation in the fight against terrorism. The question of preventing the abuse of the financial system by terrorist financiers is ignored in Rurithanian law because it was not an issue at the time the original antiterrorism legislation was adopted. Can Rurithania claim that it is in compliance with its international obligations and that its present legal framework is enough? Does the fact that Al-Qaeda and related organizations are not present in the country provide support for this assertion?

FATF Special Recommendation I requires states to ratify the SFT Convention and to implement relevant UNSC Resolutions on terrorist financing. For more information on FATF Special Recommendation I, see Appendix B.

5.1 What steps should be taken?

Every country should take immediate steps to ratify and implement fully the SFT Convention.

- Ratification means that states take legislative or executive steps to approve the convention.
- Implementation means that states adopt policies and measures, including legislation if needed, to ensure effective implementation of the SFT Convention under the state's national legal system.

States should also take steps to implement UNSC Resolutions relating to the prevention and suppression of terrorist financing. Resolution 1373 (2001) is of primary importance for domestic legislative regimes. But Resolution 1267 (1999) and subsequent related resolutions also are important in defining the legal regime of sanctions against presumed terrorist individuals and entities.

5.2 What more should be done?

The members of the UN also have a duty to collaborate with the Counter-Terrorism Committee and the 1267 Committee:

- By providing feedback on their implementation measures in the form of periodic reports
- By supplying information on suspected terrorists or terrorist entities to be included on the list of the 1267 Committee
- By contributing to the removal of names that should no longer appear on the list.

FATF Recommendation 35 requires that other instruments should be ratified as well—among them the Palermo Convention on organized crime and the Vienna Convention on illicit drug trafficking. Countries should take immediate steps to become party to, and implement fully, the Vienna Convention, the Palermo Convention, and the 1999 UN International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Note that in addition to these conventions, Resolution 1373 (2001) calls upon states to become party to other treaties related to the fight against terrorism.

QUESTION 9. Let us return now to the case on Rurithania. Can Rurithania assert that it has complied with its international obligations and that its existing legal framework is enough? Does the fact that Al-Qaeda and related organizations are not operating in the country support that assertion? Think about your solution, and jot down your answers in the space provided below.

6

Offenses to be criminalized

FATF Special Recommendation II requires that countries criminalize terrorist financing, terrorist acts, and terrorist organizations. It is not sufficient to criminalize money laundering; the financing of terrorism must be criminalized as a separate offense. For more information on FATF Special Recommendation II, see Appendix C.

6.1 How is the offense of financing of terrorism defined?

The offense of financing of terrorism occurs when a “person by any means, directly or indirectly, unlawfully and willfully, 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 terrorist act, by a terrorist organization or an individual. There are two key elements: the mental and material elements.

- The mental element – This means that the act must have been done willfully and intentionally, or with knowledge of the illegal intent of the use of the funds.
- The material element – Broadly defined, this means that there is the fact of providing or collecting funds.

Knowledge check

QUESTION 10. Does the simple fact of collecting funds for use in terrorist activity constitute the criminal offense of terrorist financing?

- a) Yes b) No

QUESTION 11. Is *attempting* to finance terrorism also an offense?

- a) Yes b) No

QUESTION 12. If terrorist financing occurs in a different jurisdiction, can it be prosecuted? Should it be?

- a) Yes b) No

QUESTION 13. What are the appropriate penalties for individuals and entities convicted of financing terrorism?

QUESTION 14. What is the link between the offense of terrorist financing and money laundering?

7

Freezing, seizing, and confiscating terrorist assets

Let us start by determining which of the following figures represent the total amount of terrorist assets blocked in the United States in 2003:

- a) \$8,000,500
- a) \$5,991,931
- b) \$771,956
- c) \$300,589

The answer is b. The assets blocked under three U.S. antiterrorist programs were as follows in 2003:

AL-QAEDA	\$ 771,956
HAMAS	\$ 5,196,634
PALESTINIAN ISLAMIC JIHAD	\$ 17,746
KAHANE CHAI	\$ 201
TALIBAN	\$ 5,394
Total assets	\$ 5,991,931²

A key tenet of the fight against terrorism is that breaking the chain of financing will diminish terrorists' capacities to carry out terrorist acts. If the financing chain is to be broken, countries must be able to take legal steps against the funds on which terrorists and their organizations depend. *Freezing, seizing, and confiscation* are the three major legal tools available for that purpose.

7.1 Freezing, seizing, and confiscation: what are the differences?

- *Freezing* indicates prohibition by a court or other competent authority of the transfer, conversion, disposition, or movement of property. The frozen funds or assets remain the property of the owner and under the administration,

² Source: "Terrorist Assets Report, Calendar Year 2003," Twelfth Annual Report to the Congress on Assets in the United States of Terrorist Countries and International Terrorism Program Designees. <http://www.treasury.gov/offices/eotffc/ofac/reports/tar2003.pdf>. The three U.S. programs are Specially Designated Global Terrorists (SDGTs), Specially Designated Terrorists (SDTs), and Foreign Terrorist Organizations (FTOs).

control, or management of the financial institution that held the funds at the time of freezing.

- *Seizing* means prohibiting the transfer, conversion, disposition, or movement of property, but with the added qualification that the court or other competent authority temporarily assumes custody or control of the property. The assets or funds remain the property of the owner, but possession, administration, and management of the asset is taken over by a relevant competent authority or a court.
- *Confiscation, which includes forfeiture*, means the permanent deprivation of funds or other assets by order of a court or other competent authority, which transfers the ownership of funds or assets from the original owner to the state.

The objectives of these measures differ. The goal of freezing assets is preventive—to deprive the owner of control over the assets to prevent them from being spent or dispersed. Seizing and confiscation have both a preventive and a punitive objective: to deter future criminal acts by seizing property, temporarily or permanently.

7.2 Taking the measures against terrorists' assets

Freezing, seizing, and confiscation are dealt with in slightly different ways in the SFT Convention, the UNSC Resolutions, and the Special Recommendations. FATF Special Recommendation III states that each country should immediately implement measures to freeze funds or other assets belonging to terrorists, those who finance terrorism, and terrorist organizations, in accordance with UN resolutions relating to the prevention and suppression of the financing of terrorist acts. In addition, the FATF recommends the adoption and implementation of measures for the seizure and confiscation of assets. For more information on FATF Special Recommendation III, see Appendix D.

The UNSC Resolutions impose on states an obligation to freeze terrorists' assets. Resolution 1267 (1999) ordered the freezing of the assets of specific individuals and entities, whereas Resolution 1373 (2001) put in place a general obligation of states to freeze terrorist assets and left to each country the choice of the means to be used for that purpose. States may have national lists of terrorists and terrorist entities.

Resolution 1373 and specially designated nationals

Resolution 1373

Resolution 1373 (2001) calls for states to “freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting

on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities.”

Specially designated nationals

In the United States, the Office of Foreign Assets Control (Treasury Department) maintains a list of “specially designated nationals” whose properties can be blocked. The member states of the European Union maintain a uniform system of lists.

The SFT Convention is the most comprehensive of all the instruments under discussion. It requires not only the freezing, seizing, and confiscation of the assets of terrorists, but it also obliges states to be able to identify and detect them.

7.3 Setting up the necessary national legal framework

FATF Special Recommendation III requires countries to “adopt and implement measures, including legislative ones, that 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 organizations.” The FATF recommends similar legislative measures with respect to cash couriers. States should be able to stop or restrain currency or bearer instruments suspected to be related to the financing of terrorism or money laundering (see section 13, Supervising nonprofit organizations and other legal entities, in this module).

In addition to having in place a legislative and administrative framework for freezing and confiscating terrorist assets, states are expected to designate “competent authorities” to assume these missions. In practice, this means that states must:

- Have effective systems for communicating information on the freezing of terrorist assets to the financial sector through the relevant agencies
- Have an adequate level of coordination among customs, immigration, and other related authorities for the purpose of preventing cash couriers from contributing to terrorist financing and money laundering
- Ensure that authorities have been designated to give effect, as needed, to freezing actions undertaken by foreign jurisdictions.

7.4 Challenges

Tracking the funds and assets of terrorists is a difficult and daunting task. On average, the seizure and confiscation of assets from terrorists and terrorist organizations are not large.

Another difficulty is that compared with other operations of military nature, terrorist attacks are relatively cheap to finance. For example, the IRA bomb attempt of the British Cabinet in 1984 probably costs less than £10,000.

Knowledge check

QUESTION 15. What should be targeted for seizures? Funds, assets, or properties?

- a) Funds
- b) Assets
- c) Properties
- d) All of the above

QUESTION 16. Mechanisms for freezing, seizure, and confiscation should be compatible with the rule of law.

- a) True
- b) False

For discussion

How are the three concepts—freezing, seizing, and confiscation—implemented in your country? What entity is responsible for freezing, seizing, and confiscating the assets of terrorist financiers?

8

Reporting suspicious transactions related to terrorism

According to FATF Special Recommendation IV, financial institutions should promptly report suspicious transactions to the competent authorities, if they “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.” For more information on FATF Special Recommendation IV, see Appendix E.

As a prerequisite to the obligation to report suspicious transactions, financial institutions are required to implement customer due diligence (CDD) obligations (Article 18 of the SFT Convention).

8.1 Under what circumstances should a transaction be reported?

The FATF standard recommends filing a report with the relevant authority under the following circumstances:

- When it is suspected that funds are linked to terrorist financing, or
- When there are *reasonable grounds* to suspect that funds are linked to terrorist financing.

The first criterion, *suspicion*, entails a subjective analysis. The second, *reasonable grounds*, requires reporting under a broader set of circumstances and relies on an objective analysis. The same idea is reflected in Article 18 of the SFT Convention, which refers to unusual and suspicious transactions. The provision explains that “the unusual character of an operation” covers “all complex, unusual, large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose.”

Case study

An individual’s account activity and inclusion on a UN list indicate a possible link to terrorist activity

An individual residing in a neighboring country maintained a demand deposit account and a savings account in country N. The bank that maintained the accounts noticed in April 2001 that funds were being gradually withdrawn from the accounts. At that point it decided to monitor the accounts more closely.

The bank’s suspicions were reinforced when a name very similar to the account holder’s appeared in the consolidated list of suspected persons and entities issued by the UNSC’s Committee on Afghanistan (UNSC Resolution 1333/2000). The bank immediately filed a report with the financial intelligence unit (FIU) in country N.

—continued

The FIU analyzed the financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened in 1990 and had been fed primarily by cash deposits. In March 2000, the account holder made a sizeable transfer from his savings account to his checking account. Those funds were used to buy a single-premium life insurance policy and to purchase certificates of deposit.

From mid- to late April, there were transfers from the savings account to his demand deposit account. Those funds were then transferred by check to persons and companies located in neighboring countries and in other regions. In May and June 2001, the individual sold the certificates of deposit he had purchased and transferred the profits to the accounts of companies based in Asia and to that of a

company in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred the proceeds to an account at a bank in his country of origin. The last transaction was carried out on August 30, 2001, shortly before the September 11 attacks in the United States. Finally, the anti-money laundering unit in the individual's country of origin sent to country N information on suspicious operations carried out by the account holder and by the companies that received the transfers. Many of these names also appeared in the files of the FIU. The case is currently under investigation.

Source: FATF, Guidance for Financial Institutions for Detecting Terrorist Financing, April 24, 2002.

8.2 Challenges

It should be acknowledged that the possibility that a bank or other financial institution will be able to identify an operation as involving terrorist financing is relatively low. Unless a bank identifies a party to a transaction as a terrorist (for example, because his name appears on a list of suspected terrorists), the most it can normally do is to review transactions and report those that appear to be suspicious.

8.3 What types of institutions are expected to submit reports?

Banks and nonbank financial institutions should comply with the country's AML/CFT laws and regulations. The FATF recommends that the following types of financial institutions should be subject to compliance:

- Banks
- Bureaux de change (currency exchange offices)
- Stockbrokers
- Insurance companies
- Money transfer services

In addition, other businesses and professions that are subject to national AML/CFT laws should be covered by the reporting requirement—note, however, that some of the covered businesses and professions are only required to report for certain types of activities. The covered businesses and professions include:

- Casinos (including Internet casinos)
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Lawyers, notaries, other independent legal professionals, and accountants
- Trust services and providers of company service providers

Lawyers, notaries, other independent legal professionals, and accountants are required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction related to specific listed activities (see FATF Recommendation 12.d). These activities include the purchase and sale of real estate; the management of clients' money, securities, or other assets; the management of bank, savings, or securities accounts; the organization of contributions for the creation, operation, or management of companies; and the creation, operation, or management of legal persons or arrangements, and buying and selling of business entities. Please also review Module 3a, SAR/STRs, for further information.

CONNECTION WITH AML REGIMES

- Generally the same reporting regime should already be in place for anti-money laundering purposes.
- States should ensure that their regimes for fighting money laundering and terrorist financing are consistent.

9

Enhancing international cooperation

FATF Special Recommendation V states that “each country should afford another country [...] 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.” For more information on Special Recommendation V, see Appendix F.

International cooperation in combating the financing of terrorism is essential for success in the fight against terrorism at the global and national levels. The SFT Convention (articles 10, 11, 12–15, 18.3) has established a comprehensive set of norms for international cooperation, whereas UNSC Resolution 1373 (2001) covers the issue in broad terms (paragraphs 2.c, 2.d and 2.f). Specifically, paragraph 2.f of Resolution 1373 (2001) provides that “states shall [...] afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.”

9.1 Mutual legal assistance

The primary purpose of international cooperation is to foster a wide range of mutual legal assistance. This includes measures such as exchange of information and assistance in connection to criminal, civil enforcement, and administrative inquiries.

“Mutual legal assistance” should mean the authority to provide a full range of legal assistance.

Mutual legal assistance includes:

- Taking of evidence
- Production of documents for investigation or as evidence
- Search and seizure of documents or items relevant to criminal proceedings or investigations
- Ability to enforce a foreign restraining, seizure, confiscation, or forfeiture order in a criminal matter

The exchange of information generally occurs through mutual legal assistance mechanisms, which are generally established by treaties on a bilateral or

multilateral basis. But other means of mutual exchanges of information can be organized through:

- FIUs
- Other governmental agencies cooperating under a memorandum of understanding or letter of agreement.

9.2 Extradition of offenders and other forms of cooperation

A second purpose of international cooperation is to facilitate the extradition of individuals charged with financing of terrorism, terrorist acts, or terrorist organizations. This means that countries should

- take appropriate measures to ensure that they do not provide safe havens for individuals charged with financing terrorism, terrorist acts, or terrorist organizations; and
- have in place procedures for authorizing the extradition of terrorist financiers.

Political exceptions are not possible in cases involving the extradition of persons charged with financing of terrorism.

9.3 Challenges: A good legal framework is meaningless if states are not proactive

The best legislation in the world is of little use without the will to use it. States express their will to fight the financing of terrorism through international cooperation—for example, by communicating to the UN 1267 Committee the names of persons suspected of involvement in terrorist activities and by sharing that information with other interested states.

As another example, in the area of declaration and disclosure systems related to cash couriers (see section 13), states should take the necessary measures to retain, for use by the authorities responsible for mutual cooperation, information on the carrying of currency and bearer negotiable instruments.

UNSC Resolution 1373 imposes upon states a general obligation of due diligence in international cooperation. States must

- deny safe haven to those who finance, plan, support, or commit terrorist acts; and
- prevent those who finance, plan, facilitate, or commit terrorist acts from using their territories for those purposes, regardless of the territory in which the acts occur.

Please review Module 2 and Module 5 for further information.

 **Knowledge check**

QUESTION 17. Is there any provision for a political exception with respect to the extradition of persons charged with the financing of terrorism?

- a) Yes
- b) No

QUESTION 18. The provision of mutual legal assistance is mandatory.

- a) True
- b) False

QUESTION 19. How can the exchange of information among the countries be established?

- a) By law
- b) By memorandum of understanding
- c) By treaty
- d) Any of the above

10

Measures required for alternative remittance systems

To fight terrorist financing effectively, mechanisms must be put in place to control the cross-border movements of currencies. A legal requirement to report suspicious transactions is of little use if only some of the intermediaries providing financial services are subject to it. By the same logic, freezing terrorist funds will not be effective if informal intermediaries that transfer funds from one country to another country are beyond the reach of legal controls. Experience shows that money transfer systems have indeed been used to finance terrorists' operations. For that reason, and because of the need to improve the transparency of these systems, FATF Special Recommendation VI calls upon countries to ensure that all money and value transmission services are subject to all FATF Recommendations that apply to banks and other financial institutions. For more information on FATF Special Recommendation VI, see Appendix G.

Let us analyze the following case.

Case study Rurithania and hawalas

Rurithania is a country with hard-working immigrant communities who remit funds to their home country to support their relatives. Instead of relying on the regulated financial sector, however, most immigrants prefer to use unorthodox money transfer systems that have grown up based on cultural traditions. Informal money transfers are cheaper and offer access to areas not served by formal systems. One informal system, the *hawala* system common in the Middle East and South Asia, makes it possible to transfer money without physical movement of funds. How? The *hawala* operator in the country of the originator of the transfer

contacts his or her correspondent in the country of destination and instructs him or her to give cash to the recipient of the transfer. Just like banks, *hawala* operators later settle their mutual claims. Immigrants in Rurithania use money transfer businesses for legitimate and benign purposes. But recently the Rurithanian authorities have begun to fear that terrorist organizations are using these unregulated money remittance systems to finance terrorism. The sobering fact is that these small businesses can be used not only as storefront operations, but also as an entry point into the whole financial sector.

Covering all money and value transfer services

Special Recommendation VI aims to ensure that countries impose AML/CFT requirements on *all forms* of money and value transfer systems, formal and informal.

Informal money and value transfer systems are also called alternative remittance services. Formal money and value transfer services are provided by banks and other regulated financial institutions (nonbank financial institutions, or NBFIs). Informal money and value transfer services are a type of financial service in which money or another form of value is moved from one geographic location to another through informal or unsupervised networks or mechanisms. These services increase the risk of abuse by terrorists and those who collect and provide funds to terrorist organizations. Some of the informal systems are legal; others are not. Informal systems include the black market peso exchange, hundi, and *hawala* systems.

Knowledge check

QUESTION 20. Which of the following figures is closest to the actual amount of money sent abroad each year by people working outside their home country?

- a) About US\$500 million
- b) About US\$900 million
- c) About US\$50 billion
- d) About US\$100 billion

For discussion

What do you think states should do about money transfer services? What is the situation in your country?

Informal remittances

Only the FATF Special Recommendations and the SFT Convention address the issue of informal money remitters. FATF Special Recommendation VI provides that states should:

- license or register all money and value transfer services, formal and informal;
- subject all formal and informal money transfer services to the FATF Recommendations (in particular, Recommendations 4–16 and 21–25) and the FATF Special Recommendations; and
- ensure that persons or legal entities that provide money transfer services illegally are subject to administrative, civil, or criminal sanctions.

The SFT Convention calls upon the states not only to supervise money transfer services (Article 18.2a), but also to consider measures for monitoring the cross-border transport of funds (Article 18.2b).

“ For discussion ”

Is the introductory case on Rurithania and *hawalas* unrealistic? What is the situation in your country?

**Two other possible scenarios:
The United States and India***The United States*

The situation in Rurithania is by no means implausible. Indeed, it could describe the current situation in many countries. The United States adopted legislation (The USA PATRIOT Act) to require informal money transfer services to register with the U.S. Treasury Department and, at the state level, to get a license for money transfers. In addition, these businesses must have adequate AML programs in place. This legislation does not resolve all the issues. Supervisory authorities must implement the controls and law enforcement authorities must ensure that informal money transfer businesses comply with the legislation. (31 USC 5330 and 31 CFR 103.41)

India

India's approach is quite different. *Hawala* transactions are banned under India's Foreign Exchange Management Act. India has consistently taken the stand that "registration" of *hawala* dealers is an oxymoron; by their very nature, in the Indian view, *hawala* transactions, especially those relating to terrorist activities, are clandestine. Because the *hawala* system is based on trust and, therefore, generates little in the way of records, neither licensing nor registration could ever succeed.

Source: Letter dated May 28, 2004, from the Permanent Representative of India to the Chairman of the UN Counter-Terrorism Committee, attached to UN document S/2004/45 1, June 3, 2004

11

Measures required for wire transfers

Consider the following two situations. The answers to the questions will be discussed at the end of this section.

QUESTION 21. A bank receives a wire transfer from a bank located in a foreign country. The transfer does not contain the name or address of the originator of the wire. Is this

- a) A minor concern?
- b) Something that should alert the bank and trigger an internal check for a possible suspicious transaction?
- c) Something that is not important as long as the other elements of the wire conform to proper financial practice?
- d) Something that should immediately be reported to the authorities?

QUESTION 22. Bank A receives an international wire transfer through the intermediary services of the correspondent bank of a foreign bank B which does not contain meaningful originator information. Is this

- a) A minor concern?
- b) Something normal given that it is the role of the correspondent bank to conduct the necessary checking if need be?
- c) Something that is irrelevant because the correspondent bank had already checked this information about the wire transfer?
- d) Something that should alert the bank and justify an internal checking for a possible suspicious transaction to be reported?

11.1 What is a wire transfer?

According to the Interpretative Note to FATF Special Recommendation VII, the “terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.”

As a means of moving funds across borders, wire transfers are just the sort of transaction that should be under scrutiny for possible money laundering and terrorist financing. For that reason FATF Special Recommendation VII sets forth a

special standard on wire transfers that is not directly reflected in the text of the SFT Convention and UNSC resolutions. For more information on FATF Special Recommendation VII, see Appendix H.

11.2 What is the FATF's standard on wire transfers?

FATF Special Recommendation VII obliges states to take specific measures to ensure that financial intermediaries:

- Make sure that accurate and meaningful information on the originator (the name, address, account number) is included in the wire transfer or related message
- Retain the originator's information with the wire transfer or related message through the chain of payment (correspondent banks are part of that chain)
- Enhance their scrutiny of wire transfers that do not include information on the originator and be alert to the possibility of suspicious transactions.

11.3 Who is covered by the wire transfer standard?

The standard is very clear—and it casts a wide net. All financial institutions, as defined by the FATF Forty Recommendations, should be subjected to these requirements. But Special Recommendation VII is particularly relevant to banks and other remittance service providers.

FATF Special Recommendation VII addresses only the lack of meaningful information on the originator of wire transfers. In broader terms, however, it is important to remember that Special Recommendation IV requires financial institutions to report transactions if they suspect that the funds may be used for terrorism.

Information on both the originator and the beneficiary deserves some scrutiny

The following case provides an example of the use of EFT (electronic funds transfer) to transfer funds from Canada to suspected terrorist organizations.

Suspicious use of wire transfers

FINTRAC, the Canadian FIU, received reports from various financial institutions regarding three individuals sending funds to the same person in a foreign country. These individuals had accounts at separate financial institutions and seemed unrelated.

The first individual is a student living in Canada (as reported by one of the financial institutions), who brought in large amounts of U.S. currency, exchanged it for Canadian currency, deposited checks drawn on financial institutions in the United States, requested a draft payable to a currency exchange company, and wired funds to a foreign country of concern. This individual had accounts with three different financial institutions and provided each institution with different addresses, phone numbers, and occupations. One of the addresses belonged to a mailbox service, one of many international mail forwarding centers in Canada. Another address was listed under the name of one of the other two individuals.

—continued

The second individual was reported to be an accountant who deposited and received large amounts of money in his personal account and then wired funds to the same country of concern. This individual had four different addresses.

The third individual deposited \$10,000 in cash in his account. An EFT report received by FINTRAC showed that on the same day \$10,000 was sent by this individual to the same foreign country of concern. His reported address matched an address provided by one of the other individuals.

Several EFT reports received by FINTRAC showed that the same person in the foreign country was receiving money from all three individuals.

This case was identified as a case of potential terrorist financing because of

- multiple unlinked transactions benefiting the same individual;
- deposits that were followed within a short time by wire transfers to or through a location of specific concern;
- multiple reporting entities reporting suspicious transactions;
- significant and round-number dollar deposits to personal accounts over a short period; and
- unexplained inconsistencies in the identification process.

Source: FATF-XV Typologies Exercise (2003–2004) Compilation of Country Submissions: Part 8.

Now let us revisit the two situations presented at the beginning of this section.

QUESTION 21. A bank receives a wire transfer from a bank located in a foreign country. The transfer does not contain the name or address of the originator of the wire. Is this

- a) A minor concern?
- b) Something that should alert the bank and trigger an internal check for a possible suspicious transaction?
- c) Something that is not important as long as the other elements of the wire conform to proper financial practice?
- d) Something that should immediately be reported to the authorities?

QUESTION 22. Bank A receives an international wire transfer through the intermediary services of the correspondent bank of a foreign bank B which does not contain meaningful originator information. Is this

- a) A minor concern?
- b) Something normal given that it is the role of the correspondent bank to effect the necessary checking if need be?
- c) Something that is irrelevant because the correspondent bank had already checked this information about the wire transfer?
- d) Something that should alert the bank and justify an internal checking for a possible suspicious transaction to be reported?

12

Dealing with cash couriers

Consider the following case.

Case study

Cross-border cash movement

The government of Rurithania appears to have been successful in regulating and controlling alternative remittance systems through the registration process. Entities that handle a daily volume of US\$15,000 in remittances must now be licensed by the central bank for prudential purposes. But despite the success the government has achieved, the central bank has observed (through its monetary surveillance department) that

the amount of remittances moving through registered and licensed entities has declined, while there has been an increase in people crossing the border with hard currency. Customs officials have confirmed this trend and indicated that because there is no limit on how much cash individuals can carry across the border there is little that can be done. The customs officials have asked the central bank to look into the matter.

12.1 Why monitor cross-border transportation of cash?

The objective of FATF Special Recommendation IX on cash couriers is to address the risk that terrorist financiers or money launderers may seek to avoid the effect of regulations on alternative remittance systems (Special Recommendation VI) by using cash couriers to move assets across international borders. This Special Recommendation requires the monitoring of cross-border transportation of cash and bearer negotiable instruments and the adoption of an appropriate domestic legal framework for the implementation of this new Recommendation. This is in line with the general recommendation of UNSC Resolution 1526 (2004), which urges “all States [...] to establish internal reporting requirements and procedures on the trans-border movement of currency based on applicable thresholds” (paragraph 5). Similar provision could also be found in article 18.2b of the SFT Convention. For more information on FATF Special Recommendation IX, see Appendix I.

12.2 What is targeted?

FATF Special Recommendation IX deals with the act of carrying *cash or its equivalent* across national borders. Under the recommendation, states are

required to monitor the carrying of currency or bearer negotiable instruments, whether by a natural person or by post or freight.

- Currency refers to banknotes and coins in circulation as a medium of exchange.
- Bearer negotiable instruments are monetary instruments in bearer form (checks, money orders, traveler's checks, and so forth).

FATF Special Recommendation IX targets the cross-border transportation of cash or its equivalent under two sets of circumstances: first, when the currency or negotiable instrument is suspected to be related to terrorist financing or money laundering; and second, when it has been falsely disclosed or declared. The distinction is important. It means that states not only need to have a system for declaring or disclosing cross-border transportation of cash or cash equivalents, but also they need to be able to detect these operations when there is a suspicion of criminal activity.

12.3 What sort of action is required?

States should take several steps to comply with Special Recommendation IX. States should have:

- Measures in place to detect the transportation by couriers of cash or cash equivalents
- The power to stop or restrain the cash or cash equivalent
- Effective, proportionate, and dissuasive sanctions in case of violations of the law, including the possible confiscation of the cash or cash equivalent.

Detection systems may vary among states. They should not excessively inconvenience the public or overburden the customs agencies. The right balance must be found between the use of administrative mechanisms, on one hand, and intelligence information, on the other. There are two systems by which the physical transportation of cash or its equivalent may be detected.

I. DECLARATION SYSTEM

Under a declaration system persons carrying across the border currency or bearer negotiable instruments exceeding a certain value (for example, EUR/US\$ 15,000) are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the threshold is sufficiently low to meet the objectives of Special Recommendation IX.

II. DISCLOSURE SYSTEM

Under a disclosure system persons carrying across the border currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

Cash couriers

A British national, Mr. Butler, asked H to carry cash from the United Kingdom to Spain for real estate transactions he intended to make in that country. The courier did not make it to Spain because he was stopped by British customs under the Drug Trafficking Act 1994. Driving a hired car, H was stopped at Portsmouth by a British Customs and Excise officer. When asked how much cash he was carrying, H answered, “£500.” A subsequent search of the car turned up £240,000. H stated that the sum in question belonged to a friend who was meeting him in Spain. H was subsequently questioned about the money by Customs and Excise officials. He repeated that he was taking the money out of the country for another individual who intended to use it to buy an apartment in Spain. The money was seized and sent for forensic testing.

Source: Extract from Butler v. The United Kingdom, 06/27/2002, European Court of Human Rights, Reports of Judgments and Decisions 2002-VI.

12.4 Implementation of sanctions

FATF Special Recommendation IX requires that sanctions be applied in two situations:

- When a person makes a false declaration or disclosure (for example, declaring \$500 but carrying \$10,000). The sanctions should be effective, proportionate, and dissuasive.
- When the cash or bearer negotiable instruments transported are related to terrorist financing or money laundering. In this case, the cash or bearer negotiable instruments should be confiscated. To do this, states must have the proper confiscation regime in place.

When a customs official stops or restrains cash, this is not a sanction. It is a temporary interference with the rights of the courier or of the owner. However, the interference must not extend beyond a reasonable time—the time needed to collect further information or evidence of criminal activity.

12.5 Challenges to the implementation of FATF Special Recommendation IX

So far, few states have systems in place to comply with FATF Special Recommendation IX. Some may have legislation dealing with the specific case of cash couriers (usually in connection with drug trafficking). Others may hope to use their exchange control legislation to satisfy the requirement of the Recommendation. However, it should be kept in mind that the objective of the recommended monitoring system is both broader and more specific than the goal of exchange controls. It is broader because its aim is to ensure that terrorists and other criminals cannot finance their activities or launder the proceeds of their crime, whatever the crime may be. It is more specific because measures aimed at controlling the cross-border flow of currency, including cash or cash equiva-

lents, for balance-of-payments purposes are often not sufficient and adequate to combat terrorism.

When implementing the Special Recommendation IX, states respect their obligation not to interfere with legitimate trade. Nothing in this Recommendation should be construed to allow states to restrict trade payments between countries for goods and services, or to limit the movement of capital in contravention of their obligations under treaties, conventions, or other agreements.

Knowledge check

QUESTION 23. Is the physical transport of gold or precious metal covered by FATF Special Recommendation IX?

- a) Yes b) No

QUESTION 24. If a customs officer discovers that a cash carrier has not disclosed the true amount of currency or bearer negotiable instruments he is carrying, should the officer have the authority to request and obtain further information with regard to the origin of the cash?

- a) Yes b) No

13

Supervising nonprofit organizations and other legal entities

FATF Special Recommendation VIII addresses the risk of abuse or misuse by terrorist organizations and terrorist financiers of entities legally created under domestic laws. Its aim is thus to prevent juridical persons from being used as a cover for or as a means of financing their activities. For more information on FATF Special Recommendation VIII, see Appendix J.

13.1 What entities should be under scrutiny?

Because it refers to “entities” in general, FATF Special Recommendation VIII is broad in scope. Remember that financing for terrorism may come from legitimate sources. Any juridical person, even businesses that appear perfectly legitimate, might conceivably be used as a screen for collecting funds for terrorists and their organizations. For these reasons, states must be sure that the legal definition of financing terrorism includes funds derived from legitimate sources and take the steps necessary to prevent this type of funding.

Examples of entities under scrutiny

Osama bin Laden and his organization, Al-Qaeda, have based their financial empire in part on ordinary business activities. Some of the businesses from which bin Laden and Al-Qaeda derive funds are quite substantial; others are very small. According to a researcher with the International Policy Institute for Counter-Terrorism, “Al-Qaeda has at one time operated ostrich farms and shrimp boats in Kenya, bought tracts of forest in Turkey, engaged in diamond trading in Africa and acquired agricultural holdings in Tajikistan. Many of these minor enterprises—such as the fishing business in Kenya—served as a cover for terrorist operations.” (Source: Yael Shahar. “Tracing bin Laden’s Money—Easier said than done.” September 21, 2001. <http://www.ict.org.il/articles/tabid/66/articlesid/71>.)

“Terrorist groups are increasingly using ‘front companies,’ commercial enterprises that engage in legitimate business, but which are also used to mix illicit revenues with legitimate profits from commercial enterprise. These front businesses are involved in everything from convenience stores to international investment management services.”

Source: Bedi Rohand, *Money Laundering Controls and Prevention*, London, ISI Publications, 2004: 315) For another case involving a diamond trading company, see example 3 in *Guidance for Financial Institutions in Detecting Terrorist Financing*, FATF, 2002.

FATF Special Recommendation VIII also stresses the vulnerabilities of nonprofit organizations, warning that charities, religious, educational, social, and fraternal organizations can be misused by terrorists. According to the standard, countries should ensure that nonprofits cannot be misused

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

Nonprofit organizations

“One nonprofit organization solicited donations from local charities in a donor region, in addition to fund raising efforts conducted at its headquarters in a beneficiary region. This nonprofit organization falsely asserted that the funds collected were destined for orphans and widows. In fact, the finance chief of this organization served as the head of organized fundraising for Osama bin Laden. Rather than providing support for orphans and widows, funds collected by the nonprofit organization were turned over to al-Qaeda operatives.” For another example, see Module 1: Where do money laundering and terrorist financing operations take place?

Source: FATF, “Combating the Abuse of Nonprofit Organizations: International Best Practices,” October 2002, p. 7.

FATF Special Recommendation VIII is necessarily rather general because the different entities categorized as nonprofit organizations take many different legal forms—among them associations, foundations, fundraising committees, community service organizations, corporations in the public interest, and limited companies—and because the nature of their operations varies from one jurisdiction to the next. Thus, the standard suggests a form of self-assessment by each country. States are asked to review their national legislation for risks and weaknesses.

13.2 What kind of oversight is needed? By whom?

States are not required to adopt any specific solution. FATF Special Recommendation VIII does not impose a particular model.

- Steps should be taken to ensure the transparency and accountability of nonprofit organizations and action taken to address serious risks and vulnerabilities.
- These actions should be guided by the principle that the oversight should be flexible, effective and proportional to the risk of abuse. Note that FATF’s “International Best Practices” are a good source of direction and practical advice.

Who ensures the oversight? Solutions vary among countries. For instance, the United Kingdom set up a Charity Commission and has in place a system of registration. Tax authorities might play a role in certain jurisdictions. But traditionally, the objective of tax authorities, in respect of charities, is to verify that the benefits of tax relief are passed on to recipients (through projects and grants). Implementation of the FATF standard, therefore, entails consequently that the agencies responsible for such oversight functions broaden their focus.

Knowledge check

Please answer the following questions.

QUESTION 25. Can the fight against terrorist financing justify restrictions on charitable activities?

QUESTION 26. Should states be more flexible regarding the activities of religious nonprofit organizations?

QUESTION 27. When nonprofit organizations disburse funds to foreign organizations should this cause special concern?

For discussion

Based on your personal experience and your knowledge of circumstances in your country, do you believe that the measures outlined in international standards on preventing the financing of terrorism are likely to be effective? Can

measures such as the freezing and confiscation of assets prevent terrorist acts and curtail the activities of terrorist organizations?

Should states try to supervise informal money transfer services? Is it possible to control informal business? What about the risk that remitters will seek and find unregulated ways to provide this type of underground business?

Check your understanding

QUESTION 28. Although the SFT Convention does not offer a definition of _____, it does define _____. That definition emphasizes two aspects of the financing of terrorism: providing funds and _____ funds with the intention that they should be used, or with the knowledge that they will be used, to carry out terrorist acts.

QUESTION 29. Various international instruments deal with the issue of the financing of terrorism. From the list that follows, select the assertions that are true.

- a) The SFT Convention is the most comprehensive international instrument on the financing of terrorism.
- b) The SFT Convention is the only instrument that covers the freezing of funds.
- c) UNSC 1373 (2001) sets up a general framework of anti-terrorism measures and is mandatory for all states.
- d) The FATF Special Recommendations cover specific issues of the financing of terrorism that are not always addressed by other instruments.

QUESTION 30. International standards and obligations concerning the financing of terrorism fall principally on _____. However, some rules also target specific _____ and terrorist _____. The UN 1267 Committee has established a system of periodically reviewing _____ of suspected terrorists and terrorist organizations.

QUESTION 31. Is ratification of the SFT Convention the only measure states should take to comply with international rules on terrorist financing?

QUESTION 32. According to the SFT Convention and UNSC Resolution 1373, must states criminalize the financing of terrorism when the offense is committed abroad by one of their nationals?

QUESTION 33. Which of the following statements is true?

- a) States have a duty to freeze or seize the assets of terrorists. Actual confiscation is optional and may be done at the discretion of states.
- b) States are obliged to establish a legal framework for the freezing, seizure, and confiscation of assets of terrorists. They may choose the means of implementing those measures in their national legal system.
- c) States have no obligation to freeze the assets of terrorists and terrorist organizations listed by the UN 1267 Committee provided they maintain their own list of terrorists and terrorist organizations.

QUESTION 34. States should make sure that their legislation obligates their financial institutions and, for certain types of activities, other professionals (such as dealers in precious _____ and _____ lawyers, notaries, and so on) to report suspicious transactions. This duty applies not only to the CFT regime, but also to the state's _____ regime. Under the CFT regime, institutions must report to the authorities when they suspect that funds are linked to the financing of terrorism or when there is _____ to suspect that funds are so linked (for example, when a party to a suspicious transaction is listed as terrorist).

QUESTION 35. States' obligation to cooperate at the international level extends only to the criminal dimension of the fight against terrorist financing.

- a) True
- b) False

QUESTION 36. Which assertion is most accurate?

- a) The FATF Special Recommendations address the issue of the weakness of formal financial systems to specifically cover the problem of wire transfers and impose duties on financial intermediaries, such as requiring meaningful information on the originator of a wire.
- b) The FATF Special Recommendations address the issue of the weakness of formal and informal financial systems by imposing specific duties on financial intermediaries with respect to wire transfers and remittance systems.

QUESTION 37. With respect to charities and nonprofit organizations, there is no specific model that states must adopt. Special Recommendation VIII essentially requires that states ensure the transparency and accountability of nonprofit organizations and take corrective action where serious vulnerabilities exist.

a) True b) False

Summary

In this module, we discussed the following;

- The rationale for combating the financing of terrorism
- The UN instruments that must be ratified and implemented
- The kind of offenses that should be criminalized
- The measures required to freeze, seize, and confiscate terrorist assets
- How to report suspicious transactions related to terrorism
- How to enhance international cooperation
- The nature of alternative remittance systems and the measures required to monitor them
- The measures applicable to wire transfers and cash couriers
- The supervision of nonprofit organizations



Appendix A: References

FATF Recommendations

- The Forty Recommendations (FATF, June 2003)
<http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf>
- Special Recommendations on Terrorist Financing (FATF, October 2004)
<http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf>

Useful Web sites

- Fight against Terrorism, Council of Europe
http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against_terrorism/default.asp
- Terrorism, United Nations Office on Drugs and Crime
<http://www.unodc.org/unodc/terrorism.html>
- UN action against terrorism, United Nations [conventions, declarations, news, and developments]
<http://www.un.org/terrorism/>

Reference Documents

- Combating the Abuse of Nonprofit Organizations: International Best Practices (FATF, October 2002)
<http://www.fatf-gafi.org/dataoecd/39/19/34033761.pdf>
- Guidance Notes for the Special Recommendations on Terrorist Financing and the Self-Assessment Questionnaire (FATF, March 2002)
<http://www.fatf-gafi.org/dataoecd/39/20/34033909.pdf>
- Guidance for Financial Institutions in Detecting Terrorist Financing (FATF, April 2002)
<http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf>
- Suppressing the Financing of Terrorism: A Handbook for Legislative Drafting (IMF, August 2003)
<http://www.imf.org/external/pubs/nft/2003/SFTH/>
- United Nations Convention for the Suppression of the Financing of Terrorism (UN, 1999)
<http://untreaty.un.org/English/Terrorism/Conv12.pdf>

- United Nations Security Council Resolution 1267 (UN, October 1999)
<http://www.un.org/Docs/scres/1999/sc99.htm>
- United Nations Security Council Resolution 1269 (UN, October 1999)
<http://www.un.org/Docs/scres/1999/sc99.htm>
- United Nations Security Council Resolution 1333 (UN, December 2000)
<http://www.un.org/Docs/scres/2000/sc2000.htm>
- United Nations Security Council Resolution 1373 (UN, September 2001)
<http://www.un.org/Docs/scres/2001/sc2001.htm>
- United Nations Security Council Resolution 1390 (UN, January 2002)
<http://www.un.org/Docs/scres/2002/sc2002.htm>
- United Nations Security Council Resolution 1452 (UN, December 2002)
<http://www.un.org/Docs/scres/2002/sc2002.htm>
- United Nations Security Council Resolution 1455 (UN, January 2003)
http://www.un.org/Docs/sc/unsc_resolutions03.html
- United Nations Security Council Resolution 1456 (UN, January 2003)
http://www.un.org/Docs/sc/unsc_resolutions03.html
- United Nations Security Council Resolution 1526 (UN, January 2004)
http://www.un.org/Docs/sc/unsc_resolutions04.html
- Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols (UNODC, 2003)
http://www.unodc.org/pdf/crime/terrorism/explanatory_english2.pdf



Appendix B: FATF Special Recommendation I

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 UN International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the UN resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly UN Security Council resolution 1373.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)

SR I: Ratification and implementation of UN instruments

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.
- Jurisdictions should implement five UN Security Council resolutions: S/RES/1267(1999), S/RES/1269(1999), S/RES/1333(2000), S/RES/1373(2001) and S/RES/1390(2001).

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 UN. *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.

The UN Convention was open for signature from January 10, 2000 to December 31, 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 UN in New York. Those countries that have not signed the Convention may accede to it (see Article 25 of the Convention). The full text of the UN Convention may be consulted at <http://untreaty.un.org/English/Terrorism.asp>. As of March 19, 2002, 132 countries have signed, and 24 have deposited ratification instruments. On March 10, 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 April 10, 2002. The Web page containing information on the status of the Convention is located on the UN Web site 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/Treaty Handbook/hbframeset.htm](http://untreaty.un.org/English/Treaty%20Handbook/hbframeset.htm). The texts of the relevant UN Security Council resolutions may be consulted on the UN Web site at <http://www.un.org/documents/scres.htm>.



Appendix C: FATF Special Recommendation II

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalize the financing of terrorism, terrorist acts, and terrorist organisations. Countries should ensure that such offenses are designated as money laundering predicate offenses.

INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION II:

CRIMINALISING THE FINANCING OF TERRORISM AND ASSOCIATED MONEY LAUNDERING

Objective

- 1) Special Recommendation II (SR II) was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and *inter alia* money laundering, another objective of SR II is to emphasize this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. The basis for criminalising terrorist financing should be the UN International Convention for the Suppression of the Financing of Terrorism, 1999.³

Definitions

- 2) For the purposes of SR II and this Interpretative Note, the following definitions apply:
 - a) The term *funds* refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, traveler's checks, bank check, money orders, shares, securities, bonds, drafts, letters of credit.
 - b) The term *terrorist* refers to any natural person who (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts;

³ Although the UN Convention had not yet come into force at the time that SR II was originally issued in October 2001, and thus is not cited in the SR itself, the intent of the FATF has been from the issuance of SR II to reiterate and reinforce the criminalization standard as set forth in the Convention (in particular, Article 2). The convention came into force in April 2003.

- (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
- c) The term *terrorist act* includes (i) an act that constitutes an offence within the scope of, and as defined in, one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and (ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.
- d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.
- e) The term terrorist organisation refers to any group of terrorists that (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Characteristics of the Terrorist Financing Offense

- 3) Terrorist financing offences should extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

- 4) Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.
- 5) Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.
- 6) Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).
- 7) It should also be an offence to attempt to commit the offense of terrorist financing.
- 8) It should also be an offence to engage in any of the following types of conduct:
 - a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note
 - b) Organizing or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note
 - c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offense; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offense
- 9) Terrorist financing offences should be predicate offences for money laundering.
- 10) Terrorist financing offenses should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.
- 11) The law should permit the intentional element of the terrorist financing offense to be inferred from objective factual circumstances.
- 12) Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (for example, due to fundamental principles of domestic law), civil or administrative liability should apply.
- 13) Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil, or administrative proceedings in countries in which more than one form of liability is available.
- 14) Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil, or administrative sanctions for terrorist financing.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)¹

SR II: Criminalising the financing of terrorism and associated money laundering

This Recommendation contains two elements:

- Jurisdictions should criminalize “the financing of terrorism, of terrorist acts and of terrorist organizations.”
- Jurisdictions should establish terrorist financing offenses as predicate offenses for money laundering.

In implementing SR II, jurisdictions must either establish specific criminal offenses for terrorist financing activities, or they must be able to cite existing criminal offenses 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 Web site 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.

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 Web site at http://www.fatfgafi.org/40Recs_en.htm.

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.

¹Please note that the reference to Recommendation 4 in the guidance note refers to the 1996 version of the FATF 40 Recommendations.



Appendix D: FATF Special Recommendation III

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 organizations in accordance with the UN 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 organizations.

INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION III:

FREEZING AND CONFISCATING TERRORIST ASSETS

Objectives

- 1) FATF Special Recommendation III consists of two obligations. The first requires jurisdictions to implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant UN resolutions. The second obligation of Special Recommendation III is to have measures in place that permit a jurisdiction to seize or confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court.
- 2) The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative; the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.

Scope

- 3) Special Recommendation III is intended, with regard to its first requirement, to complement the obligations in the context of the UNSC resolutions relating to the prevention and suppression of the financing of terrorist

acts—S/RES/1267(1999) and its successor resolutions, S/RES/1373(2001) and any prospective resolutions related to the freezing, or if appropriate seizure, of terrorist assets. It should be stressed that none of the obligations in SR III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding.⁴ The focus of SR III instead is on the preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups.

- 4) S/RES/1267(1999) and S/RES/1373(2001) differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations.
- 5) S/RES/1267(1999) and its successor resolutions obligate jurisdictions to freeze without delay the funds or other assets owned or controlled by Al-Qaeda, the Taliban, Osama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaeda and Taliban Sanctions Committee established pursuant to UN Security Council resolution 1267 (the Al-Qaeda and Taliban Sanctions Committee), including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory. The Al-Qaeda and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999). All jurisdictions that are members of the United Nations are obligated by S/RES/1267(1999) to freeze the assets of persons and entities so designated by the Al-Qaeda and Taliban Sanctions Committee.⁵
- 6) S/RES/1373(2001) obligates jurisdictions⁶ to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other

⁴ For instance, both the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) and UN Convention against Transnational Organised Crime (2000) contain obligations regarding freezing, seizure, and confiscation in the context of combating transnational crime. Those obligations exist separately and apart from obligations that are set forth in S/RES/1267(1999), S/RES/1373(2001) and SR III.

⁵ When the UNSC acts under Chapter VII of the UN Charter, the resolutions it issues are mandatory for all UN members.

⁶ The UNSC was acting under Chapter VII of the UN Charter in issuing S/RES/1373(2001) (see previous footnote).

assets frozen. Additionally, to ensure that effective cooperation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

Definitions

- 7) For the purposes of SR III and this Interpretive Note, the following definitions apply:
- a) The term *freeze* means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.
 - b) The term *seize* means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is affected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.
 - c) The term *confiscate*, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the state. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets.⁷

⁷ Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

- d) The term *funds or other assets* means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, traveler's checks, bank checks, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends, or other income on or value accruing from or generated by such funds or other assets.
- e) The term *terrorist* refers to any natural person who (i) commits, or attempts to commit, terrorist acts⁸ by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts or terrorist financing; (iii) organizes or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.
- f) The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings, or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out terrorist acts.
- g) The term *terrorist organization* refers to any legal person, group, undertaking, or other entity owned or controlled directly or indirectly by a terrorist(s).
- h) The term *designated persons* refers to those persons or entities designated by the Al-Qaeda and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).
- i) The phrase *without delay*, for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaeda and

⁸ A terrorist act includes an act which constitutes an offense within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, International Convention against the Taking of Hostages; Convention on the Physical Protection of Nuclear Material; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf; International Convention for the Suppression of Terrorist Bombings; and the International Convention for the Suppression of the Financing of Terrorism (1999).

Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organization. The phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Freezing without delay terrorist-related funds or other assets

8) To fulfill the preventive intent of SR III, jurisdictions should establish the necessary authority and adopt the following standards and procedures to freeze the funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with both S/RES/1267(1999) and S/RES/1373(2001):

- a) **Authority to freeze, unfreeze, and prohibit dealing in funds or other assets of designated persons.** Jurisdictions should prohibit by enforceable means the transfer, conversion, disposition, or movement of funds or other assets. Options for providing the authority to freeze and unfreeze terrorist funds or other assets include the following:
- (i) Empowering or designating a competent authority or a court to issue, administer, and enforce freezing and unfreezing actions under relevant mechanisms
 - (ii) Enacting legislation that places responsibility for freezing the funds or other assets of designated persons publicly identified by a competent authority or a court on the person or entity holding the funds or other assets and subjecting them to sanctions for noncompliance.

The authority to freeze and unfreeze funds or other assets should also extend to funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by such terrorists, those who finance terrorism, or terrorist organizations.

Whatever option is chosen there should be clearly identifiable competent authorities responsible for enforcing the measures.

The competent authorities shall ensure that their nationals or any persons and entities within their territories are prohibited from making any funds or other assets, economic resources or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of: designated persons, terrorists; those who finance terrorism; terrorist organizations; entities owned or controlled, directly or indirectly, by such persons or entities; and persons and entities acting on behalf of or at the direction of such persons or entities.

- b) **Freezing procedures.** Jurisdictions should develop and implement procedures to freeze the funds or other assets specified in paragraph (c) below

without delay and without giving prior notice to the persons or entities concerned. Persons or entities holding such funds or other assets should be required by law to freeze them and should furthermore be subject to sanctions for noncompliance with this requirement. Any delay between the official receipt of information provided in support of a designation and the actual freezing of the funds or other assets of designated persons undermines the effectiveness of designation by affording designated persons time to remove funds or other assets from identifiable accounts and places. Consequently, these procedures must ensure (i) the prompt determination whether reasonable grounds or a reasonable basis exists to initiate an action under a freezing mechanism and (ii) the subsequent freezing of funds or other assets without delay upon determination that such grounds or basis for freezing exist. Jurisdictions should develop efficient and effective systems for communicating actions taken under their freezing mechanisms to the financial sector immediately upon taking such action. As well, they should provide clear guidance, particularly financial institutions and other persons or entities that may be holding targeted funds or other assets on obligations in taking action under freezing mechanisms.

- c) ***Funds or other assets to be frozen or, if appropriate, seized.*** Under Special Recommendation III, funds or other assets to be frozen include those subject to freezing under S/RES/1267(1999) and S/RES/1373(2001). Such funds or other assets would also include those wholly or jointly owned or controlled, directly or indirectly, by designated persons. In accordance with their obligations under the UN International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention (1999)), jurisdictions should be able to freeze or, if appropriate, seize any funds or other assets that they identify, detect, and verify, in accordance with applicable legal principles, as being used by, allocated for, or being made available to terrorists, those who finance terrorists or terrorist organizations. Freezing or seizing under the Terrorist Financing Convention (1999) may be conducted by freezing or seizing in the context of a criminal investigation or proceeding. Freezing action taken under Special Recommendation III shall be without prejudice to the rights of third parties acting in good faith.
- d) ***De-listing and unfreezing procedures.*** Jurisdictions should develop and implement publicly known procedures to consider delisting requests upon satisfaction of certain criteria consistent with international obligations and applicable legal principles, and to unfreeze the funds or other assets of de-listed persons or entities in a timely manner. For persons and entities designated under S/RES/1267(1999), such procedures and criteria should be in accordance with procedures adopted by the Al-Qaeda and Taliban Sanctions Committee under S/RES/1267(1999).

- e) **Unfreezing upon verification of identity.** For persons or entities with the same or similar name as designated persons, who are inadvertently affected by a freezing mechanism, jurisdictions should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner upon verification that the person or entity involved is not a designated person.
- f) **Providing access to frozen funds or other assets in certain circumstances.** Where jurisdictions have determined that funds or other assets, which are otherwise subject to freezing pursuant to the obligations under S/RES/1267(1999), are necessary for basic expenses; for the payment of certain types of fees, expenses, and service charges, or for extraordinary expenses⁹, jurisdictions should authorize access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and subject to approval of the Al-Qaeda and Taliban Sanctions Committee. On the same grounds, jurisdictions may authorize access to funds or other assets, if freezing measures are applied pursuant to S/RES/1373(2001).
- g) **Remedies.** Jurisdictions should provide for a mechanism through which a person or an entity that is the target of a freezing mechanism in the context of terrorist financing can challenge that measure with a view to having it reviewed by a competent authority or a court.
- h) **Sanctions.** Jurisdictions should adopt appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing freezing mechanisms by financial institutions and other persons or entities that may be holding funds or other assets as indicated in paragraph 8(c) above. Failure to comply with such legislation, rules or regulations should be subject to civil, administrative, or criminal sanctions.

Seizure and Confiscation

- 9) Consistent with FATF Recommendation 3, jurisdictions should adopt measures similar to those set forth in Article V of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), Articles 12 to 14 of the UN Convention on Transnational Organized Crime (2000), and Article 8 of the Terrorist Financing Convention (1999), including legislative measures, to enable their courts or competent authorities to seize and confiscate terrorist funds or other assets.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)

This recommendation contains three major elements:

- Jurisdictions should have the authority to freeze funds or assets of (a) terrorists and terrorist organizations and (b) those who finance terrorist acts or terrorist organizations.

⁹ See Article 1, S/RES/1452(2002) for the specific types of expenses that are covered.

- 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 organizations, and (c) property intended or allocated for use in terrorism, in terrorist acts, or by terrorist organizations.
- 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 organizations; and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organizations.

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 authorizing 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.

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:

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.

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.

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.

With regard to freezing in the context of SR III, the terms *terrorists*, *those who finance terrorism*, and *terrorist organizations* 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.



Appendix E: Special Recommendation IV

IV. Reporting suspicious transaction 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 organizations, they should be required to report promptly their suspicions to the competent authorities.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)[†]

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.
- 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.

For SR IV, the term *financial institutions* refers to both banks and NBFIs. In the context of assessing implementation of FATF Recommendations, NBFIs include, at 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 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.

The term *competent authority*, for the purposes of SR IV, is understood to be either the jurisdiction's FIU or another central authority that has been designated by the jurisdiction for receiving disclosures related to money laundering. With regard to the terms *suspect* and *have reasonable grounds to suspect*, the

[†]Please note that the reference to Recommendation 15 in the guidance note below refers to the 1996 version of the FATF 40 Recommendations.

distinction is being made among levels of mental certainty that could form the basis for reporting a transaction. The first term—that is, a requirement to report to competent authorities when a financial institution suspects that funds are derived from or intended for use in terrorist activity—is a subjective standard and transposes the reporting obligation called for in FATF Recommendation 15 to SR IV. The requirement to report transactions when there are reasonable grounds to suspect that the funds are derived from or intended for use in terrorist activity is an objective standard, which is consistent with the intent of Recommendation 15 although somewhat broader. In the context of SR IV, jurisdictions should establish a reporting obligation that may be based either on suspicion *or* on having reasonable grounds to suspect.



Appendix F: FATF Special Recommendation V

V. International cooperation

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 organizations. 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 organizations, and should have procedures in place to extradite, where possible, such individuals.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)

This recommendation contains five elements:

- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions through *mutual legal assistance mechanisms*.
- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions by means *other than through mutual legal assistance mechanisms*.
- Jurisdictions should have specific measures to permit the denial of “safe haven” to individuals involved in terrorist financing.
- Jurisdictions should have procedures that permit the extradition of individuals involved in terrorist financing.
- Jurisdictions should have provisions or procedures to ensure that “claims of political motivation are not recognized as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing.”

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 [Self Assessment Questionnaire on Terrorist Financing] between international cooperation through *mutual legal assistance mechanisms* on the one hand and information exchange through means *other than through mutual legal assistance*.

For the purposes of SR V, the term *mutual legal assistance* means the power to provide a full range of both noncoercive 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).

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 (MOU), exchanges of letters, and so on.

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>.

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.



Appendix G: FATF Special Recommendation VI

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 NBFIs. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil, or criminal sanctions.

INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION VI: ALTERNATIVE REMITTANCE

General

- 1) Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.
- 2) Special Recommendation VI consists of three core elements:
 - a) Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems.
 - b) Jurisdictions should ensure that money/value transmission services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (2003) (in particular, Recommendations 4–6 and 21–25) and the Eight Special Recommendations¹⁰ (in particular SR VII).

¹⁰ After the ninth special recommendation was added in 2004, it is now FATF Nine Special Recommendations.

- c) Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without a license or registration and that fail to comply with relevant FATF Recommendations.

Scope and Application

- 3) For the purposes of this recommendation, the following definitions are used.
- 4) *Money or value transfer service* refers to a financial service that accepts cash, checks, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, or transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third-party final payment.
- 5) A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through NBFIs or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (or parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala*, *hundi*, *fei-chien*, and the *black market peso exchange*.¹¹
- 6) *Licensing* means a requirement to obtain permission from a designated competent authority to operate a money/value transfer service legally.
- 7) *Registration* in this recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.
- 8) The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents, which must be made available to the designated competent authority. An *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

Applicability of Special Recommendation VI

- 9) Special Recommendation VI should apply to all persons (natural or legal), which conduct for or on behalf of another person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.

¹¹ The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.

- 10) Jurisdictions need not impose a separate licensing/registration system or designate another competent authority in respect to persons (natural or legal) already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF Forty Recommendations (2003) (in particular, Recommendations 4–16 and 21–25) and the Eight Special Recommendations (in particular SR VII).

Licensing or Registration and Compliance

- 11) Jurisdictions should designate an authority to grant licences and/or carry out registration and ensure that the requirement is observed. There should be an authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations (including the Eight Special Recommendations). There should also be effective systems in place for monitoring and ensuring such compliance. This interpretation of Special Recommendation VI (for example, the need for designation of competent authorities) is consistent with FATF Recommendation 23.

Sanctions

- 12) Persons providing money/value transfer services without a license or registration should be subject to appropriate administrative, civil, or criminal sanctions.¹² Licensed or registered money/value transfer services that fail to comply fully with the relevant measures called for in the FATF Forty Recommendations or the Eight Special Recommendations should also be subject to appropriate sanctions.

Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) (Extract)^{2†}

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.

¹² Jurisdictions may authorize temporary or provisional operation of money/value transfer services that are already in existence at the time of implementing this special recommendation to permit such services to obtain a license or to register.

[†] Please note that the reference to recommendations in the guidance note below refers to the 1996 version of the FATF 40 Recommendations.

- 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.

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.

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 NBFIs 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.

The term *informal money or value transfer system* also refers to a financial service whereby funds or value are moved from one geographic location to another. However, in some jurisdictions, these informal systems have traditionally operated outside the regulated financial sector in contrast to the “formal” money remittance/transfer services described in the preceding paragraph. Some examples of informal systems include the parallel banking system found in the Americas (often referred to as the “Black Market Peso Exchange”), the *hawala* or *hundi* system of South Asia, and the Chinese or East Asian systems. For more information on this topic, see the FATF-XI Typologies Report (3 February 2000), available through the FATF Web site at http://www.fatfgafi.org/FATDocs_en.htm#Trends, or the Asia Pacific Group Report on Underground Banking and Alternate Remittance Systems (18 October 2001), available through the APG Web site at http://www.apgml.org/content/typologies_reports.jsp.

Where *licensing or registrations 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 infor-

mal systems or networks. This corollary interpretation of SR VI (for example, the need for designation of competent authorities) is consistent with FATF Recommendation 26.

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 Web site (http://www.fatfgafi.org/40Recs_en.htm).



Appendix H: FATF Special Recommendation VII

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 monitoring of suspicious activity funds transfers that do not contain complete originator information (name, address and account number).

INTERPRETIVE NOTE TO SPECIAL RECOMMENDATION VII: WIRE TRANSFERS

Objective

- 1) Special Recommendation VII (SR VII) was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available (i) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (ii) to financial intelligence units for analyzing suspicious or unusual activity and disseminating it as necessary, and (iii) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions. Due to the potential terrorist financing threat posed by small wire transfers, countries should aim for the ability to trace all wire transfers and should minimize thresholds taking into account the risk of driving transactions underground. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system. The FATF will continue to monitor the impact of SR VII and conduct an assessment of its operation within three years of full implementation.

Definitions

- 2) For the purposes of this interpretive note, the following definitions apply.
- a) The terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
 - b) *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different countries. This term also refers to any chain of wire transfers that has at least one cross-border element.
 - c) *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same country. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the wire transfer may be located in another country.
 - d) The term *financial institution* is as defined by the FATF Forty Recommendations (2003). The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.
 - e) The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

Scope

- 3) SR VII applies, under the conditions set out below, to cross-border and domestic transfers between financial institutions.

Cross-border wire transfers

- 4) Cross-border wire transfers should be accompanied by accurate and meaningful originator information. However, countries may adopt a de minimus threshold (no higher than USD or EUR 1,000). For cross-border transfers below this threshold:
- a) Countries are not obligated to require ordering financial institutions to identify, verify record, or transmit originator information.
 - b) Countries may nevertheless require that incoming cross-border wire transfers contain full and accurate originator information.
- 5) Information accompanying qualifying cross-border wire transfers must always contain the name of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included.

- 6) Information accompanying qualifying wire transfers should also contain the address of the originator. However, countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.
- 7) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be exempted from including full originator information, provided they include the originator's account number or unique reference number (as described in paragraph 8), and the batch file contains full originator information that is fully traceable within the recipient country.

Domestic wire transfers

- 8) Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, financial institutions need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator.
- 9) The information must be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate authorities. Law enforcement authorities should be able to compel immediate production of such information.

Exemptions from SR VII

- 10) SR VII is not intended to cover the following types of payments:
 - a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, and the necessary information should be included in the message.
 - b) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

ROLE OF ORDERING, INTERMEDIARY, AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

- 11) The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the standards set out in the FATF Forty Recommendations (2003).

Intermediary financial institution

- 12) For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.
- 13) Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

Beneficiary financial institution

- 14) Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SRVII standards.

Enforcement mechanisms for financial institutions that do not comply with wire transfer rules and regulations

- 15) Countries should adopt appropriate measures to monitor effectively the compliance of financial institutions with rules and regulations governing wire transfers. Financial institutions that fail to comply with such rules and regulations should be subject to civil, administrative, or criminal sanctions.

Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) (Extract)

This recommendation consists of three elements:

- Jurisdictions should require financial institutions to include originator information on funds transfers sent within or from the jurisdiction.
- Jurisdictions should require financial institutions to retain information on the originator of funds transfers, including at each stage of the transfer process.
- Jurisdictions should require financial institutions to examine more closely or to monitor funds transfers when complete originator information is not available.

For the purposes of SR VII, three categories of financial institutions are specifically concerned (banks, bureaux de change, and money remittance/transfer

services), although other financial services (for example, stockbrokers, insurance companies, and so on) may be subject to such requirements in certain jurisdictions.

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.

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 organizations, for example) and thus warrant eventual reporting to the competent authority.



Appendix I: FATF Special Recommendation IX

IX. Cash couriers

IX. Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate, and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and SR III, which would enable the confiscation of such currency or instruments.

INTERPRETIVE NOTE TO SR IX: CASH COURIERS

Objectives

- 1) FATF SR IX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures (i) to detect the physical cross-border transportation of currency and bearer negotiable instruments, (ii) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, (iii) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, (iv) to apply appropriate sanctions for making a false declaration or disclosure, and (v) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. Countries should implement SR IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.

Definitions

- 2) For the purposes of SR IX and this Interpretative Note, the following definitions apply.
- 3) The term bearer negotiable instruments includes monetary instruments in bearer form, such as traveler's checks; negotiable instruments (including checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including check, promissory notes, and money orders) signed, but with the payee's name omitted.¹³
- 4) The term currency refers to banknotes and coins that are in circulation as a medium of exchange.
- 5) The term physical cross-border transportation refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (i) physical transportation by a natural person, or in that person's accompanying luggage or vehicle, (ii) shipment of currency through containerized cargo, or (iii) the mailing of currency or bearer negotiable instruments by a natural or legal person.
- 6) The term false declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
- 7) The term false disclosure refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
- 8) When the term related to terrorist financing or money laundering is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations; or (ii) laundered proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

¹³ For the purposes of this Interpretative Note, gold, precious metals, and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals, or precious stones, it should consider notifying, as appropriate, the Customs Service, or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.

The types of systems that may be implemented to address the issue of cash couriers

- 9) Countries may meet their obligations under SR IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:
- a) Declaration system: The key characteristics of a declaration system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a preset, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the preset threshold is sufficiently low to meet the objectives of SR IX.
 - b) Disclosure system: The key characteristics of a disclosure system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

Additional elements applicable to both systems

- 10) Whichever system is implemented, countries should ensure that their system incorporates the following elements:
- a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.
 - b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.
 - c) Information obtained through the declaration/disclosure process should be available to the FIU either through a system whereby the FIU is notified about suspicious cross-border transportation incidents or by making the declaration/disclosure information directly available to the FIU in some other way.
 - d) At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration, and other related authorities on issues related to the implementation of SR IX.
 - e) In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of

money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

- f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with SR V and Recommendations 35–40. To facilitate such cooperation, in instances when (i) a declaration or disclosure which exceeds the maximum threshold of EUR/USD 15,000 is made, or (ii) where there is a false declaration or false disclosure, or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by the appropriate authorities. At a minimum, this information will cover: (i) the amount of currency or bearer negotiable instruments declared/disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

Sanctions

- 11) Persons who make a false declaration or disclosure should be subject to effective, proportionate, and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil, or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and SR III, which would enable the confiscation of such currency or bearer negotiable instruments.



Appendix J: FATF Special Recommendation VIII

VIII: Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Nonprofit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

- By terrorist organizations posing as legitimate entities
- To exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures
- To conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

Interpretive Note to Special Recommendation VIII: Nonprofit Organizations

INTRODUCTION

- 1) Nonprofit organizations play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated, however, that terrorists and terrorist organizations exploit the nonprofit organization sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organizations and operations. This misuse not only facilitates terrorist activity but also undermines donor confidence and jeopardizes the very integrity of nonprofit organizations. Therefore, protecting the nonprofit organization sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of nonprofit organizations.
- 2) Nonprofit organizations may be vulnerable to abuse by terrorists for a variety of reasons. Nonprofit organizations enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some nonprofit organizations have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the nonprofit organization and the country, NPOs may often be subject to little or no governmental oversight (for

example, registration, record keeping, reporting, and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees). Terrorist organizations have taken advantage of these characteristics of nonprofit organizations to infiltrate the sector and misuse nonprofit organization funds and operations to cover for or support terrorist activity.

OBJECTIVES AND GENERAL PRINCIPLES

- 3) The objective of SR VIII (SR VIII) is to ensure that nonprofit organizations are not misused by terrorist organizations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes. In this Interpretative Note, the approach taken to achieve this objective is based on the following general principles:
 - a) Past and ongoing abuse of the nonprofit organizational sector by terrorists and terrorist organizations requires countries to adopt measures both (i) to protect the sector against such abuse and (ii) to identify and take effective action against those nonprofit organizations that either are exploited by or actively support terrorists or terrorist organizations.
 - b) Measures adopted by countries to protect the nonprofit organization sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and with the general public that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all nonprofit organizations are integral to ensuring the sector cannot be misused for terrorist financing.
 - c) Measures adopted by countries to identify and take effective action against nonprofit organizations that either are exploited by or actively support terrorists or terrorist organizations should aim to prevent and prosecute as appropriate terrorist financing and other forms of terrorist support. Where nonprofit organizations suspected of or implicated in terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should to the extent reasonably possible avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by nonprofit organizations.

- d) Developing cooperative relationships among the public, private, and nonprofit organization sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on and information sharing in the nonprofit organization sector to address terrorist financing related issues.
- e) A targeted approach in dealing with the terrorist threat to the nonprofit organization sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each jurisdiction.
- f) Flexibility in developing a national response to terrorist financing in the nonprofit organization sector is also essential to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

- 4) For the purposes of SR VIII and this interpretative note the following definitions apply:
 - a) The term *nonprofit organization* refers to a legal entity or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social, or fraternal purposes, or for the carrying out of other types of “good works.”
 - b) The terms FIU, legal arrangement, and legal person are as defined by the FATF Forty Recommendations (2003) (the FATF Recommendations).
 - c) The term funds is as defined by the Interpretative Note to FATF Special Recommendation II.
 - d) The terms freezing, terrorist, and terrorist organization are as defined by the Interpretative Note to FATF Special Recommendation III.
 - e) The term appropriate authorities refers to competent authorities, self-regulatory bodies, accrediting institutions, and other administrative authorities.
 - f) The term *beneficiaries* refers to those natural persons, or groups of natural persons who receive charitable, humanitarian, or other types of assistance through the services of the nonprofit organization.

MEASURES

- 5) Countries should undertake domestic reviews of their nonprofit organization sector or have the capacity to obtain timely information on its activities, size, and other relevant features. In undertaking these assessments, countries should use all available sources of information to identify features and types of nonprofit organizations, which by virtue of their activities or characteristics, are at risk of being misused for terrorist financing.¹⁴ Countries should also

¹⁴ For example, such information could be provided by regulators, tax authorities, FIUs, donor organizations, or law enforcement and intelligence authorities.

periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

- 6) There is a diverse range of approaches in identifying, preventing, and combating terrorist misuse of nonprofit organizations. An effective approach, however, is one that involves all four of the following elements: (a) outreach to the sector, (b) supervision or monitoring, (c) effective investigation and information gathering, and (d) effective mechanisms for international cooperation. The following measures represent specific actions that countries should take with respect to each of these elements to protect their nonprofit organization sector from terrorist financing abuse.

a) ***Outreach to the nonprofit sector concerning terrorist financing issues***

- (i) Countries should have clear policies to promote transparency, integrity, and public confidence in the administration and management of all nonprofit organizations.
- (ii) Countries should encourage or undertake outreach programs to raise awareness in the nonprofit organization sector about the vulnerabilities of nonprofit organizations to terrorist abuse and terrorist financing risks, and the measures that nonprofit organizations can take to protect themselves against such abuse.
- (iii) Countries should work with the nonprofit organization sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.¹⁵
- (iv) Countries should encourage nonprofit organizations to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

b) ***Supervision or monitoring of the nonprofit organization sector***

Countries should take steps to promote effective supervision or monitoring of their nonprofit organization sector. In practice, countries should be able to demonstrate that the following standards apply to nonprofit organizations which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector's international activities.

- (i) Nonprofit organizations should maintain information on (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information

¹⁵ The FATF's Combating the Abuse of Nonprofit Organizations: International Best Practices provides a useful reference document for such exercises.

should be publicly available either directly from the nonprofit organization or through appropriate authorities.

- (ii) Nonprofit organizations should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.
- (iii) Nonprofit organizations should be licensed or registered. This information should be available to competent authorities.¹⁶
- (iv) Nonprofit organizations should have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the nonprofit organization's stated activities.
- (v) Nonprofit organizations should follow a "know your beneficiaries and associate nonprofit organizations¹⁷" rule, which means that the nonprofit organization should make best efforts to confirm the identity, credentials and good standing of their beneficiaries and associate nonprofit organizations. Nonprofit organizations should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.
- (vi) Nonprofit organizations should maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organization. This also applies to information mentioned in paragraphs (i) and (ii) above.
- (vii) Appropriate authorities should monitor the compliance of nonprofit organizations with applicable rules and regulations.¹⁸ Appropriate authorities should be able to properly sanction relevant violations by nonprofit organizations or persons acting on behalf of these nonprofit organizations.¹⁹

c) *Effective information gathering and investigation*

- (i) Countries should ensure effective cooperation, coordination, and information sharing to the extent possible among all levels of appropriate authorities or organizations that hold relevant information on nonprofit organizations.

¹⁶ Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, nonprofit organizations are already registered with tax authorities and monitored in the context of qualifying for favorable tax treatment (such as tax credits or tax exemptions).

¹⁷ The term associate nonprofit organizations includes foreign branches of international nonprofit organizations.

¹⁸ In this context, rules and regulations may include rules and standards applied by self-regulatory bodies and accrediting institutions.

¹⁹ The range of such sanctions might include freezing of accounts, removal of trustees, fines, decertification, de-licensing, and deregistration. This should not preclude parallel civil, administrative, or criminal proceedings with respect to nonprofit organizations or persons acting on their behalf where appropriate.

- (ii) Countries should have investigative expertise and capability to examine those non-profit organisations suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations.
- (iii) Countries should ensure that full access to information on the administration and management of a particular non-profit organisation (including financial and programmatic information) may be obtained during the course of an investigation.
- (iv) Countries should establish appropriate mechanisms to ensure that when there is suspicion or reasonable grounds to suspect that a particular non-profit organisation: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with all relevant competent authorities in order to take preventive or investigative action.

d) ***Effective capacity to respond to international requests for information about an non-profit organisation of concern***

Consistent with SR V, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular non-profit organisations suspected of terrorist financing or other forms of terrorist support.

Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) (Extract)

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 organizations, to prevent their misuse for terrorist financing purposes.
- 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.

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.

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 organized 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.

In the SAQTF, the term *off-shore 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.

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*, and so on.



Answers

Module 6 Answers

Answer 1

The financing of terrorism is providing financial support for terrorism or for those who encourage, plan, or engage in terrorism. The source of terrorist financing may be legitimate, in contrast to the source of laundered money. CFT efforts are aimed at impeding terrorist financing. (See section 1.3 in Module 1: What is terrorist financing and how does it contrast with money laundering?)

Answer 2

The answer is (c). The main difference between money laundering and terrorist financing is that terrorist financing may come from legitimate sources, such as donations to charities, as well as illegitimate sources. By contrast, money laundering involves only ill-gotten funds obtained by illicit acts.

Answer 3

Terrorist financing not only poses a threat to security; it also undermines economic prosperity and poses a long-term threat to development by diverting money from productive to unproductive uses, damaging the country's reputation in the eyes of investors and tourists, and generating crime and corruption. It can have a devastating impact on stability, transparency, and the efficiency of financial systems. (See section 2 in Module 1: The implications of money laundering and terrorist financing for development.)

Answer 4

In reality all of these characteristics are part of a weak AML/CFT regime. (See section 2 in Module 1: The implications of money laundering and terrorist financing for development.) Countries have a great deal of flexibility in meeting the international AML/CFT standards. Among the few universal requirements are ratification and implementation of the Vienna and Palermo Conventions, criminalization of money laundering and terrorist financing, and implementation of procedural measures, such as laws that allow for freezing and confiscation. (See section 2, in Module 2: What legal and institutional arrangements satisfy international standards.) Otherwise, it is up to each country to adopt laws that are consistent with its own domestic legal system. (See section 4 in Module 2: Where can one find model laws?)

It is also up to each country to designate the "competent authorities" that supervise financial institutions and other non-financial businesses and professions. Given the wide scope of financial institutions, it is likely that countries will need

to create more than one supervisory body. (Review the country examples presented in Section 1 in Module 3: Responsibility for effective supervision.)

Answer 5

No. The terms of the SFT Convention do not leave room for any such justification. According to Article 6 of the Convention, states should “ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious, or other similar nature.”

Answer 6

No. Although people disagree on what terrorism is, there is general agreement about what it is *not*. The right to strike is not in question. Nor is peaceful demonstration. Some jurisdictions have decided to insert expressly in their CFT legislation exceptions for this type of political activity.

Answer 7

This is a key issue blocking the adoption of a definition of terrorism for the draft United Nations comprehensive convention on international terrorism. So far, no exception of this type has been inserted in the draft. But it is safe to say that groups struggling against foreign occupation will have to comply with humanitarian law (for example, protection of civilians). In addition, an armed conflict, even noninternational, is not justification for armed groups to commit terrorist acts.

Answer 8

The acts committed by the Liberation Front of Valachia are terrorist acts. Bombing infrastructure endangers civilians and is clearly a situation covered by the SFT Convention. Providing financial support for such acts is financing terrorism. By contrast, there is no reason to consider the Free Valachia party as an organization that has committed terrorist acts. Individuals must have the right to exercise their right to demonstrate and their right of free speech through a political party. Unless it can be proved that the party has financed specific terrorist acts, a terrorist, or a terrorist organization, international standards on the financing of terrorism may not apply.

Answer 9

The fact that a country has already adopted legislation on terrorism does not mean that no further steps need to be taken at the domestic level to ensure the efficiency of the legal framework for combating terrorist financing. The fact that Al-Qaeda and connected groups have not attacked the country and that evidence of terrorist financing has not yet been reported is not a valid reason for not acting. Rurithania should ratify the SFT Convention and ensure that its

national legislation and legal framework enable it to comply with international rules and standards on combating the financing of terrorism.

Answer 10

Yes. If the intentional element described above is present, the simple fact of collecting funds constitutes the criminal offense of financing terrorism under FATF Special Recommendation II. It is not relevant whether the funds collected were actually used to carry out a terrorist act or whether they were connected to a particular terrorist act.

Answer 11

Yes. The SFT Convention is very clear on this issue. The attempt to commit an offense of financing terrorism is also an offense for the purpose of the SFT Convention (Article 2.4).

Answer 12

Yes. Financing terrorism is a criminal offense even if the offenders are located in another jurisdiction. The extraterritorial dimension of terrorist activities cannot be a pretext for doing nothing. There is no doubt that states must criminalize the financing of terrorism on their territory. It should be equally clear that when a national of country A commits the offense of financing terrorism on the territory of country B, that action should be a prosecutable offense under the legislation of country A. (See article 7 of the SFT Convention for other extraterritorial situations and paragraph 1.b of Resolution 1373 (2001).

Answer 13

According to the SFT Convention, the offense of financing of terrorism should be punishable by appropriate penalties (Article 4.2). Actually, the convention and the Resolution 1373 (2001) stress the fact that the offense of financing terrorism has a “grave nature” or is a “serious criminal offense” (Resolution Paragraph 2.e). This standard leaves to each party the right to define the exact penalties entailed by the acts of financing of terrorism. Examples of penalties are long-term imprisonment, punitive fines, withdrawal or suspension of business licenses, or suspension or removal of management or directors of legal entities.

The SFT Convention requires of states that legal entities (such as shell banks and international corporations) located on their territory or organized under their laws must be held liable when an individual responsible for management or control of the entity has, in that capacity, committed an offense of financing terrorism. In addition, if cash is transported across borders and used in terrorist financing, states are required by FATF SR IX on cash couriers to adopt confiscation measures (see section 13).

Answer 14

The financing of terrorism must be considered a predicate offense of money laundering. In the many legal systems where the financing of terrorism is already considered a serious crime, the law on money laundering—which applies to the laundering of the proceeds of *serious crimes*—will automatically cover the financing of terrorism among the predicate offenses of money laundering. In countries that maintain a list of the predicate offenses of money laundering, terrorist financing must be added to the list.

Answer 15

The answer is (d). The SFT Convention refers only to “funds” of terrorists. FATF SR III, on the other hand, covers “funds and other assets.” In the same vein, Resolution 1373 (2001) requires broadly the seizure of “funds and other financial assets or economic resources of a person.” But looking at the definition of funds in the SFT Convention, it appears that the three instruments have similar coverage. A state may not interpret the term “funds” restrictively in order to exclude other forms of property from the scope of the international obligations.

Answer 16

True: Measures for freezing and confiscation of terrorists’ assets should proceed in accordance with national legislation and in conformity with human rights and international obligations. For example:

- a) States should allow persons whose funds have been frozen to challenge the measure in court.
- d) States should have procedures for considering requests to be removed from lists of suspected terrorists and to unfreeze the assets of de-listed persons.
- e) States should ensure that the rights of third parties acting in good faith are not impaired by the freezing of assets.
- f) States should authorize access to funds frozen pursuant to Resolution 1267 (1999) if access is needed to cover basic expenses or certain fees recognized under Resolution 1452 (2002).

Answer 17

No. There is no room for a political exception.

Answer 18

True. The scope of the obligation may vary from state to state depending on the international instruments it has accepted. But as a matter of principle, states are bound to provide assistance in the suppression of terrorist financing.

Answer 19

The answer is (d). Exchange of information may occur on the basis of a bilateral or multilateral treaty, or under the terms of domestic legislation. Less formal methods, such as a memorandum of understanding among agencies, may be preferred by the parties.

Answer 20

The answer is (d). According to the World Bank, workers' remittances have climbed steadily since 1998, reaching US\$93 billion in 2003, up 20 percent from 2001. They are now the second most important financial flow to developing countries after foreign direct investment. Remittances are almost twice as great as flows of official aid. (Source: *Global Development Finance 2004*.)

Answer 21

The answer is (b). If a bank receives a wire transfer from a bank located in a foreign country that does not contain the name or address of the originator of the wire, it should consider this omission as a cause for concern. The standard of enhanced scrutiny, and FATF SR IV, oblige banks to have in place a mechanism for monitoring and detecting suspicious transactions.

Answer 22

The answer is (d). When bank A receives an international wire transfer from foreign bank B through a financial intermediary and that transfer does not contain meaningful originator information, it is the duty of bank A to give the transfer the same enhanced scrutiny that it would give to a direct wire. That a correspondent bank was involved does not change this. FATF SR VII underlines the importance of retaining the wire information through the entire chain of payment. But this requirement does not relieve the bank at the end of the payment chain from its duty to monitor possible suspicious transactions.

Answer 23

No. Gold, other precious metals, and precious stones are not among the assets considered as cash equivalents, despite their high liquidity and their use in certain situations as a means of exchange or of transmitting value. But the cross-border transportation of these items may be subject to other control mechanisms established by customs laws and regulations.

Answer 24

Yes. Although SR IX does not mention it expressly, the accompanying Interpretative Note makes it clear that state agencies responsible for implementing a declaration or disclosure system should be entitled to request further informa-

tion on the origin of cash from a person who provides false information in the course of carrying it across a border. This power is necessary if the monitoring process is to be effective.

Answer 25

FATF SR VIII does not suggest that countries should crack down on the entire nonprofit sector. The vast majority of charities provide important services to their communities; for that reason, states should balance the pros and cons of oversight mechanisms to avoid interference with legitimate charitable activities.

FATF Best Practice explains “the charitable sector is a vital component of the world economy and of many national economies and social systems that complements the activity of the governmental and business sectors in supplying a broad spectrum of public services and improving quality of life. We wish to safeguard and maintain the practice of charitable giving and the strong and diversified community of institutions through which it operates.”

Answer 26

FATF SR VIII does not impose a single oversight model. States retain the flexibility to choose the best means of achieving the goal set by the standard. Measures should be based on an objective assessment of the risks of abuse. Thus, considerations of religion, per se, should not interfere with the level of oversight.

Answer 27

Oversight of charities should focus on the financial operations of the organizations in question. Greater scrutiny would be recommended in the case of disbursements to foreign recipients. In such cases, there is a clear risk that charities are being used to finance international terrorist activities.

For the U.S. guidelines on this topic, see U.S. Department of the Treasury, *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities*.

Answer 28

Terrorism—the financing of terrorism—collecting

Answer 29

The correct assertions are (a), (c), and (d).

Answer 30

States—individuals—organizations or entities—lists

Answer 31

No. In addition to ratifying the SFT Convention states must implement the convention in their national legal system. States also should ensure that they comply with the mandatory terms of relevant UN Security Council resolutions and should take the necessary measures for implementing the FATF Special Recommendations.

Answer 32

Yes. This is supported by the instruments cited above. States should criminalize offenses committed abroad by their nationals as well as those committed on their territory.

Answer 33

The answer is (b).

Answer 34

stones—metals—anti—money laundering—reasonable grounds

Answer 35

False. The duty of states to cooperate pertains not only to criminal procedures but also to civil enforcement and administrative investigations related to the fight against the financing of terrorism.

Answer 36

Assertion (b) is most accurate.

Answer 37

True

Money laundering and the financing of terrorism are global problems that not only threaten a country's security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than \$1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The *Combating Money Laundering and the Financing of Terrorism* training program was developed by the World Bank's Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide's modules are:

- Module 1:** Effects on Economic Development and International Standards
- Module 2:** Legal Requirements to Meet International Standards
- Module 3a:** Regulatory and Institutional Requirements for AML/CFT
- Module 3b:** Compliance Requirements for Financial Institutions
- Module 4:** Building an Effective Financial Intelligence Unit
- Module 5:** Domestic (Inter-Agency) and International Cooperation
- Module 6: Combating the Financing of Terrorism**
- Module 7:** Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering's Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction's AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.

