Studies in Conflict & Terrorism, 35:712–732, 2012

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/1057610X.2012.712032

Routledge
Taylor & Francis Group

Private Actors in the Fight Against Terrorist Financing: Efficiency Versus Effectiveness

OLDRICH BURES

Department of International Relations and European Studies
Metropolitan University
Prague, Czech Republic

In several areas of the post-9/11 efforts to fight terrorism, private rather than public entities have shouldered the bulk of the burden. This has been especially the case in the fight against terrorist financing where private financial institution are legally obliged to monitor the billions of daily financial transactions and report the suspicious ones to public authorities for further investigation. Since private financial institutions are geared toward making profits and where the money has come from has traditionally not been of great interest to them, it is important to investigate how they have coped with these demanding requirements.

Terrorists, like everyone else, need money and resources to survive and function. The underlying logic of combating terrorist financing (CTF) is therefore straightforward—if the money can be shut down, so can the terrorist activities that it was meant to finance. Shutting down terrorist finances, however, has proven to be a formidable task. In this article, I argue that to a significant extent, this is due to the lack of appreciation of the role of private financial institutions (FIs) that are legally obliged to carry out public CTF regulations in practice. In particular, there is a cause for concern that private FIs' (over-)efficiency in reporting large numbers of suspicious financial transactions actually further undermines the already low effectiveness of the global CTF regime.

The structure of this article is as follows. The first section introduces two key global international CTF frameworks that have been developed by the United Nations and the Financial Action Task Force. The second section describes the role of private actors in CTF, with a special focus on formal financial institutions. The internal shortcomings of the smart sanctions and anti–money laundering CTF models are analyzed in the third section. The fourth section offers an analysis of the difficulties of private actors when it comes to applying the risk-based model within the publicly regulated CTF framework. The fifth section introduces the profit versus security dilemma that FIs have had to address when responding to the public regulatory CTF requirements. In combination with the difficulties of the risk assessment model, the profit versus security dilemma has led to the phenomenon

Received 20 September 2011; accepted 5 February 2012.
The author gratefully acknowledges financial support from the Czech Science Foundation under the research grant no. P408/11/0395.
Address correspondence to Oldrich Bures, Metropolitan University Prague, Dubecska 900/10, Prague 10, 100 31, Czech Republic. E-mail: obures@alumni.nd.edu

of defensive compliance whereby FIs report even marginally suspicious transactions. In section six, I therefore argue that efficiency does not equal effectiveness when it comes to FIs' role in CTF.

Countering Terrorist Financing: Rationale and Frameworks

According to much of the available literature, CTF efforts relate to counterterrorism in the same way as anti–money laundering efforts relate to crime reduction: "The rationale is in both cases the same—like other criminals, terrorists cannot operate without financial resources."[1] As such, both terrorist financing and traditional financial crimes leave "a financial footprint that allows us to trace financial flows, unravel terrorist financing networks, and uncover terrorist sleeper cells."[2] If successfully executed, CTF measures should also mitigate the first mover advantage terrorist otherwise hold. In some cases, limiting the available resources "may prevent some attacks from taking place, or at least can reduce the impact of attacks that cannot be prevented."[3] In addition, CTF efforts should also help to track operatives, chart relationships, and deter individuals from supporting terrorist organizations both directly[4] and indirectly, through diversion of funds from charitable and other organizations.[5] Moreover, unlike much of the other evidence relating to terrorism, which can be "suspect, the product of interrogation, rewards, betrayals, deceits . . . a financial record doesn't lie."[6] As such, it is more reliable than other forms of intelligence when it comes to reconstructing events after terrorist attacks and gaining better understanding of the terrorist group's modus operandi and internal organization. According to some experts, we may actually be witnessing a "recalibration of CTF strategy with a growing emphasis on the strategic and operational value of financial intelligence (FINITN) rather than money per say."[7] Finally, in addition to the preventative, deterrent, investigative, and analytical functions, CTF measures also have an important political utility "as they demonstrate concrete policy measures that governments can take in a multi-faceted effort to counter future acts of terrorism."[8]

There also appears to be a general consensus that given the global nature of contemporary terrorism, it is essential to ensure uniform international implementation of CTF measures. This is, however, inherently difficult due to the seemingly never-ending dispute about the definition of terrorism,[9] which complicates both academic research and practical counterterrorism efforts at the international level. Moreover, terrorist groups vary in their organizational form and thus also in the ways they raise, store and move funds.[10] Prior to 9/11, terrorism was financed on national basis through criminal activities (protection rackets, bank robberies etc.); and/or on transnational basis through fundraising in states with sizeable diasporas for the armed struggle in the "home" state; and/or through states funding foreign groups as proxies for the achievement of their own foreign policy goals. After 9/11, however:

> [T]he advent of self-supporting 'nomadic terrorist networks' with global or regional, rather than separatist, goals, such as al-Qaeda, has added a new dimension to the problem. A nomadic group moves between jurisdictions and operates in different jurisdictions. It can obtain its financing in one region, but carry out operations by means of active cells stationed in, or transferred to, another region.[11]

It is therefore clear that one financial safe haven is enough to wrack any international CTF efforts, whose strength and effectiveness are determined by the weakest link in the international cooperation frameworks. Thus, in order to "starve the terrorists of funding,

turn them against each other, rout them out of their safe hiding places, and bring them to justice,"[12] several parallel national, regional, and global CTF processes have been put in place since the 1970s. As discussed elsewhere, these processes interact and overlap in numerous ways[13] and, as discussed below, they increasingly rely on the participation of private sector actors. It is, nevertheless, possible to identify two key contemporary CTF frameworks whose logic has, at least since 9/11, shaped CTF efforts worldwide—the smart sanctions model advanced by the United Nations (UN) Security Council and the anti–money laundering model advanced by G-7's Financial Action Task Force (FATF).

The Smart Sanctions Model (UN Security Council)

In the aftermath of the 9/11 attacks, the UN Security Council took a rather radical measure by adopting UN Security Council resolutions (UN SCR) 1373 resolution under Chapter VII of the UN Charter, which (among other things) explicitly obliges all UN Member States to criminalize acts of financing of international terrorism, and of making available funds to terrorists, as well as to freeze funds and other financial assets of persons and groups engaged in terrorist activities. The resolution contains no time limit and UN Member States are obliged to report to the UN Counter-Terrorism Committee, which reviews the reports submitted in order to identify weaknesses in states' laws and implementation of laws relating to terrorist financing.[14] In addition, it is important to mention at least three other UN Security Council resolutions in the CTF context, which effectively trigged the adoption of the so-called "smart sanctions"[15] approach in the context of international counterterrorism. Generally speaking, UN smart sanctions work by creating a Sanctions Committee which draws up a "blacklist" of targeted persons and/or groups, imposing obligations on all UN Member States to, for example, freeze the listed persons' assets, impose travel bans on them and criminalize any attempts to provide them with financing or weapons. Specifically, in the context of counterterrorism, the 1999 UN SCR 1267 condemned the use of Afghanistan as a safe haven for terrorists and established a Sanction Committee to assure compliance of all UN Member States with the measures intended to interdict and freeze all financial support to the Taliban regime. The 2000 UN SCR 1333 added the call for the freezing of funds and financial assets of bin Laden, the Al Qaeda organization and all its associates, which were all added to a special UN list of terrorist organizations and individuals. Since 2002, this UN list is maintained by the direction of UN SCR 1390, which called for its regular up-dating by the UN SCR 1267 Sanction Committee. After the last up-date in January 2010, it contained 501 names of individuals and groups,[16] most of which were listed on the basis of secret intelligence material supplied by UN Member States. As discussed extensively in the legal literature, this has generated a great deal of criticism and, in some countries, even court trials.[17]

The Anti–Money Laundering Model (Financial Action Task Force)

Given the aforementioned similarities of anti–money laundering and CTF processes, and taking into account that "criminalization of terrorist financing is largely useless without backing it up with a strong regulatory framework for the activities of financial institutions,"[18] it is not surprising that the Financial Action Task Force (FATF) on Money Laundering nowadays sets and promotes the adoption of global standards to combat both money laundering and terrorist financing. Established at the 1989 G-7 summit, the FATF has become one of the most elaborate mechanisms in the contemporary international system for capturing the financial resources of would-be terrorists.[19] First published in 1990 and

updated in 1996 and 2003 to keep pace with the changing tactics of illicit money changers and to reflect the corresponding new UN anti–money laundering instruments, FATF's Forty Recommendations for pursuing the fight against money laundering are nowadays widely recognized as the international standard in this area.[20] Following the 9/11 events, the FATF convened an extraordinary meeting to specifically consider the financing of terrorism. The result of this meeting was an expansion of the FATF's mandate to cover CTF and in late 2001 the organization issued additional eight Special Recommendations for that purpose. These were complemented by an additional recommendation issued in October 2004. Collectively, they are known as FATF's Nine Special Recommendations (9SR)[21] and although there is no binding obligation to enforce them,[22] they are nowadays widely recognized as the international standard in the fight against terrorist finances.

Private Actors and the Fight Against Terrorist Financing

Although promulgated by public international bodies, the achievement of the aforementioned objectives of CTF efforts within both the UN-led smart sanctions and the FATF's AML models "require financial institutions and other market players to become watchmen and report suspicious or unusual activities to 'the competent [public] authorities,"'[23] that is, to the national Financial Intelligence Unites (FIUs).[24] The representatives of some public agencies have even argued that "[p]artnerships between the public and private sector represent one of the strongest means to detect, deter, disrupt and deny terrorist and other criminal organizations illicit profits and material support required to fuel their evil acts."[25] According to Petersen:

> [P]rivate partnerships are formulated as the third leg in an approach to terrorism—the first two being intelligence and surveillance (or technology). The main argument in favour of private-public partnerships is that, because it is no longer possible to distinguish between foreign and domestic security and terrorism can possibly affect us all, the engagement of a wide range of societal groups is necessary to prevent terrorist attacks.[26]

Alternatively, because of the large number of both public and private actors involved in CTF efforts, where "[p]revention, detection and reporting are carried out by private partners, while the public partners have an analytic and repressive task,"[27] a number of authors have written about the emergence of new "security spaces,"[28] "complex assemblages,"[29] and "neoliberal governmentality"[30] in the fight against terrorism. In all of these conceptualizations of the role of private actors in CTF, one can clearly detect the blurring of separation between public and private authority, and an increasingly important role of the latter when it comes to the day-to-day efforts to tackle terrorist financing.

In practical terms, financial organizations (such as banks, and insurance and investment companies) as well as certain non-financial organizations (such as lawyers, guarding companies, or casinos and dealers in high-value goods) are supposed to contribute to the public CTF efforts by adopting "a risk management process for dealing with money laundering and terrorism financing. This process includes recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks."[31] More specifically,

> Banks are expected to establish and maintain effective [customer due diligence] CDD measures at the point of establishing a customer relationship and on an

> on-going basis as necessary thereafter, the maintenance of adequate records, the ability to identify suspicious transactions and file STRs as necessary, the use of comprehensive programs for the training of staff, and the maintenance of effective compliance and internal audit mechanism.[32]

These measures should allow private financial institutions to detect suspicious transactions and/or customers, which in turn they are obliged to report to the public regulatory bodies, the FIUs. Known as Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs), they differ in their scope and their legal definition as well as method of collection is specified by each state.[33] In general, however, they usually contain the following fields: the reasons for suspicion, information on the transaction (such as the place, date, time, or period of time in which the suspicious acts occurred), the currency and the amount of money involved, extensive personal identification details, the official address of the customer, and account/credit card numbers of the persons or companies involved, the financial instruments (cash, checks, credit cards, e-money, etc.), number of transactions, status of the transactions, detailed information on the objects involved and the countries and institutions concerned by the transaction, information on the institution making the declaration, and a field to further describe the situation in more detail. The FIUs' personnel review the reported SARs in order to discover terrorist financing by searching through their databases "for certain characteristics such as combinations of specific countries, names and amounts of money. These searches can be combined with information from a range of other sources such as law enforcement, administrative or public registers, information and databases from private companies and open sources, most importantly the Internet search tool Google."[34] The precise procedure, database access, and follow-up on positive SARs varies from country to country, depending on the type of the national FIU.[35] The more important point is that while the entire process appears to be clear in theory, it has been far more challenging to ensure proper utilization of the aforementioned CTF measures in practice.

Not So Smart Sanctions and Anti–Money Laundering CTF Models

The first set of difficulties that (not only) private financial institutions face is due to the fact that it still remains unclear whether the smart sanction and the AML regimes themselves are appropriate for dealing with terrorist financing. Regarding the former, a major problem with the current blacklisting approach to CTF is due to the fact that blacklists themselves are inherently both under- and over-inclusive. This reflects the difficulties of providing accurate information precisely identifying a particular party or entity as a sanctions target:

> If a precise match with a government blacklist is required, targeted individuals and entities might escape the controls due to minor variations in the names. Conversely, if not enough rigor is applied in the matching process, the black-listing system can easily be overwhelmed by the number of false matches. A similar issue arises when common names appear on the blacklist, generating a large number of unintended matches.[36]

The false matches problem is, moreover, increasing every year because "the designation lists of those suspected of providing support to terrorist organizations in the UN, the European Union and particular countries (notably the USA) have grown so long and with so many common names as to offer limited assistance and pose issues of due process and enforceability."[37] For example, originally, only 29 individuals and 14 organizations were

placed on the EU list in 2001 but as of June 2009, there were already 57 individuals and 47 organizations.[38]

Another problem is that the current CTF blacklisting regime is neither smart nor targeted enough because the same sanction measures are applied against the direct and primary targets (e.g., top cadres of Taliban and Al Qaeda) and against a party who only incidentally dealt with them.[39] Moreover, as Charles Calomiris pointed out shortly after 9/11, if Osama bin Laden "can recruit 30 people willing to die on his behalf, he will have no problem getting 100 to open bank accounts."[40] The implication is that technological solutions using risk analysis methods "may be easily circumvented by mundane methods using the large pool of supporters attracted to the declared goals of a terrorist organisation." All they need to do is to add "to their 'normal' pattern of financial transactions . . . a small monthly transfer to another account, using cash provided to them anonymously."[41] It is therefore not surprising that some experts have even argued that there is "no independent evidence whatsoever that the blacklisting technique has any significant effect on limiting terrorist financing"[42] and pointed out that the current "political statement" blacklisting approach can actually make the task of tracing money flows more difficult. According to Fitzgerald, this is because of (a) the prevailing uncertainty regarding the details of the controls; (b) the obligations the sanctions impose; and (c) the manner of the sanctions enforcement.[43] Importantly, a key shortcoming in all three areas lies in the lack of appreciation of the role of the private sector and its compliance with CTF measures. Thus, as Favarel-Garrigues et al. pointed out in their study of the French banks' role in CTF, the term public–private partnership frequently used by public officials "seems somewhat inappropriate for defining relationships between banks and law enforcement agencies. It should be borne in mind that banks have been forced to comply with AML/CTF policy, and that the 'partnership' was clearly imposed 'by command'—that is, by the government."[44]

Regarding the AML approach to CTF, a major difficulty reported by some FATF member jurisdictions is "that terrorist financing might not meet the definition of money laundering [which] meant that they were limited in the actions they could take against terrorist monies in the framework of anti-money laundering laws."[45] As a consequence, the generally assumed CTF/organized crime analogy may not only be misleading, but counterproductive. This is because terrorism, which generally speaking seeks political objectives and money is therefore merely the means to an end, differs significantly from organized crime, whose primary objective is the money, or profit-making, itself. Terrorist financing (TF), therefore, differs from criminal money laundering (ML) in several critical ways: the direction of the related financial transactions, the tolerance for failure, the motivations of the participants, and the scale of the activity to be suppressed.[46] Moreover, while the nature of standard "dirty-to-clean" money laundering process is relatively well understood, "the full nature and potential of the 'clean-to-dirty' processes associated with terrorist financing are less well defined and understood."[47]

This is not to deny that there can be substantial overlap between ML and TF, especially in cases of the more traditional pre-9/11 terrorism and in dysfunctional states, but for many of the post-9/11 terrorist groups, the standard organized crime concept of money laundering ("dirty" money coming into the ordinary economy to be "cleaned") may not apply. In fact, the pattern is often reversed:

> A large lawfully earned sum is transferred to a state where the target is situated, whereupon the sum is split into several working accounts used for preparing the terrorist act. Even this pattern may be lacking where the active cell is home

> grown and has its own lawful sources of income. Their transaction records and account "profiles" will show few, if any, suspicious tendencies.[48]

This was also acknowledged by the National Commission on Terrorist Attacks upon the United States, which noted that none of the FATF Special Recommendations against terrorist financing issued shortly after 9/11 would have red-flagged any of the hijackers' transactions, if they had been in place before the attacks. An in-depth analysis of their operations suggested that suspicious transactions reports could not have been filed before because there was nothing irregular or unusual about them anyway.[49] The problem is, as Vlcek pointed out, that "[f]reezing the accounts of known terrorists and terrorist organisations does not tackle the unknown accounts of supporters containing the moneys that will be used for the next to-be-determined attack."[50]

Risks of the Risk Assessment Model in CTF

The second set of difficulties that private FIs have to address in response to the CTF "regulatory tsunami"[51] has to do with the very logic of the risk assessment approach and its applicability for CTF measures. Although risk management models are neither new nor uncommon to private sector actors, including FIs, they normally operate on the assumption that the company is able to quantify the extent of loss that would arise in the event that the risk occurs. For several reasons, however, this is extremely difficult, if not impossible, to do within the framework of the two aforementioned CTF models. Firstly, while there is data useful for developing risk assessment models for most types of business risk, the same cannot be said of the CFT risks because it is rather difficult to assess how much money is actually being laundered. The International Monetary Fund (IMF) estimated the total as a figure equal to between 2 percent and 5 percent of the world's Gross Domestic Product (GDP) (e.g., up to $2 trillion annually).[52] However, the critics have challenged the credibility of the IMF's methodology, claiming that "the only thing that can be stated with certainty is that the actual figure is not likely to be less than 0% or more than 100%."[53] Such claims are further supported by the fact that even FATF's attempts to calculate estimates of AML flows have failed in the past.[54] The data reported by the companies themselves in a 2007 survey by PriceWaterhouseCoopers suggests that although 12 percent perceived money laundering as a high risk to their organization, only 4 percent of these companies actually reported having experienced incidents related to money laundering.[55] One can therefore conclude with Verhage that "the perceived threat of money laundering ... [is] higher than the actual occurrence."[56] Most importantly, however, due to difficulties with establishing the proper magnitude of the CTF risk, the private FIs not only cannot estimate the significance of the money laundering problem but they are also left "with no clear benchmark of what would constitute success or of what an 'acceptable' figure for global laundered funds might be."[57] As a consequence, many FIs have concluded that it is better to err on the side of over reporting anything that looks even remotely suspicious (see below).

It is also interesting to note that according to a 2001 report by the U.S. Federal Bureau of Investigation approximately 50 percent of the total money laundered goes through the United States.[58] This may be one of the reasons why both the AML and the smart sanction models have their origins and strong support in the United States, whose government took advantage of the post-9/11 window of opportunity to overrule the objections of both private FIs and privacy lobbyist to more intrusive customer due diligence. In particular, the Patriot Act enforced a larger access to bank information for police and judicial services, which in turn also prompted the U.S. government officials to explicitly link the AML/CTF regimes

to U.S. foreign policy priorities in order to ensure the competitiveness of the U.S. financial sector by "reducing unfair competitive advantage of inadequately regulated jurisdictions."[59] On the one hand, the U.S. pressure to promote its own CTF standards worldwide makes sense because "some countries have few incentives to enthusiastically join the fight against money laundering and only strong leadership from other countries . . . may persuade them otherwise."[60] On the other hand, by imposing one-size-fits-all CTF measures "that are inappropriate for a country's level of development and in the process overwhelm scarce national resources, we may not effect even a modest progression towards compliance with the international standard."[61]

Moreover, although this article is focused on the role of formal private financial institutions, it is important to note that CTF efforts have had significant impact on the quality of life of individuals all over the world. To begin with, the aforementioned CTF measures have had severe repercussions on the informal remittance systems that are crucial for millions of people in the developing countries.[62] At least partly, this due to the fact that formal FIs have too often discontinued working with money services business due to "the erroneous view" that they all "present a uniform and unacceptably high risk of money laundering."[63] Alternatively, in the developed countries, some experts have pointed out that CTF measures do not only prevent the formal financial system against misuse by terrorists and money launderers, but also exclude vulnerable groups without a regular income or fixed address, such as the homeless, migrants, and students.[64] Thus, as Vlcek noted, the important point to keep in mind "is that constraining the informal banking system has the potential of a far more detrimental impact upon developing states than it has for any likelihood to identify and isolate terrorists."[65]

Secondly, although several international,[66] national,[67] and private bodies[68] have produced guidelines for identifying suspicious transactions, it is still not entirely clear how FIs are supposed to identify CTF risks:

> The situation varies across countries, but in general terms little or no specific guidance has been given as to how to determine whether or not a customer or a partner may be linked to or involved in terrorist financing. Is running the names of clients through databases of national and international blacklists and sanctions lists sufficient? Should banks and other reporting institutions watch out for connections to "countries of risk"?[69]

At the moment, it therefore appears that it up to the individual FIs to evaluate the transaction and customers on a largely discretionary basis: "Essentially, banks are now expected to make a value judgment about customers and their money and whether they may be involved in some terrorist activity, in the future."[70] According to an IMF report, the vagueness is actually intentional and should be understood as "another form of constructive ambiguity":

> The notion of suspicion is intentionally left vague so as to leave both money launderers and banks uncertain. Thus, money launderers cannot rely on simple rules to avoid being reported. Furthermore, banks are forced to constantly improve their understanding of how money laundering is done.[71]

In practice, however, the representatives of private FIs have criticized the fact that very few general clues for TF activities have been developed thus far: "A single financial transaction that raises suspicion could relate to anything. So the effectiveness of the reporting system depends heavily on the ingenuity of the analyst and on the other data he has available."[72]

Thus, although public policy makers hoped that the discretionary risk-based approach will help to increase the quality of SARs from the private sector, due to the absence of clear criteria, risk assessment in practice indeed appears to be largely based on the tenacity of AML/CTF compliance official/s in individual FIs:

> The compliance officer is at the heart of the anti-money laundering investments by financial institutions and therefore represents an important actor in the complex. In short, this compliance officer will check transactions made by staff and clients, give training to staff and superiors, investigate clients' backgrounds when necessary and make reports to the CTIF-CFI whenever a client or a transaction seems suspicious or could be related to money laundering or the financing of terrorism.[73]

The problem is that although compliance departments vary in size, related to the size of the financial institution, ranging from one single compliance officer in smaller banks to seventy plus officers in large transnational FIs,[74] the magnitude of their task is daunting. According to Cameron, just the New York InterBank system handles 200,000 payments totaling $1.1 trillion every day.[75]

Thirdly, given the vast number of transactions on daily basis, it is not surprising that even the biggest U.S. banks with the best automated interdiction software acknowledge that some "leakage" is inevitable: "Large banking institutions handle millions of transactions each day and, despite state of the art interdiction systems, frequent staff training and the institutions best efforts, it is statistically inevitable that a large bank will have inadvertent violations of sanctions."[76] This is rather problematic given that according to the UN Analytical Support and Sanctions Monitoring Team, the "[o]nly the sophisticated attacks of 11 September 2001 required significant funding over six figures. Other Al Qaeda terrorist operations have been far less expensive."[77] The report specifically stated that the Madrid bombings in 2004 cost about $2,000 and the Report of the Official Account of the Bombings in London in July 2005 estimated that the London bombings cost less than £8,000.[78] Moreover, the trend for local Islamist terrorist groups is toward self-funding so external funding is much less important than before 9/11.[79] Similarly, the available data on terrorist campaigns conducted by the "older" domestic terrorist groups in Europe indicates that they also do not require extensive funding to carry out deadly attacks.[80] Interestingly enough, this evidence has prompted some observes to argue that "every dollar matters" because even small disruptions in the flow of terrorist funds "can stop or postpone an imminent terrorist attack."[81] Others have noted that it is important to keep in mind that "while the operational costs of terrorism may be low . . . , the total cost of a terrorist attack is probably much higher, due to the requirements of recruiting, training, indoctrination, living expenses, and disseminating information."[82] Nevertheless, regardless of what estimates one prefers, former U.S. Defense Secretary Donald Rumsfeld was correct when he complained that "[t]he cost-benefit ratio is against us! Our cost is billions against the terrorists' costs of millions."[83]

Profit Versus Security Dilemma

The third set of difficulties is due to the fact that although private and public actors nowadays indeed interact in a "new CTF security space," this does not mean that they share the same objectives:

> There is actually an important difference between the interests of the regulator and the reporting entities. The latter does not want to spend much time investigating and reporting suspicious transactions since their objective is to make profit. From a short term business perspective strict controls represent extra costs and refusing certain clients make them lose money.[84]

Thus, when it comes to CTF, private institutions face what could be called a profit versus security dilemma. As all private enterprises, FIs are indeed geared towards making profits and where the money has come from and what it is being used to finance has not, traditionally, been of great interest to them. Demands and sanctions therefore have to be placed on FIs:

> [T]o overcome their natural reluctance to make too many problems for depositors, and thus kill the 'golden goose'." At the same time, it is evident that financial institutions must engage in a large degree of self-policing for the monitoring to work properly. Where they are worried that they may themselves have breached difficult-to-follow and overly demanding legal requirements (especially as regards blacklists) they are not going to report themselves.[85]

As a consequence, as profit-maximizing entities, FIs face a tradeoff: they can either report less, thereby saving them the costs to make all the reports for the FIU but accepting the possibility to get sanctioned, or they can increase the amount of reporting to decrease the chance of getting sanctioned, but having to accept the extra costs related to the extra reports.[86]

As discussed in the following section, within the current regulatory framework, FIs have overwhelmingly opted for the latter option. To a large extent, this is because unlike size of the actual risk of terrorist financing in the financial sector, the costs of (non-)compliance with the CTF requirements are already well known and substantial. For example, the Peterson Institute of International Economics estimated the gross financial costs of the U.S. AML regime for 2003 at $7bn ($25 per capita): government/public sector $3bn; private sector compliance $4bn, general public (costs passed on by the private sector) $1bn.[87] Alternatively, a 2004 Swiss study found that AML measures account for 45 percent of the total regulatory burden and 2 percent of the total costs in Swiss private banking.[88] Specifically, FIs incur direct expenses by "establishing and maintaining risk management and compliance systems, the prospect of reduced income as a result of decisions to forgo certain lines of business, costs that might be associated with the possible diversion of resources from other aspects of the bank's work, and the more intangible, yet important costs of inconvenience to customers."[89] Even more importantly, however, FIs face various potential costs, which include "civil and criminal monetary penalties, other sanctions such as cease and desist orders, or the removal of management, the loss of some lines of business and reputational damage which can result in a loss of business."[90] The available evidence suggests that the latter type of costs can be so substantial that they can bring into question not only the company's share price and customer base, but its very existence (see Table 1). This concerns especially the small banks, because "the cost CTF of regulation exhibits strong economies of scale."[91]

In light of the substantial penalties for non-compliance with CTF measures, it is not surprising that much of the available literature suggests that "banks are merely going through the procedures as evidence of compliance rather than in the expectation of unearthing criminal activity."[92] Although a few studies have argued that at least the bigger FIs can

Table 1
Examples of banks fined for AML/CTF non-compliance

Bank	Date	Fine and its justification
ABN-AMRO Bank (U.S.)	2005	Fined $80 million for failing to implement an effective anti–money laundering program.
Arab Bank (U.S.)	2004	Fined $24 million for failing to implement an effective anti–money laundering program.
AmSouth Bank (U.S.)	2004	Fined $50 million for failing to implement an effective anti–money laundering program.
Commercial Bank of Syria and its subsidiary Syrian Lebanese Bank	2004	Designed as "financial institutions of primary money laundering concern" by U.S. authorities, no business with U.S. FIs.
Riggs Banks (U.S.)	2004	Civil penalties $25 million and criminal penalties of $16 million for failing to implement an effective anti–money laundering program. Later it was taken over by a PNC bank.
Citigroup (U.S., Japanese branch)	2004	Japanese regulators ordered the bank to close its private operations due to concerns about failure of AML internal system controls. The value of the company's shares declined by 2.75 percent the week following the announcement.
Bank of Scotland (UK)	2004	Fined £1,250,000 for failing to keep customer identification records to the required standard.
Abbey National Bank (UK)	2003	Fined £2,320,000 for failures to comply with existing anti–money laundering regulations
The Northern Bank (UK)	2003	Fined £1,250,000 for failures to comply with existing anti–money laundering regulations

Sources: Barry R. Johnston and Ian Carrington. "Protection the Financial System from Abuse: Challenges to Banks in Implementing AML/CTF Standards," *Journal of Money Laundering Control* 9(1) (2006), p. 52; William Vlcek, "Securitization Beyond Borders: Exceptionalism Inside the EU and Impact on Policing Beyond Borders European Measures to Combat Terrorist Financing and the Tension Between Liberty and Security," Challenge Working Paper Work Package 2. September 2005, p. 20. Available at http://www2.lse.ac.uk/internationalRelations/centresandunits/EFPU/EFPUpdfs/EFPUchallengewp1.pdf (accessed 20 January 2008).

actually derive tangible benefits from their compliance with the CFT requirements, such as the development of sophisticated customer databases that can be used for marketing tools[93] or the development of new products,[94] the majority of experts agree that in addition to the fear of penalization from public authorities, FIs investments in CTF measures serve one primary goal—reputation protection: "Since the AML-battle has now put severe strains on banks, the reputational risk (and following from this, the impact on profit-making) has become too high to take. . . . Banks chose to intensify their checks and procedures, as any association with terrorism financing could have disastrous effects."[95]

It is important to note, however, that although the CTF framework requirements are designed in a way that inevitably provokes fear of penalties and reputational damage, "this fear does not automatically mean that reporting institutions will provide higher quality intelligence to the authorities in a consistent and methodical way, because the system is

largely based on vague concepts and subjective assessments."[96] Moreover, FIs are only fined for false negatives, that is, for not reporting transactions which are later prosecuted as money laundering or terrorist financing judged to be suspicious ex-post. In contrast, they are not fined for false positives, i.e. for reporting legal transactions as money laundering or terrorist financing.

Implications for CTF Efforts: Efficiency Versus Effectiveness

The combination of the aforementioned internal shortcomings of the CTF model and the fact that compliance by FIs with its requirements is primarily "undertaken to prevent a negative impact on, rather than as an enhancement to, reputation,"[97] has led to proliferation of defensive SAR filings that report even marginally irregular activity. Also referred to as the practice of "umbrella reports,"[98] it has become the primary mechanism of FIs' compliance officials who are coping with the problematic CTF requirements by "doing enough to proverbially 'cover their backs.'"[99] Even though some FIs' officials have vehemently denied following a simple "cover your ass" policy in anonymous interviews,[100] the available data on the amount of SARs points to the contrary. Although much information in many countries is still secret and the differences in national definitions of a suspicious activity/transaction obscure cross-country comparisons, Table 2 clearly indicates that the overall number of SARs submitted to national FIUs has increased over the years since 1994, with major hikes following the 9/11 terrorist attacks and the subsequent introduction of the smart-sanctions and AML models to fight terrorist financing.

The problem with the "cover your ass" policy is that the "efficiency" of compliance officers in meeting the CTF requirements by filling a high number of SARs does not necessarily translate into effectiveness in the fight against terrorist financing. In addition to placing a substantial burden on the public FIUs that have to process a large amount of data of dubious value, the increasing number of reported transactions serves to further bury suspicious transactions actually indicative of terrorist financing, which represent only a small share of the reported SARs (see Table 3). Thus, some experts, such as Liesel Annible, the U.K. president of the Association of Certified Fraud Examiners, believe that "the system can actually help criminals": "What does NCIS do with all these reports? Firms are now disclosing so much because of the fear of prosecution that there is a danger of serious infringements being hidden by and lost under all the noise of all the minor problems and unfounded suspicions. All these SARs just gum up the works—the vast majority are just stored."[101]

This was also confirmed in an IMF study, which found the "cover your ass" policy as strikingly similar to the effects of the so-called *Theory of "Crying Wolf*:"

> [E]xcessive reporting . . . fails to identify what is truly important by diluting the information value of reports. The intuition can be best understood through an analogy with the tale: "The boy who cried wolf". In the tale, the boy cried wolf so often, that his cries became meaningless. Similarly, excessive reporting, which will be referred to as "crying wolf", fails to identify what is truly relevant.[102]

Moreover, the study revealed that the relation between the height of the sanctions imposed on FIs for non-compliance and the effectiveness of the whole AML process until conviction can be depicted in a Laffer curve: if sanctions get too high their impact on effectiveness is negative.[103]

Table 2
Number of suspicious activity report filings by year in selected countries

State	1994	1995	1996	1997	2002	2003	2004	2005	2006
Belgium	2,183	3,926	5,771	7,747	13,120	9,953	11,234	10,148	9,938
Germany	3,282	2,935	3,289	NA	8,261	6,602	8,062	8,241	10,051
France	684	866	902	1,213	8,719	9,019	10,842	11,553	12,047
Netherlands	3,546	2,994	2,572	NA	24,741	37,748	41,003	38,481	NA
United Kingdom	15,007	13,170	16,125	14,148	56,023	94,718	154,536	195,702	213,561
United States	NA	NA	62,473	81,242	281,373	507,217	689,414	919,230	1,078,894

Source: Liliya Gelemerova, "On the Frontline against Money Laundering: The Regulatory Minefield," *Crime, Law and Social Change* 52 (2009), p. 51. Data based on FIUs annual reports. Includes reports related to both money-laundering and terrorist financing.

Table 3
Number of suspicious activity report filings related to terrorist financing

Germany	2002	2003	2004	2005	2006	2007	2008	2009
SARs total	8,261	6,602	8,062	8,241	10,051	9,080	7,439	9,046
CTF related SARs	90	127	114	104	59	90	65	98

Source: Michael Brzoska, *The Role of Effectiveness and Efficiency in the European Union's Counterterrorism Policy: The Case of Terrorist Financing*, Economics of Security Working Paper 51. July 2011. Available at http://www.diw.de/documents/publikationen/73/diw_01.c.377385.de/diw_econsec0051.pdf (accessed 28 August 2011). Based on data from Bundeskriminalamt 2010.

Although the criteria for measuring effectiveness of CTF policies are still up to debate due to the difficulties of establishing causality between output, outcome, and impact,[104] the available data confirms that high reporting efficiency by FIs has thus far not led either to depriving the terrorist of more funding or in locking them up behind the bars in large numbers. Regarding the former, the available data confirms that higher numbers of SARs have not led to higher amounts of frozen terrorist assets (see Figure 1). Regarding the latter, only the experiences of few FATF jurisdictions indicate some "usefulness" of the money laundering model at the operational level. In most other countries, however, the pattern is often reversed and evidence of money laundering/terrorist financing comes to light during the course of other criminal investigations. According to a Eurostat study, for example, out of 17 EU Member States that provided data on the number of cases initiated by law enforcement agencies on the basis of Suspicious Transaction Reports sent by the national

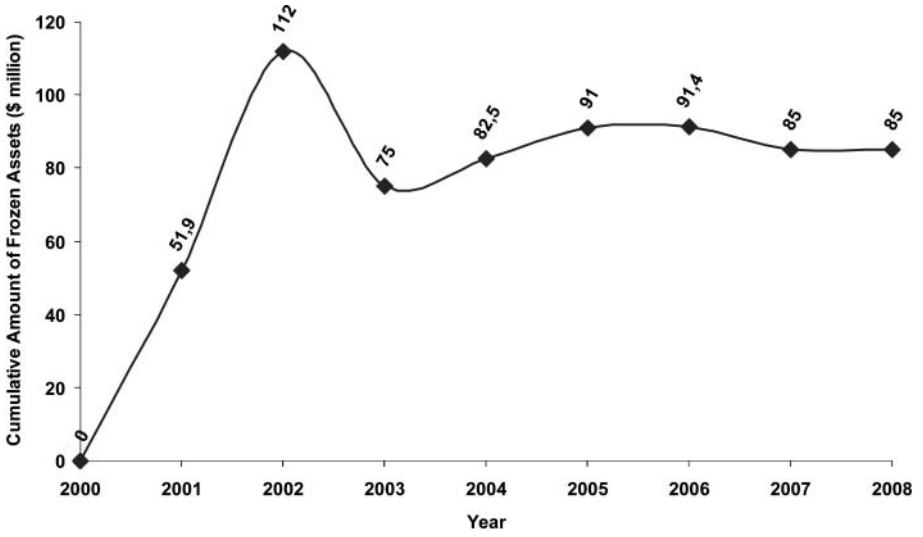

Figure 1. Cumulative worldwide amounts of frozen terrorist assets, 2000–2008. Source: Data for years 2000–2007 come from the *Seventh Report of the Analytical Support and Sanctions Implementation Monitoring Team*, S/2007/677 (November 2007), p. 45. Data for 2008 come from the *Eighth Report of the Analytical Support and Sanctions Implementation Monitoring Team*, S/2008/324 (May 2008), p. 19.

FIUs in 2007 and 2008, ten countries reported less than 100 cases annually.[105] Given the low number of terrorist related reports, one can therefore concur with Cameron that "there is little cause to believe that the mechanisms put in place will allow more than sporadic detection of terrorist financing. To the extent, then, that these measures have been 'sold' as means of preventing terrorist outrages this certainly represents a misrepresentation."[106] Indeed, there have been only few convictions thus far for violations of CTF laws. In the United Kingdom for example, there have been about 10 convictions for CTF offenses out of a total of about 100 convictions under the entire spectrum of the existing counterterrorism legislation.[107]

Pessimism about the effectiveness of existing CTF measures is also apparent from the few available national case studies and surveys of FIs' employees. According to a case study on the role of French banks in CTF, for example, most compliance officers "have been surprised by the sparse results of the 'war on terror' since 9/11: 'We have reported about 20 terrorism-financing cases: just bullshit that has scared us for nothing'."[108] Similarly, an evaluation of the Dutch CTF system showed that high numbers of reports do not automatically result in a higher effectiveness of the system.[109] Furthermore, it suggested that "introducing measures just to increase the number of reports, may only result in a widening of the gap between public and private actors within the AML complex, as the usefulness of the system is increasingly questioned by the private institutions.[110] In a 2004–2005 survey of the U.K. financial services industry, almost two-thirds of the respondents said the existing AML measures were too severe in proportion to the risks of money laundering. They "clearly believe that the UK has approached a 'tipping point' where past, current and future costs of such legislation are perceived to be greater than the benefits." The survey also revealed that "[o]verall, UK-based companies comply with AMLR in order to avoid sanctions from the authorities, and not because they perceive AMLR as representing good business practice or as being effective at combating money laundering."[111] Another survey among banks in Switzerland, Germany, and Singapore found that "the AML rules' implementation is highly burdensome and causes significant costs and efforts throughout the banks" and that "the impact of money laundering prevention on the predicate offences is small."[112] Finally, 77 percent of the interviewed Belgium compliance officers also complained that the government saddles the banking sector with governmental tasks: "This gives rise to the interpretation that the AML complex is mainly a one-way street in which private actors need to invest, while receiving very little in return."[113]

Concluding Remarks

Although the fight against terrorism is generally considered to be the top priority of national security, private, rather than public, entities have shouldered the bulk of the burden when it comes to fighting terrorist financing. The findings of this article, however, suggest that the current combination of "smart" sanctions and the AML models may not represent the best way to engage the private sector in the fight against terrorist financing. First, the two dominant CTF models have been based on a number of assumptions about the nature of terrorist financing that may not be warranted for many contemporary terrorist groups. Second, although they require execution by private sector entities, the CTF measures are based on the logic of risk assessment, which is rather problematic when it comes to the threat of terrorism that is extremely difficult to quantify for individual financial institutions. Third, the public authorities have provided the private sector with only vague clues for detecting costumers and/or transactions that may be linked to terrorist financing while demanding that FIs put in place elaborate and costly surveillance mechanisms and procedures. Fourth,

it should be kept in mind that private entities are primarily profit, rather than security, maximizers. As a consequence, due to the substantial penalties for non-compliance and reputational concerns, private FIs have resorted to the practice of defensive compliance with the public CTF regulations by (over-)reporting. This reporting "efficiency" has, however, further diminished the already dubious effectiveness of the CTF regime.

It is, therefore, questionable whether the existing CTF arrangements can ever meet the requirements of an effective CTF regime, for example, one which is: (1) *comprehensive* (e.g., capable of covering a wide variety of sources that may generate material signals in the detection of potential terrorist acts or actors); (2) *selective* (received data must be effectively filtered in order to focus activities and to reduce the workload); (3) s*mart* (e.g., search for clues as well as further information from various sources in order to check and double check suspicions as well as to establish and test hypotheses).[114] Moreover, the costs of the CTF measures are not only financial—liberty, human rights, and justice can also fall victim to misguided measures. Thus, although the numerous legal dilemmas were only briefly mentioned in this article, all CTF measures need to be designed to ensure compatibility with fundamental rights and general principles of law. As one anonymous reviewer aptly noted, counterterrorist measures which are repeatedly quashed in courts can hardly be considered "effective."

Notes

1. Kathryn L. Gardner, "Terrorism Defanged: The Financial Action Task Force and International Efforts to Capture Terrorist Finances," in David Cortright and George A. Lopez, eds., *Uniting Against Terror: Cooperative Nonmilitary Responses to the Global Terrorist Threat* (Boston, MA: MIT Press, 2007), pp. 159–186.

2. U.S. Department of the Treasury, *Oral Testimony of David D. Aufhauser, General Counsel, Department of the Treasury Before the Judiciary Subcommittee on Terrorism, Technology and Homeland Security*. 26.6.2003. Available at http://www.treasury.gov/press/release/reports/js5071.pdf (accessed 20 May 2006).

3. Thomas J. Biersteker and Sue E. Eckert, *Countering the Financing of Terrorism* (London: Routledge, 2007), p. 1.

4. Laura K. Donohue, *The Cost of Counterterrorism: Power, Politics, and Liberty* (Cambridge: Cambridge University Press, 2008), p. 122.

5. Biersteker and Eckert, *Countering the Financing of Terrorism*, p. 2.

6. U.S. Department of the Treasury, *Testimony of David D. Aufhauser*.

7. Marc Parker and Max Taylor, "Financial Intelligence: A Price Worth Paying?" *Studies in Conflict & Terrorism* 33(11) (2010), p. 949.

8. Biersteker and Eckert, *Countering the Financing of Terrorism*, p. 2.

9. Alex Schmid, "Terrorism—The Definitional Problem," *Case Western Reserve Journal of International Law* 36(2) (2004), pp. 375–419.

10. For detailed analyses, see chapters 2–9 in Biersteker and Eckert, *Countering the Financing of Terrorism*.

11. Iain Cameron, "Terrorist Financing in International Law," in Ilias Bantekas, ed., *International and European Financial Criminal Law* (London: Butterworths/Lexis Nexis, 2006), p. 66.

12. George W. Bush, *President Freezes Terrorists' Assets*. The White House, 24 September 2001. Available at www.whitehouse.gov/news/releases/2001/09/# (accessed 14 May 2007).

13. Oldrich Bures, *EU Counterterrorism Policy: A Paper Tiger?* (Burlington, VT: Ashgate, 2011); Eleni Tsingou, *Global Governance and Transnational Financial Crime: Opportunities and Tensions in the Global Anti-Money Laundering Regime*, CSGR Working Paper No 161/05. May 2005. Available at http://wrap.warwick.ac.uk/1959/1/WRAP_Tsingou_wp16105.pdf (accessed 28 July 2011); William Vlcek, "Securitization Beyond Borders: Exceptionalism Inside the EU and Impact on

Policing Beyond Borders European Measures to Combat Terrorist Financing and the Tension Between Liberty and Security," Challenge Working Paper Work Package 2. September 2005. Available at http://www2.lse.ac.uk/internationalRelations/centresandunits/EFPU/EFPUpdfs/EFPUchallengewp1.pdf (accessed 20 January 2008).

14. For more information about CTC, see http://www.un.org/sc/ctc

15. Also known as "targeted sanctions" because unlike the comprehensive sanctions that have been traditionally used by the international community against states, they are specifically tailored to directly effect only a limited number of individuals and/or groups associated with the governing elite. See David Cortright and George A Lopez, *Smart Sanctions: Targeting Economic Statecraft* (Boulder, CO: Lynne Rienner Publishers, 2002).

16. For the most current list, see http://www.un.org/sc/committees/1267/consolist.shtml

17. See Martin Nettesheim, "U.N. Sanctions Against Individuals—A Challenge to the Architecture of European Union Governance," *Common Market Law Review* 44 (2007): 567–600, and Iain Cameron, "UN Targeted Sanctions, Legal Safeguards and the European Convention on Human Rights," *Nordic Journal of International Law,* 72(2) (2003), pp. 159–214.

18. Cameron, "Terrorist Financing in International Law," p. 89.

19. Currently, the full FATF membership includes thirty-one nations and two international bodies, representing a high percentage of the world's financial activity. One hundred and thirty jurisdictions representing more than 85 of the world's population and 90–95 percent of economic output have made political commitments to implement FATF recommendations. Gardner, "Terrorism Defanged: The Financial Action Task Force and International Efforts to Capture Terrorist Finances," p. 158.

20. The list of all Forty Recommendations are available at http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

21. The list of 9 Special Recommendations is available at http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html.

22. The UN Security Council has stopped short of adopting a Chapter VII resolution ordering states to enforce the FATF's recommendations, but it has "strongly urged" them to do so in UN SCR 1617.

23. Liliya Gelemerova, "On the Frontline Against Money Laundering: The Regulatory Minefield," *Crime Law Soc Change* 52 (2009), p. 36.

24. Despite substantial differences between their legal statuses, size, and competences, FIUs purposes are the same in all countries: "[R]eceiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation." Mara Wesseling, *New Spaces Governing the EU's Fight Against Terrorism Financin.* Paper presented at the Annual Meeting of the ISA's 50th Annual Convention "Exploring the Past, Anticipating the Future," New York City, 15 February 2009. Available at http://www.allacademic.com/meta/p311342_index.html (accessed 21 February 2010).

25. Marcy M. Forman, "Combating Terrorist Financing and Other Financial Crime Through Public Sector Partnerships," *Journal of Money Laundering Control* 9(1) (2006), p. 112.

26. Karen Lund Petersen, "Risk, Responsibility and Roles Redefined: Is Counterterrorism a Corporate Responsibility?" *Cambridge Review of International Affairs* 21(3) (2008), p. 409.

27. Antoinette Verhage, "Between the Hammer and the Anvil? The Anti-Money Laundering-Complex and Its Interactions with the Compliance Industry," *Crime Law Soc Change* 52 (2008), p. 9.

28. Wesseling, *New Spaces Governing the EU's Fight Against Terrorism Financing*, p. 2.

29. Parker and Taylor, "Financial Intelligence: A Price Worth Paying?" p. 953.

30. Gilles Favarel-Garrigues, Thierry Godefroy, and Pierre Lascoumes, "Reluctant Partners? Banks in the Fight against Money Laundering and Terrorism Financing in France," *Security Dialogue* 42(2) (2011), p. 181.

31. Financial Action Task Force, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*. June 2007. Available at http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf (accessed 21 November 2008).

32. Barry R. Johnston and Ian Carrington, "Protection the Financial System from Abuse: Challenges to Banks in Implementing AML/CTF Standards," *Journal of Money Laundering Control* 9(1) (2006), p. 50.

33. Joras Ferwerda et al., *Performing in the Books—Assessing Countries' Anti Money Laundering Policy in the Light of Strategic Reporting*. Paper presented at the 6th ECPR General Conference, University of Iceland, Reykjavik, Iceland, 25–27 August 2011. Available at www.ecprnet.eu/MyECPR/proposals/reykjavik/uploads/papers/2734.pdf (accessed 1 September 2011).

34. Wesseling, *New Spaces Governing the EU's Fight Against Terrorism Financing*, pp. 8–9.

35. Among the EU Member States, for example, 12 FIUs are administrative FIUs, 11FIUs have a law enforcement basis, 3 FIUs are hybrid or independent and one is judicial. European Commission, *Report from the Commission on the Implementation of the Council Decision of 17 October 2000 Concerning Arrangements for Cooperation Between Financial Intelligence Units of the Member States in Respect of Exchanging Information (2000/642/JHA), COM(2007) 827 Final*. December 2007. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0827:FIN:EN:HTML (accessed 30 May 2008).

36. Select Committee on Economic Sanctions House of Lords, "Memorandum by Professor Peter Fitzgerald, Stetson University College of Law," *The Impact of Economic Sanctions*, Volume II: Evidence. 9 May 2007. Available at http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeconaf/96/96ii.pdf (accessed 26 January 2009).

37. Nikos Passas, "Setting Global CFT Standards: A Critique and Suggestions," *Journal of Money Laundering Control* 9(3) (2006), p. 283.

38. Council of the European Union, *Council Common Position 2009/468/CFSP of 15 June 2009 updating Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Common Position 2009/67/CFSP*, OJ L 151/48.

39. House of Lords, "Memorandum by Professor Peter Fitzgerald," p. 156.

40. The Economist, "Getting to Them Through Their Money," *The Economist*, 27 September 2001.

41. Vlcek, "Securitization Beyond Borders," p. 18.

42. Cameron, "Terrorist Financing in International Law," p. 81.

43. House of Lords, "Memorandum by Professor Peter Fitzgerald," p. 150.

44. Favarel-Garrigues, Godefroy, and Lascoumes, "Reluctant Partners?," p. 192.

45. Vlcek, "Securitization Beyond Borders," p. 12.

46. Friedrich Schneider and Paul Caruso, *The (Hidden) Financial Flows of Terrorist and Transnational Crime Organizations: A Literature Review and Some Preliminary Empirical Results*, Economics of Security Working Paper 52. August 2011. Available at http://www.economics-of-security.eu/sites/default/files/WP52_Schneider_Hidden_Financial_Flows.pdf (accessed 28 August 2011).

47. John Howell & Co., *Independent Scrutiny: The EU's Efforts in the Fight Against Terrorist Financing in the Context of the Financial Action Task Force's Nine Special Recommendations and the EU Counter Terrorist Financing Strategy* (European Commission, 1 February 2007), p. 8.

48. Cameron, "Terrorist Financing in International Law," p. 72.

49. National Commission on Terrorist Attacks Upon the United States, *Monograph on Terrorist Financing*. 21 August 2004. Available at http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf (accessed 9 February 2006).

50. Vlcek, "Securitization Beyond Borders," p. 22.

51. Passas, "Setting Global CFT Standards," p. 283.

52. Banker editor, "Money Laundry Monitor," *The Banker,* 6 Octobert 2003. Available at http://www.thebanker.com/Tech-Trading/Technology/Money-laundry-Monitor (accessed 26 June 2011).

53. R. T. Naylor, *Wages of Crime* (Ithaca: Cornell University Press, 2004), p. 30.

54. Tsingou, *Global Governance and Transnational Financial Crime*, p. 4. Also see Friedrich Schneider, *Money Laundering and Financial Means of Organized Crime: Some Preliminary Empirical Finding*, Economics of Security Working Paper 26. February 2010. Available at http://www.economics-of-security.eu/sites/default/files/WP26_Money%20Laundering%20and%20OC_Empirical%20Findings.pdf (accessed 28 August 2011).

55. PriceWaterhouseCoopers, *Economic Crime: People, Culture and Controls. The 4th Biennial Global Economic Crime Survey.* 2007. Available at http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/pwc_2007gecs.pdf (accessed 20 January 2008).

56. Verhage, "Between the Hammer and the Anvil?," p. 12.

57. Tsingou, *Global Governance and Transnational Financial Crime*, pp. 3–4.

58. Cited in Tsingou, *Global Governance and Transnational Financial Crime*, p. 7.

59. Tsingou, *Global Governance and Transnational Financial Crime*, p. 11.

60. Beth A. Simmons, "The International Politics of Harmonisation: The Case of Capital Market Regulation," *International Organisation* 55(3) (2001), pp. 605–607.

61. Johnston and Carrington, "Protection the Financial System from Abuse," p. 60.

62. See Jeroen Gunning, "Terrorism, Charities, and Diasporas: Contrasting the Fundraising Practises of Hamas and al Qaeda Among Muslims in Europe," in Thomas J. Biersteker and Sue E. Eckert, eds., *Countering the Financing of Terrorism* (London: Routledge, 2007), pp. 93–125.

63. Johnston and Carrington, "Protection the Financial System from Abuse," p. 58.

64. Wesseling, *New Spaces Governing the EU's Fight Against Terrorism Financing*, p. 2.

65. Vlcek, "Securitization Beyond Borders," p. 17.

66. For example, European Parliament and the European Council. *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing*, OJ L 309.

67. For example, UK Joint Money Laundering Steering Group (JMLSG) comprehensive guidance manual, available at the JMLSG website: http://www.jmlsg.org.uk

68. For example, the Wolfsberg Group of Banks principles. Available at www.wolfsbergprinciples.com

69. Gelemerova, "On the Frontline Against Money Laundering," pp. 41–42.

70. Vlcek, "Securitization Beyond Borders," p. 18.

71. Előd Takats, *A Theory of Crying Wolf: The Economics of Money Laundering Enforcement*, IMF Working Paper 07/81. 8 April 2007, Available at www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf (accessed 8 September 2011).

72. John Howell & Co., *Independent Scrutiny*, p. 28.

73. Verhage, "Between the Hammer and the Anvil?," p. 15.

74. Ibid., p. 23.

75. Cameron, "Terrorist Financing in International Law," p. 74.

76. House of Lords, "Memorandum by Professor Peter Fitzgerald," p. 156.

77. UN Analytical Support and Sanctions Monitoring Team, *First Report of the Analytical Support and Sanctions Monitoring Team Appointed Pursuant to Resolution 1526 (2004) Concerning Al-Qaida and the Taliban and Associated Individuals and Entities*, S/2004/679. Available at http://daccessdds.un.org/doc/UNDOC/GEN/N04/469/63/PDF/N0446963.pdf?OpenElement (accessed 25 August 2004).

78. Home Office, *The Report of the Official Account of the Bombings in London on 7 July 2005*, HC 1087. 11.5. London: The Stationery Office. Available at http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf (accessed 18 January 2009).

79. Loretta Napoleoni, "Terrorism Financing in Europe," in Jeanne K. Giraldo and Harold A. Trinkunas, eds., *Terrorism Financing and State Responses: A Comparative Perspective* (Stanford, CA: Stanford University Press, 2007), p. 176.

80. Donohue estimated the annual costs of Provisional Irish Republican Army at £1,5 million but noted that some of the smaller IRA splinter groups, such as Continuity IRA, operated on a budget of £30,000 or less. Donohue, *The Cost of Counterterrorism: Power, Politics, and Liberty*, p. 128.

81. M. J. White cited in Biersteker and Eckert, *Countering the Financing of Terrorism*, p. 13.

82. Al Qaeda, for example, spends only about 10 percent on operational costs. Biersteker and Eckert, *Countering the Financing of Terrorism*, p. 8.

83. Cited in Biersteker and Eckert, *Countering the Financing of Terrorism*, p. 8.

84. Wesseling, *New Spaces Governing the EU's Fight Against Terrorism Financing*, p. 11.

85. John Howell & Co., *Independent Scrutiny*, p. 94.

86. Takats, *A Theory of Crying Wolf*, pp. 27–30.

87. Peter Reuter and Edwin Truman, *Chasing Dirty Money: The Fight Against Money Laundering* (Washington, D.C.: Peterson Institute for International Economics, 2004), p. 15.

88. Ivo Hubli and Geiger Hans, *Regulatory Burden: Die Kosten der Regulierung von Vermoegensverwaltungsbanken in der Schweiz*, ISB Working Paper 37. April 2004. Available at www.isb.unizh.ch/publikationen/pdf/workingpapernr37.pdf (accessed 28 August 2011).

89. Johnston and Carrington, "Protection the Financial System from Abuse," p. 57.

90. Ibid.

91. Hans Geiger and Oliver Wuensch, "The Fight Against Money Laudering—An Economic Analysis of a Cost-Benefit Paradoxon," *Journal of Money Laundering Control* 10(1) (2007), p. 92.

92. Jackie Harvey and Sin Fung Lau, "Crime-Money, Reputation and Reporting," *Crime Law Soc Change* 52 (2009), pp. 58–59.

93. Tsingou, *Global Governance and Transnational Financial Crime*, p. 15; Parker and Taylor, "Financial Intelligence," p. 951.

94. Verhage, "Between the Hammer and the Anvil?" p. 27.

95. Ibid., p. 13.

96. Gelemerova, "On the Frontline Against Money Laundering," p. 48.

97. Harvey and Lau, "Crime-Money, Reputation and Reporting," p. 58.

98. Favarel-Garrigues, Godefroy, and Lascoumes, "Reluctant Partners," p. 185.

99. Harvey and Lau, "Crime-Money, Reputation and Reporting," pp. 58–59.

100. Verhage, "Between the Hammer and the Anvil," p. 30.

101. Cited in Vlcek, "Securitization Beyond Borders," pp. 13–14.

102. Takats, www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf, p. 4.

103. Takats, *A Theory of Crying Wolf*, pp. 21–22.

104. Michael Brzoska, *The Role of Effectiveness and Efficiency in the European Union's Counterterrorism Policy: The Case of Terrorist Financing*, Economics of Security Working Paper 51. July 2011. Available at http://www.diw.de/documents/publikationen/73/diw_01.c.377385.de/diw_econsec0051.pdf (accessed 28 August 2011).

105. The other six EU Member States reported between 132–906 cases for 2008. Only in the case of Germany, where all STRs are legally bound to result in the initiation of criminal proceedings, the number exceeded 1,000 cases (7,349 in 2008). Cynthia Tavares, Geoffrey Thomas, and Mickael Roudaut, *Money Laundering in Europe: Report of Work Carried Out by Eurostat and DG Home Affairs*, Eurostat Methodologies and Working Paper. 2010. Available at epp.eurostat.ec.europa.eu/cache/ITY../KS-RA../KS-RA-10-003-EN.PDF (accessed 28 August 2011).

106. Cameron, "Terrorist Financing in International Law," p. 105.

107. Brzoska, *Role of Effectiveness and Efficiency in the European Union's Counterterrorism Policy*, p. 13.

108. Favarel-Garrigues, Godefroy, and Lascoumes, "Reluctant Partners," p. 185.

109. Verhage, "Between the Hammer and the Anvil," p. 25.

110. Ibid., pp. 25–26.

111. M. Yeandle et al., *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions*. Corporation of London, 2005. Available at http://www.icaew.com/index.cfm/route/144554/icaew_ga/pdf (accessed 14 May 2011).

112. Geiger and Wuensch, "The Fight Against Money Laundering," p. 91.

113. Verhage, "Between the Hammer and the Anvil," p. 23.

114. John Howell & Co., *Independent Scrutiny*, p. 39.