



United Nations

COUNTER-TERRORISM

IMPLEMENTATION TASK FORCE

CTITF

CTITF Working Group Report

Tackling the Financing of Terrorism

**CTITF
PUBLICATION
SERIES**

**OCTOBER
2009**

[blank inside cover]

CTITF Working Group Report

Tackling the Financing of Terrorism



UNODC

United Nations Office on Drugs and Crime

**The World Bank
International Monetary Fund
United Nations Office on Drugs and Crime**

With the support of:

**Counter-Terrorism Committee Executive Directorate
Monitoring Team of the 1267 Committee
INTERPOL**



United Nations
New York, 2009

About the United Nations Counter-Terrorism Implementation Task Force

The United Nations Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 to ensure overall coordination and coherence in the counter-terrorism efforts of the United Nations system. CTITF is chaired by a senior United Nations official appointed by the Secretary-General and consists of 25 United Nations system entities and INTERPOL.

The United Nations Global Counter-Terrorism Strategy, which brings together into one coherent framework decades of United Nations counter-terrorism policy and legal responses emanating from the General Assembly, the Security Council and relevant United Nations specialized agencies, has been the focus of the work of CTITF since its adoption by the General Assembly in September 2006 (General Assembly resolution 60/288).

The Strategy sets out a plan of action for the international community based on four pillars:

- Measures to address the conditions conducive to the spread of terrorism;
- Measures to prevent and combat terrorism;
- Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard;
- Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism.

In accordance with the Strategy, which welcomes the institutionalization of CTITF within the United Nations Secretariat, the Secretary-General in 2009 established a CTITF Office within the Department of Political Affairs to provide support for the work of CTITF. Via the CTITF Office, with the help of a number of thematic initiatives and working groups, and under the policy guidance of Member States through the General Assembly, CTITF aims to coordinate United Nations system-wide support for the implementation of the Strategy and catalyse system-wide, value-added initiatives to support Member State efforts to implement the Strategy in all its aspects. CTITF will also seek to foster constructive engagement between the United Nations system and international and regional organizations and civil society on the implementation of the Strategy.

United Nations
Department of Political Affairs
Counter-Terrorism Implementation Task Force
New York, NY 10017

Website: www.un.org/terrorism/cttaskforce

Contents

Acronyms	iv
Introduction	1
Chapter 1. General Application of Combating the Financing of Terrorism Measures	3
Chapter 2. Criminalizing Terrorism Financing	5
Chapter 3. Enhancing Domestic and International Cooperation	7
A. Effectiveness of financial intelligence units	7
B. Public sector cooperation	8
C. Collaboration with the private sector	9
Chapter 4. Value Transfer Systems	11
A. The need for terrorism financing indicators	11
B. Vulnerabilities in the wire transfer system	12
C. Cash couriers	12
D. Alternative remittance systems	13
E. Emerging technologies	14
Chapter 5. Non-Profit Organizations	16
Chapter 6. Freezing of Assets	19
A. Improving listing quality and legitimacy	20
B. Improving outreach to stakeholders	22
C. Coordinating before listing	22
Report Contributors	25

Acronyms

AML	anti-money laundering
ARS	alternative remittance systems
CFT	combating the financing of terrorism
CTED	Counter-Terrorism Committee Executive Directorate
CTITF	Counter-Terrorism Implementation Task Force
FIU	financial intelligence unit
FATF	Financial Action Task Force
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organization
MT	Monitoring Team of the 1267 Committee
NPO	non-profit organization
TF	terrorism financing
UNODC	United Nations Office on Drugs and Crime
WG	Working Group

Introduction

In the *United Nations Global Counter-Terrorism Strategy (General Assembly resolution 60/288)*, adopted by consensus by all Member States on 8 September 2006, the General Assembly highlighted the importance of addressing the financing of terrorism and the need for Member States to implement comprehensive measures that meet all international standards.

The Counter-Terrorism Implementation Task Force, a coordinating and information-sharing body consisting of 25 entities from the United Nations system and other international organizations, established a Working Group on Tackling the Financing of Terrorism to assist States in this regard. The Working Group is led by the International Monetary Fund (IMF), the World Bank and the United Nations Office on Drugs and Crime (UNODC), and supported by the Monitoring Team of the 1267 Committee (MT), the Counter-Terrorism Committee Executive Directorate (CTED) and the International Criminal Police Organization (INTERPOL).

The Working Group aims to examine the various components of strategies tackling the financing of terrorism and make proposals that would contribute to increasing the effectiveness of the implementation by Member States of international standards, including the Financial Action Task Force (FATF) *Special Recommendations*.

In order to meet this objective, the Working Group has taken stock of compliance with international standards for combating the financing of terrorism by:

(1) A review of available literature on implementation by Member States of international standards for combating the financing of terrorism. The standards considered included those set forth in relevant Security Council resolutions, the *International Convention for the Suppression of the Financing of Terrorism* and the nine *FATF Special Recommendations*;

(2) A review of statistical data and other relevant information regarding the implementation, and obstacles to implementation, of international standards for combating the financing of terrorism by UNODC, the World Bank and IMF, with the assistance of the MT and CTED;

(3) Solicitation of input from a range of experts within a variety of sectors/communities, including on new ideas for effective implementation of international standards.

In this regard, eight round-table discussions with a range of experts across a variety of sectors and communities involved in combating terrorism financing were held. These were:

- Bankers group: February 2007;
- Financial intelligence units: April 2007;
- Regulators: April 2007;
- Intelligence agents—general: April 2007;
- Law enforcement: May 2007;
- Criminal justice officials: May 2007;
- Intelligence agents—Asia focus: April 2008;
- Multidisciplinary review: August 2008.

The findings and recommendations contained in this report reflect a distillation of nearly two years of review and analysis by the Working Group. The findings and recommendations are organized into five broad areas: (i) the criminalizing of terrorist financing; (ii) the enhancement of domestic and international cooperation; (iii) value transfer systems; (iv) non-profit organizations; and (v) the freezing of assets. The members of the Working Group, each within their respective mandates, will follow up in the period ahead on the findings and recommendations set forth in this report.

CHAPTER 1

General Application of Combating the Financing of Terrorism Measures

Background

1. Substantial progress has been achieved in understanding the phenomenon of terrorism financing and in articulating and implementing the measures necessary to address it. Terrorism financing incorporates the distinct activities of fund-raising, storing and concealing funds, using funds to sustain terrorist organizations and infrastructure, and transferring funds to support or carry out specific terrorist attacks. Funds used to support terrorism may be generated through legal or illegal means, and legitimate humanitarian or business organizations may be used unwittingly or knowingly as a channel for financial or other logistical support to terrorism.
2. Financial transactions can yield valuable intelligence that may be unavailable from other sources. Yet, detecting illicit financial activity, including terrorism financing, is difficult in the formal financial system and even more difficult outside of it. Targeted financial sanctions (including, in particular, the freezing of assets) against persons and entities suspected of providing financial support to terrorism have proved effective, but they need to be balanced with the need to track terrorist funds movements to gather intelligence on the scope of the terrorist network.
3. Furthermore, combating the financing of terrorism (CFT) measures have raised legal, institutional, political and human rights issues that are not fully resolved. This is perhaps best illustrated by recent court rulings that have called into question the procedural safeguards in the designation of persons for financial sanctions. Finding solutions to these issues remains central to maintaining the effectiveness of the system in the long run.
4. Authorities should exercise caution not to introduce laws or regulations burdening private and public sector stakeholders in the name of countering the financing of terrorism without sufficient evidence or typologies that the burden is proportionate to the risk.

5. **Finding:** Regional vulnerabilities, trends and priorities have an impact on the way in which the international standards are implemented.
6. **Recommendation:** The international community should afford greater recognition and deference to the work of the regional bodies in supporting and mediating the implementation of the international standards to the local context, in particular in the determination of risks and vulnerabilities of a country to terrorism and the financing of terrorism.
7. **Recommendation:** Proportional measures, commensurate to the risks, should be applied when considering the effectiveness or adequacy of major CFT regulations. This approach should be applied at both national and international levels, and officials should be prepared to adjust regulation where necessary.

CHAPTER 2

Criminalizing Terrorism Financing

Background

8. When the criminalization of terrorism financing was first addressed in an international instrument through the *International Convention for the Suppression of the Financing of Terrorism* in 1999, drafters were faced with the challenge of establishing a regime that would criminalize the funding of an act that had not been previously defined in a comprehensive manner. Making the financing of terrorism a legal offence separate from the actual terrorism act itself gives authorities much greater powers to prevent terrorism.
9. The Financial Action Task Force (FATF) *40 Recommendations on Money Laundering and 9 Special Recommendations on Terrorist Financing*¹ are recognized under *Security Council resolution 1617 (2005)* and the *Plan of Action* annexed to *General Assembly resolution 60/288 (2006)* as important tools in the fight against terrorism. The *40 + 9 Recommendations* are a comprehensive set of measures for an effective national regime to fight money laundering and terrorism financing. They call for the criminalization of the financing of terrorism in accordance with the *International Convention for the Suppression of the Financing of Terrorism*, among other actions.
10. **Finding:** Terrorist acts (and their financing) are perceived by some as being politically justified by their goals. This perception erodes political will to address terrorism financing, distracts attention from the fact that it is a crime, and impedes the effectiveness of international and national efforts to combat terrorism and its financing.

¹ In April 1990, the FATF issued a set of 40 Recommendations for improving national legal systems, enhancing the role of the financial sector and intensifying cooperation in the fight against money laundering. These Recommendations were revised and updated in 1996 and in 2003 in order to reflect changes in money-laundering techniques and trends. The FATF extended its mandate in October 2001 to cover the fight against terrorist financing and issued eight Special Recommendations on combating the financing of terrorism. A ninth Special Recommendation was adopted in October 2004. The FATF Recommendations can be accessed at <http://www.fatf-gafi.org>.

11. **Recommendation:** Terrorism is a form of criminality and should be addressed as such. Terrorism financing is thus a form of supporting and facilitating criminal behaviour. The *International Convention for the Suppression of the Financing of Terrorism* provides key standards. So far as this is commonly understood, enforcement efforts will receive the support of the public, which they need in order to be effective. All States are encouraged to sign it and comply with its terms.
12. **Finding:** It is difficult to determine the effectiveness of legislation criminalizing terrorism financing partly because a presumed preventive effect is by definition not measurable but also because terrorism financing provisions have been introduced only recently.
13. **Recommendation:** In order to build knowledge of what countries have done in terms of adopting measures to combat the financing of terrorism, an inventory should be made of the available criminal laws, administrative measures and implementation. It should be designed from existing standards of assessment. Such work might best be led by regional organizations or international financial institutions, acting within their respective mandates, which have already gathered much relevant information on States' measures to combat terrorism financing.
14. **Recommendation:** A broader set of indicators—beyond the number of prosecutions, investigations and convictions, or amount of assets or proceeds being frozen and/or confiscated under terrorism financing criminal laws—should be considered to assess effectiveness. Specifically, an assessment of effectiveness in any given jurisdiction should include an evaluation of which legal tools have been used effectively and which have not.

CHAPTER 3

Enhancing Domestic and International Cooperation

Background

15. Domestic and international cooperation works best when all of the relevant agencies involved in an initiative are operating on a shared understanding of “terrorism financing”, a common agenda and as much shared information as possible. A fully effective local and global effort to combat terrorism financing benefits from well-functioning, transparent and corruption-free economies that are equipped with appropriate anti-money laundering (AML) legal, regulatory and institutional frameworks. It also benefits from the institutional capacity to enforce laws and to collect, analyse and share real-time intelligence and documentary evidence within and across national borders. Properly trained financial intelligence experts are critical to making the regime effective. This includes financial intelligence unit personnel, criminal investigators, prosecutors, judges, regulators, customs officers and financial institution employees.
16. However, building this institutional capacity is difficult and expensive, and it requires sustained political commitment. Complexity arises from the problems associated with achieving and sustaining cooperation among diverse public and private actors. Many countries have encountered difficulties in putting in place legal, administrative and institutional arrangements for various reasons, including legal traditions and resource constraints. International cooperation initiatives, such as training of new personnel in one country by experienced staff in another, can constitute a key contribution to enhancing the capacity of relevant domestic agencies, such as financial intelligence units (FIUs), and to strengthening the CFT regime.

A. Effectiveness of financial intelligence units

17. **Finding:** Various assessor bodies have found that many essential domestic agencies, in particular FIUs, are undertrained and understaffed and lack a clear mandate and powers to deal with terrorism financing issues. In order to build an effective global CFT regime and public-private partnerships in this

area, well-developed domestic agencies with carefully designed mandates and powers are essential.

18. **Recommendation:** Where they exist, these deficiencies should be remedied on a priority basis. This should be handled through strengthening the FIU or alternative mechanisms with a similar function.

B. Public sector cooperation

19. **Finding:** It is difficult to assess the effectiveness of national coordination and international cooperation measures currently in place. To date, there has not been much research into identifying all of the impediments in national systems that hamper international cooperation.
20. **Recommendation:** To enhance domestic cooperation, States should ensure that they have a domestic policy-coordinating mechanism and that it works effectively.
21. **Recommendation:** Relevant international bodies and institutions, acting within their respective mandates, and Governments should conduct research with a view to identifying and removing obstacles to national coordination and international cooperation and assist affected States in finding appropriate and timely formal and informal remedies.
22. **Finding:** In some cases of suspected terrorism financing, States are not using effectively all the legal tools included in conventions that are available for mutual legal assistance and extradition.
23. **Recommendation:** An appropriate agency of the United Nations should undertake an assessment of the use of mutual legal assistance and extradition provisions in terrorism financing cases and then make recommendations on steps States could take to use them more effectively.
24. **Finding:** States that are most effective in cooperating both among domestic institutions and authorities and with their foreign counterparts are those with an established coordinating mechanism or a central coordinating body. Pre-conditions for effective cooperation include the identification of counterparts, mutual trust and well-understood and respected procedures for protecting the confidentiality of information.
25. **Recommendation:** For both international and domestic cooperation, States should take steps to increase their capacity to cooperate with, and their level of trust in, counterparts. This can be done through such measures as increasing the number of secondments and staff exchanges, having a forum for

counter-terrorism financing practitioners to meet regularly, clarifying information exchange procedures (including clear rules on disclosure to third parties) and training relevant staff.

26. **Recommendation:** It should be permissible under national legislation for competent authorities to utilize and develop informal mechanisms of cooperation that include lessons learned and best practices. These best practices on designing and utilizing mechanisms for informal information exchanges should be disseminated, and States should be encouraged to consider them. These can then be considered for international cooperation under bilateral, regional and United Nations instruments.

C. Collaboration with the private sector

27. **Finding:** Regulation can impede cooperation with the private sector and even within specific firms. For instance, branches of the same bank in different jurisdictions may not always be able to ascertain whether they are permitted to share information with one another and thus often err on the side of caution by not sharing information that could improve their efficiency and effectiveness in detecting and reporting suspicious activity.
28. **Recommendation:** An inventory of the difficulties encountered by the private sector in implementing the terrorism financing provisions should be developed to enhance mutual understanding and build confidence between the private sector and the competent authorities.
29. **Recommendation:** Competent authorities should issue guidance to the private sector that clearly states what forms of information sharing are allowed and which ones are not, and such guidance should address the requirements of both national and international information sharing.
30. **Recommendation:** Steps should be taken to enable financial institutions to share information on suspicious activity more easily both (a) between and among institutions operating within a given jurisdiction and (b) across borders among branches and affiliates of particular firms. This should be done in consideration of national laws with regard for due process of law and privacy rights.
31. **Finding:** Financial institutions' risk mitigation controls are highly driven by prudential concerns. The private sector, because of the perceived risks associated with exercising discretion, may interpret and apply regulations without regard to its own financial sector expertise. For example, overly strict regulations that do not allow a discretionary, risk-based approach can prevent

financial institutions from engaging in business with certain types of clients sometimes identified by regulators as high risk, such as non-profit organizations and money transfer operators. Denying access to formal financial channels to those players, or rendering it considerably more difficult, is ultimately counterproductive.

32. **Recommendation:** More should be done to include the private sector in general and financial institutions in particular as partners in fighting the financing of terrorism. More specifically, competent authorities should provide more information and invite more feedback on the implementation, effectiveness and design of counter-terrorism financing measures. States, together with financial institutions, should seriously consider enabling the establishment of vetted units within those institutions to allow for their greater and earlier involvement in terrorism financing (TF) investigations as well as in the development of TF national strategy and policy.
33. **Recommendation:** Regular dialogue should be conducted between authorities and the private sector to facilitate the design and adoption of appropriate regulation. Regulation should carry sanctions for poor compliance and liability protections for good-faith non-compliant procedures.
34. **Finding:** With false identification, individuals can circumvent a range of CFT preventive measures taken by financial institutions and other reporting entities. Some States have enacted laws against the fraudulent use of identity documentation required by financial institutions, and used these laws effectively to prosecute persons suspected of money laundering, terrorism financing and other financial crimes.
35. **Recommendation:** Relevant international bodies and institutions, acting within their respective mandates, and States should take appropriate steps to prohibit persons from fraudulent use of identity documentation required by financial institutions or other reporting entities.

CHAPTER 4

Value Transfer Systems

Background

36. Terrorists and terrorist groups have many methods at their disposal to move funds around the world. They can use formal financial systems or unregulated channels, or simply move money across borders in cash. There is growing evidence that terrorist groups are exploiting vulnerabilities in the international trade system to move value for illegal purposes. Whether in the form of exogenous flows from private donors directed at terrorist networks, or that of funds being moved within the same organization, the transfer of value plays a fundamental role in bringing terrorists closer to their objectives. It also affords authorities the opportunity to detect terrorist activity, disrupt it and deter further terrorism financing.
37. Many people perceive that non-traditional methods of moving money present higher risk because they are to varying degrees unregulated. It is unclear, however, whether informal value transfer systems are any more vulnerable to criminal abuse than formal ones.
38. New technologies and other alternative systems have prompted countries to revise their regulatory framework. In this process, they have begun to address terrorism financing (and money laundering) risks. The Working Group has identified specific issues that arise from different value transfer systems and approaches for dealing with them.

A. The need for terrorism financing indicators

39. **Finding:** Financial institutions usually comply with AML/CFT requirements for recognizing and reporting suspicious activity. Concrete typologies and trend analysis provide them and other reporting entities with useful guidance for the detection of money laundering. However, there has been little rigorous research into the frequency and significance of particular terrorism financing *modi operandi*. Moreover, there are few indicators—other than “hits” on sanctions lists—available to assist reporting entities in recognizing that a suspicious activity is specifically related to terrorism financing.

40. **Recommendation:** While financial institutions continue to detect suspicious transactions and report them, competent authorities should bear the responsibility of analysing such transactions and determining whether they involve terrorism financing.
41. **Recommendation:** States and relevant international bodies, acting within their respective mandates, should redouble efforts to conduct rigorous quantitative and qualitative research in order to identify typologies and trends. They should also work to develop indicators (types of transactions, products and so on) that link suspicious transactions to terrorism financing. As much as possible, these indicators should be distinguished from those of money laundering. This would help competent authorities to offer proper guidance to financial institutions regarding suspicious activities reports relevant to terrorism financing. Such analysis could also assist States in ensuring that regulation is sound.

B. Vulnerabilities in the wire transfer system

42. **Finding:** The existing standards and practices for collecting information on the sender of wire transfers (originator information) have a loophole: not all banks follow the same requirements for providing information on a transaction's originator. The international bank fund transfer system comprises thousands of institutions in hundreds of jurisdictions, making bilateral agreements among all of them infeasible and attempts to guarantee payment standards with overseas counterparts impossible at a bank-to-bank level.
43. **Recommendation:** The Bank for International Settlements Basel Committee on Banking Supervision should continue its work to identify options for addressing this loophole.

C. Cash couriers

44. International funds movements are frequently accomplished by the physical transport of funds by individuals for both legal and unlawful purposes. As this method bypasses the use of wire transfers, wire transfer controls are ineffective for detecting the financing of terrorism via cash couriers. Mitigating the risks of physical cash movements requires efforts at national borders.
45. **Finding:** Border authorities do not always have the necessary tools or powers or the required training to effectively detect or disrupt the physical movement of cash across national borders for terrorism financing purposes.

46. **Recommendation:** States should, on the basis of a rational and objective risk assessment, build the capacity of border control agents to apply counter-terrorism financing measures. The risk assessment will help ensure that measures are proportionate to the risks and that they are effective.
47. **Recommendation:** States should ensure that cooperation between customs and FIU authorities is strengthened in order to optimize the use of intelligence collected at borders. Greater information to the FIU will facilitate its analysis and support to law enforcement as noted above.

D. Alternative remittance systems

48. Alternative remittance systems (ARS) can be broadly defined as “any system used for transferring money from one location to another, and generally operating outside the banking channels”.² Such a definition includes a wide array of channels, ranging from large, fully regulated multinational companies to small, covert value transfer outlets operating incognito. Increasingly, attention has been focused on the latter type, informal, and often unregulated, ARS. In this case, operators form a parallel, underground financial system aimed at rapidly and effectively moving value within or between jurisdictions, frequently without being detected by regulators and enforcers, and usually without publicly available transaction records. They are also cheap, making them important to poor and rural communities around the globe. States have used different means in attempts to mitigate the risk of ARS as a conduit to finance terrorism, and from these experiences the Working Group has extracted findings and recommendations.
49. **Finding:** Outlawing ARS can result in driving operators further underground and thereby making them more difficult to monitor and detect. The Working Group believes that effective registration is generally preferable to prohibition. However, the implementation of international standards on licensing or registration of ARS operators appears challenging in many States.
50. **Recommendation:** States should tailor the implementation of a registration regime to the local context. International financial institutions, regional organizations and States should develop best practices on registration, and in doing so should incorporate lessons learned from various regional contexts concerning incentives for maximizing the coverage of and participation in licensing regimes.

² According to the definition provided by the FATF in its 2005 ML/TF Typologies report.

51. **Recommendation:** Financial institutions and other reporting entities should (continue to) report to authorities any transactions suspected of being part of an ARS working outside the formal financial system and Governments should ensure that systems are in place for proper oversight.
52. **Finding:** Although licensing and registration systems have already been implemented in some States, there is no methodology for measuring their effectiveness.
53. **Recommendation:** In supporting States to register or license ARS and thereby bringing them into the CFT regime, a relevant international organization, acting within its mandate, should develop a methodology to measure the effectiveness of CFT tools and determine best practices.

E. Emerging technologies

54. The rise of information and communication technologies in the past decades has facilitated economic development. The same innovations that can be used against terrorism financing by their ability to record and detect financial activities also can be instrumental in buoying it by opening new channels through which terrorists can solicit and receive funds. The two-sidedness of technological advances requires a constant vigilance on the part of policymakers, law enforcement and intelligence communities in mitigating the risks of terrorism while simultaneously promoting development, which ultimately will reduce many of the factors³ that lead to terrorism.
55. The traditional methods⁴ through which financial transactions are initiated, processed and settled are quickly being transformed by recent developments in payment systems. These are essentially technological innovations that allow transactions through new channels and structures. The most common are mobile phones, the Internet and electronic value cards.⁵ Each of these three carries varying levels of opportunity as well as risk. Because of the novelty of their use for payments, many have yet to be regulated or even fully considered by Governments. This means that the financial transactions channelled through them can fall outside the AML/CFT regulatory umbrella, existing in a grey zone between the ARS discussed above and formal financial services.

³ See the recent World Bank publication *Finance for All?* (2007) for more on how economic development can bring stability by wiping away many of the challenges that threaten it, social inequalities for example.

⁴ This includes bank branches, ATMs and conventional interfaces through traditional financial institutions.

⁵ This list is certainly not exhaustive but, as of the time of drafting, these three innovations are the most popular of new payment methods.

56. **Finding:** Many new technological breakthroughs in payment systems are not being supervised by regulatory authorities.
57. **Recommendation:** There should be early and prompt identification of risks from new technologies. Authorities should decide at what stage to apply regulation to new technologies, keeping in mind that some technological developments become obsolete quickly. International financial institutions (acting within their respective mandates), regulators and financial institutions should raise awareness and provide guidance on best practices and discuss new regulatory approaches to mitigate risk.
58. **Finding:** The complex nature of these financial services presents a further challenge to Governments once the decision to regulate them has been made. Sometimes operators are subject to multiple supervisory agencies which may provide confusing or even conflicting rules. For instance, mobile phone financial services when regulated may be supervised by telecommunications and financial authorities with different data record requirements.⁶
59. **Recommendation:** Regulation for value transfer systems should fall under one overall supervisory authority in each jurisdiction. Where there is a need for multiple authorities, the regulations should make it clear that all operators are covered and by which agency each of them is supervised.
60. **Finding:** Some new technologies, such as digital currencies, have enabled payment systems that are not fixed in any single jurisdiction but span multiple jurisdictions through the Internet. Such systems create jurisdictional challenges for regulators and law enforcement agencies.
61. **Recommendation:** Regulatory standard setters should consider establishing criteria for determining supervisory responsibility for those systems so that proper controls are in place and their multijurisdictional value transfer operations do not escape supervision.

⁶ Pierre Chatain, Raul Hernandez-Coss, Kamil Borowik and Andrew Zerzan, *Integrity in Mobile Phone Financial Services*, World Bank, Working Paper 146 (2008).

CHAPTER 5

Non-Profit Organizations

Background

62. Non-profit organization (NPO) is a broad term used to describe a plethora of entities from condominium associations to societies that raise money to support relief work overseas. The sector is enormous. Its operating expenditure is approximately 1.3 trillion dollars,⁷ equivalent to the gross domestic product of the United Kingdom or France. Its employment exceeds that of the world's largest 50 corporations combined, standing at over 40 million persons globally.⁸ NPOs' critical role in building societies is difficult to quantify, but one can attempt to illustrate it by the annual volume of money they channel to economic development assistance—\$20 billion in 2006.⁹ In many countries, including the United States, the largest donor, the level of charitable giving equals or surpasses foreign aid. This makes NPOs very important to the global economy and to developing countries in particular.
63. NPOs are also among the many vehicles that have been identified as being potentially vulnerable to terrorism financing abuse. States have moved to implement CFT controls intended to limit any risk NPOs carry. However, the actual level of risk this sector poses, or even how effective existing controls are at mitigating it, remains unclear. Risk awareness-raising among financial institutions, authorities and NPOs themselves continues to be the key tool for States moving to protect the sector from abuse and stifling over-regulation.
64. **Finding:** NPOs provide possible opportunities for terrorism financing and as such pose a potential risk, yet at the same time they play a crucial part in fighting conditions conducive to terrorism. NPOs are critical in reducing the appeal of terrorism, by building social structures and increasing intercommunity dialogue and understanding. These endeavours can prevent the causes of radical ideology from taking root. CFT measures that do not take this into

⁷ Johns Hopkins University Comparative Nonprofit Sector Project estimate in 2004 US dollars.

⁸ Johns Hopkins University Comparative Nonprofit Sector Project estimate of staff in 36 economies, over 55 per cent of whom are classified as paid staff.

⁹ OECD estimate in 2006 dollars.

account may have a distortive effect and cause net harm. It is important to be realistic about the actual use of this sector for terrorism financing. As a percentage of the total NPO financial flows, TF-related funds are very small.

65. **Recommendation:** States should avoid rhetoric that ties NPOs to terrorism financing in general terms because it overstates the threat and unduly damages the NPO sector as a whole.
66. **Finding:** It is important to recognize the difference between NPOs exploited by terrorist financiers and NPOs that are themselves complicit in terrorism financing. Both cases have arisen, but typology reporting and its application do not always make this clear.
67. **Recommendation:** The type of abuse should be considered relevant to the sort of enforcement action to be taken. For instance, it is often not necessary to shut down an entire NPO because of one suspected individual. Actions taken should be proportionate and reflect the specific risk, that is, removing a dubious trustee or branch to reduce the risk while ensuring that the NPO can continue its work.
68. **Finding:** CFT measures further the same objective as mitigation measures designed to address other financial crimes. For example, due diligence and financial disclosure standards for NPOs coincide with measures taken to mitigate the risks of fraud.
69. **Recommendation:** Any regulation designed to tackle terrorism financing by and through NPOs should be seen to be part of a much wider effort to enhance the transparency of the NPO sector—encompassing the governance, finances and partner organizations—and to strengthen the sector as a whole. States should look at well-regarded regulatory systems and involve the NPO sector in the design of regulatory systems. Maximum use should be made of information already available to Governments or to sector regulatory organizations in order to avoid burdening NPOs with redundant and onerous reporting requirements.
70. **Recommendation:** To minimize regulatory burdens on NPOs, those who promulgate regulation should ensure that risk assessments are done to allow the NPO sector to focus their compliance efforts on high-risk situations and to be clear about the “best efforts” nature of the obligation. “Best efforts” implies an NPO must, in good faith, do as much as it can reasonably be expected to do to fulfil its obligations.
71. **Finding:** Under some circumstances, including humanitarian crises, unavailability of reliable documentation, lack of existing registration requirements and lack of NPO resources, certain due diligence requirements can

be unrealistic. There exist cases in which counter-terrorism financing controls precluded aid from being delivered to those in need. This can create a void in which terrorist organizations are in fact delivering humanitarian assistance and building political support, thus worsening efforts to curb terrorism and its financing.

72. **Recommendation:** Oversight should be proportionate to the risk of abuse. For NPOs, this means that States should ensure that legal ways are identified to deliver aid during humanitarian crises, considering the use of other, not suspect, NPOs and bearing in mind the value of building civil society.

CHAPTER 6

Freezing of Assets

Background

73. One of the central components of the global effort to disrupt terrorism financing is the assets freeze of designated persons and entities. The United Nations Security Council began the effort in the late 1990s as a way to target specific parties instead of sanctioning an entire nation. Compliance with the assets freeze regime remains weak globally. Many countries do not have the legal framework to immediately freeze terrorist monies. And, even where such frameworks do exist, they are often not implemented effectively. For instance, financial institutions and authorities sometimes struggle to clarify or verify a designated person's name.
74. A second issue arising from the assets freeze relates to *Security Council resolution 1373 (2001)*. Under *Security Council resolution 1267 (1999)* and its successor resolutions, the Security Council issues names associated with the Taliban, Al-Qaida, Usama bin Laden and their supporters on a United Nations public list of sanctioned individuals and entities. *Resolution 1373 (2001)*, however, requires that States themselves determine the individuals and entities associated with terrorism generally whose funds and assets should be frozen. *Resolution 1373 (2001)* also calls on States to share the names of their suspected terrorists, meaning that recipient States must determine what effect to give to such information and to a possible freezing request from a foreign State. This requires bilateral cooperation, trust and political and legal instruments, including a test to determine when it is proper to implement freezes in response to such requests. The FATF standards call for States to decide for themselves what is reasonable and what is not.
75. A further difficulty lies in the fact that many question whether the due process rights of those persons and entities designated are being respected in the implementation of *resolution 1267 (1999)*. Perhaps most notably, the European Court of Justice ruled recently in the Kadi and Al-Barakat joint cases (3 September 2008) that implementation of *resolution 1267 (1999)*, by European Union regulations, fails to respect due process and human rights by, among other points, not providing sanctioned individuals with notice of their listing and does not offer any mechanism in which the listed individuals can appeal their designation.

A. Improving listing quality and legitimacy

76. **Finding:** States and courts have questioned the legitimacy of the designation procedures contained in *resolution 1267* and are thus questioning its freezing regime. The credibility and effectiveness of the system depend upon its being fair and legitimate and perceived as such.
77. **Recommendation:** States applying sanctions regimes should ensure to the greatest extent possible the full observance of an individual's rights to be informed of the evidence against him and to be heard. The individual should also be made aware of the procedure for designation.
78. **Finding:** As a means of achieving agreement at the international level, the pertinent resolutions have been drafted in ways that leave detailed implementation to be worked out by the Security Council Committee¹⁰ and by each State. There is no agreed common format for national or regional lists, creating practical problems for financial institutions and other entities trying to implement them.
79. **Recommendation:** National authorities are encouraged to adopt a common format for national and regional lists with agreed mandatory information fields and with as much identifier information as possible, including transliteration of names, based on the work to be done under *Security Council resolution 1822 (2008)*. This will assist financial institutions and others monitoring their activities and improve the implementation overall.
80. **Finding:** A secondary issue is that the large number of entries on the various lists limits financial institutions' ability to focus on those that are financially relevant in some jurisdictions. This may have particularly acute implications for States, financial institutions and others with low capacity to screen names on the list.
81. **Recommendation:** When considering possible additions to the sanctions regime, States may wish to pay particular attention to the listing of terrorism financiers (that is, those who actually have assets).
82. **Finding:** There is some confusion about States' obligations under the multiple Security Council resolutions on counter-terrorism financing.
83. **Recommendation:** The Security Council, both directly and through its relevant expert groups, is encouraged to increase awareness and understanding of the essential differences between the obligations placed on States by *resolution 1267 (1999)* and its successor resolutions, on the one hand, and by *resolution 1373 (2001)*, on the other.

¹⁰ The Security Council Committee established pursuant to resolution 1267 (1999) concerning Al-Qaida and the Taliban and associated individuals and entities.

84. **Finding:** Although the freezing mechanism under *resolution 1267 (1999)* is an administrative (as opposed to criminal/legal) instrument and is intended to address a specific threat without delay, in some jurisdictions, time-consuming judicial procedures must be undertaken before the measures can take effect. These approaches can impede the effectiveness of implementation of the sanctions regime because they give designated individuals and entities time to move or conceal funds and notify the terrorist network that it has been detected.
85. **Finding:** Sometimes individuals are mistaken for a listed person. Their quick exoneration is critical both from a justice and human rights perspective and to preserve the legitimacy of the listing process. To expedite the unfreezing of their assets, financial institutions need guidance on unfreezing assets of those mistakenly identified as listed parties.
86. **Recommendation:** Guidance should be provided at the domestic level by Governments issuing best practices on unfreezing. States may wish to also consider the establishment of a national help desk for financial institutions on issues related to freezing/unfreezing.
87. **Finding:** A way for terrorism financiers to avoid the assets freeze is to establish themselves under a name different from that which is on the list. By the use of a new legal entity, they may be able to operate without hindrance.
88. **Recommendation:** Governments are encouraged to find a national mechanism to allow the freezing of funds of entities that are basically designated entities under a new legal person. There are already national systems in place that are possible best practices to mitigate this risk. In one country, for instance, the law allows for immediate designation of new legal entities in the same manner that it designates terrorist organizations, that is, by executive order subsequently subject to legal review.
89. **Finding:** The designation of legal entities presents particular complexities for authorities and private sector actors when implementing freeze orders. These complexities involve the application of the principles of ownership, control and association.
90. **Recommendation:** States designating entities should provide sufficient information for financial institutions to be able to apply the above principles accurately.

B. Improving outreach to stakeholders

91. **Finding:** The assets freeze regime must have participation of all stakeholders in order to be effective. Currently, private sector involvement and partnership are not optimal.
92. **Recommendation:** Private sector participation should be improved. This can be done by, for instance, making a system freely available to the private sector that searches a database of persons designated under *resolution 1267 (1999)* and subsequent resolutions.
93. **Finding:** The existence of multiple, non-identical lists issued by various Governments and regional organizations complicates compliance. Financial institutions with branches in several jurisdictions may not be clear about which lists they have to apply, where and under what authority, especially when some countries seek to compel financial institutions to comply with their regulations globally.
94. **Recommendation:** States should be sensitive to and try to avoid or resolve problems created by regulation which imposes reporting or other legal obligations on a financial institution that conflict with those of another country. A list's scope—whether global, regional or national—should be clearly defined so that financial institutions know the geographical extent to which the list must be applied.
95. **Finding:** Financial institutions hold only a portion of the terrorists' assets. Non-financial entities may also hold such assets, including non-monetary assets.
96. **Recommendation:** States should ensure a national policy mechanism to ensure the implementation of freezing obligations and the distribution of lists not only to financial institutions but also to every institution that could be relevant to identifying terrorist assets (for example, real estate registries, non-financial businesses and others that may hold monetary or non-monetary terrorist assets).

C. Coordinating before listing

97. **Finding:** Delay in national implementation may allow terrorists to move their funds out before a freeze order goes into effect in a jurisdiction.
98. **Recommendation:** Governments should have procedures in place that automatically give effect to United Nations freezing orders, including legal obligations that financial institutions (or other establishments with access to United Nations listing information) provisionally implement a freeze upon

learning that it has been issued by the United Nations, subject to confirmation by national decree or regulation.

99. **Recommendation:** A Government proposing a listing should consider “pre-listing” communication with all countries where it believes a proposed individual or entity may have assets. The Security Council may wish to consider a procedure for immediate notification of listings to United Nations missions in advance of their public release. This would help facilitate quicker communication of the designations to each country Government.
100. **Finding:** There may be intelligence value in not immediately freezing terrorist assets. For instance, allowing terrorists to move funds within their organization’s network for a period of time could help identify previously unknown players and assets or provide more detail regarding the nature of their activity.
101. **Finding:** Carefully timing a suspect person’s designation can help balance the need to gather intelligence on a terrorist network and to deny economic resources to a terrorist organization.
102. **Recommendation:** The Security Council may wish to consider whether there could be circumstances in which it should delay a freezing order under *resolution 1267 (1999)* in order to allow investigative monitoring of assets.

Report Contributors

CTITF members

International Monetary Fund

El Khoury, Chady
Kyriakos-Saad, Nadim
Myers, Joseph
Thony, Jean-François

World Bank

Merican-Cheong, Latifah
Vaccani, Matteo
Van Der Does De Willebois, Emile
Zerzan, Andrew

United Nations Office on Drugs and Crime

De Feo, Michael
Dedeyne, Jo
Kuleshnyk, Irka
Laborde, Jean-Paul
Merckx, Dirk
O'Sullivan, Patrick
Pilgrim, Julia
Puthuppally, George
Ruthstrom-Ruin, Cecilia
Treso, Andrea

Counter-Terrorism Committee Executive Directorate

Joyce, Elizabeth

Monitoring Team of the 1267 Committee

Barrett, Richard

INTERPOL

Courteau, Jacques
Kersten, Ulrich
Ragg, Michaela

CTITF Office

Neutze, Jan
Wu, Anne

Other international organizations

Crocker, Karen	Council of Europe
Greene, Carlton	Formerly Al-Qaida/Taliban Monitoring Team

Public sector	
Argentina	
Barbaccia, José C.	Federal Prosecutor
Biagosh, Zenón	Central Bank of Argentina
Di Pasquale, Fernando	Central Bank of Argentina
Austria	
Furtner, David	Federal Ministry of Internal Affairs
Belgium	
Delepière, Jean-Claude	Cellule de traitement des informations financières
Canada	
Adams, Bill	Formerly Royal Canadian Mounted Police
Bateman, Paul	Royal Canadian Mounted Police
Intscher, Horst	Formerly Financial Transactions and Reports Analysis Centre
Reynolds, Rick	Formerly Royal Canadian Mounted Police
Egypt	
El Siwy, Adel	Egyptian Money Laundering Combating Unit
France	
Werner, François	Tracfin
Germany	
Schmitt, Martin	Bundeskriminalamt
Israel	
Yehuda, Shaffer	Money Laundering Prohibition Authority
Italy	
Maresca, Giuseppe	Ministry of Economy and Finance
Nardi, Alessio	Guardia di Finanza
Lebanon	
Abou Daher, Adel	Internal Security Forces
Karnib, Moussa	Internal Security Forces
Nasr, Maroun	Internal Security Forces
Nassar, Pierre	Internal Security Forces
Netherlands	
Bosch, Tim	Intelligence Service

Nigeria	
Okauru, A. B.	Financial Intelligence Unit
Philippines	
Aquino, Vic	Financial Intelligence Unit
Qatar	
Al Mahmoud, Turki	State Security Bureau
Switzerland	
Martinez, Damien	Bundeskriminalpolizei
Moeri, Reinhard	Anti-Money Laundering Control Authority
Stadler, Stephan	Anti-Money Laundering Control Authority
Thailand	
Prayoonrat, Seehanat	Anti Money Laundering Office
United Arab Emirates	
Al Suwaidi, Sultan Bin Nasser	Central Bank of the UAE
United Kingdom	
Laramée, Wayne	Financial Services Authority
Robinson, Philip	Financial Services Authority
United States	
Poncy, Chip	United States Treasury
Philipp, Julia	United States Treasury
Private sector	
Behram, Sepideh	American Bankers Association
Coghlan, Robert	BNP PARIBAS
Crowe, Edward F.	JPMorgan Chase & Co.
Cushing, Robert	Sumitomo Mitsui Banking Corporation
Dennison, Bill	BMO Corporate
Ganguli, Indranil	Association of German Public Sector Banks
Ketley, Alan	HSBC
Langford, William	JPMorgan Chase & Co.
Lauber, Michael	Leichtenstein Bankers Association
Mair, John	Western Union
McGinnis, James	BNP PARIBAS
McVicker, Mike	Standard Chartered Bank
Mitchell, Andrew	Furnival Chambers

Private sector (continued)

Moe, Serena D.	Citigroup
Munro, Stevenson	UBS Investment Bank
Pesce, Teresa	HSBC
Regnault, Valérie	Société Générale
Sadouk, Rachid	Attorney
Schwander, David	European Association of Public Banks
Scifo, Frank	Bank of Tokyo–Mitsubishi UFJ Ltd
Scotto, Salvatore	Bank of America
Small, Rick	American Express
Stockdale, Richard	Lloyds TSB Global Services Private Ltd
Verberk, Mark	Fortis Bank N.V.
Wegstein, Johannes	Deutsche Bank
Werner, Robert	Merrill Lynch
White, Timothy R.	Banker's Toolbox Incorporated
Ziverts, Peter	Western Union

Academia and civil society

Biersteker, Tom	Brown University
Eckert, Sue E.	Brown University
Husin, Gunawan	Consortium for Combating the Financing of Terrorism
Passas, Nikos	Northeastern University
Romaniuk, Peter	John Jay College of Criminal Justice
Shaw-Hamilton, James	Humanitarian Forum

The Counter-Terrorism Implementation Task Force is grateful to the Governments of Germany and Switzerland for their generous support of this project.

www.un.org/terrorism/cttaskforce