The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1368-5201.htm

Terrorism financing and the threat to financial institutions

Jeffrey Simser
Civil Remedies for Illicit Activities Office, Ministry of the Attorney General, Toronto, Canada

Abstract

Purpose – The purpose of this paper is to explore countering the financing of terrorism and its impact on financial institutions.

Design/methodology/approach – Actual examples of terrorist financing are considered, as well as the international and Canadian framework for financial institutions.

Findings – The system for countering the financing of terrorism can be improved to lower costs and risks to financial institutions and to enhance actionable intelligence. A balance must be sought between the objective, actionable intelligence and the mechanism used to advance that objective.

Research limitations/implications – There is limited research on terrorism financing and little statistical data.

Practical implications – Some simple and modest reforms to the framework are suggested; policy makers need to consider their goals and revaluate the existing framework.

Originality/value – There is little writing in this area. This paper would be of interest to financial institutions, regulators, law enforcement and the intelligence community.

Keywords Financial institutions, Terrorism, Money laundering, Anti-money laundering, Terrorist financing, Countering financing of terrorism, Asset forfeiture, Financial intelligence units

Paper type Research paper

> Today there are about 200 million people working and living outside their home country [. . .] together in one place they would be the world's fifth most populous country. Remittances were estimated at more than $300 billion in 2007 alone (Mavin, 2008).

Combating or countering the financing of terrorism (CFT) involves finding relatively small sums in an ocean of money[1]. How does a banker in Paris or Toronto know whether she is looking at one of the countless remittances from the Pinoy Diaspora or funding for Abu Sayyaf? That question lies at the heart of the impact of CFT on financial institutions. The question is additionally complicated given that the quantum of terrorist money in use seems relatively modest. The bombing of the London transit system in 2005 cost an estimated $15,000 (all figures in this paper are US$ amounts); the 2000 attack on the USS Cole in Yemen cost $10,000 as did the 2004 train bombings in Madrid; even the notorious 9/11 attack cost less than $500,000 to carry out[2]. Financial institutions face a great challenge in identifying patterns that would distinguish terrorist cells from other legitimate clients, particularly in the context of billions of transactions. Closer examination reveals that the amounts are higher: outside of specific activities, a terrorist organization requires money to sustain infrastructure. This paper examines CFT and the impact on financial institutions.

The views expressed in this paper are those of the author personally and do not represent the views of the Government of Ontario or of the Ministry of the Attorney General.

Journal of Money Laundering Control
Vol. 14 No. 4, 2011
pp. 334-345

1368-5201
DOI 10.1108/13685201111173811

For students of money laundering, terrorist financing is a counter-intuitive subject. Generally, terrorist financing starts out with legitimate money, often sourced in immigrant remittances and charitable organizations. That money then flows into the hands of a terrorist organization to sustain infrastructure and fund attacks. Terrorist attacks have many motivations, but profit is not one of them. This is not to say that terrorist groups are beyond committing crime to raise funds: Abu Sayyaff committed kidnappings for ransom in the Philippines and Malaysia. The profit from that activity is not an end in itself; the profit merely supports the larger objectives of the organization. In contrast, a drug dealer launders money, sourced in his illicit trading, so that the wealth might be enjoyed; the provenance is disguised to create a veneer of legitimacy and to evade law enforcement. A terrorist may disguise the money to avoid detection; the money itself is used to maintain an organizations' infrastructure or to carry out a specific act of destruction. Organized crime figures not only want to keep as much of their money as possible, they are likely to return to the activities that make profit for them. For terrorists, acts tend to be singular and excess money amplifies risk of detection. This is particularly so given CFT efforts over roughly the past 20 years. The current trend seems to have terrorist groups funding their activities locally, through fraud, drug dealing and so on.

Money as lifeblood: Al-Qaeda in Iraq

A 2008 report examined a series of personnel records seized from Al-Qaeda in Iraq's (AQI) safe houses. While there are limitations to the report[3], it offers an interesting window into one terrorism operation. The report tracked 590 foreign fighters entering Iraq through Syria from 21 countries. Generally, individuals were recruited through personal contacts, brothers or co-religionists in their home country; those personal contacts in turn linked to contacts in Syria for travel. The recruits themselves donated money (making an average payment of $2,535), as did sympathetic supporters. AQI then struggled as a terrorist organization to calibrate the use of force and suicide bombings in hostile areas to achieve political ends. While some Iraqis may share AQI's political goal, repelling foreign armed forces, few want to live next door to a suicide bomber. AQI operated in an environment made hostile not only by the coalition of troops, but also by many local Iraq citizens. Despite the risk of exposure or capture, AQI retained extensive and detailed records: spreadsheets, expense reports, policy memos, signed contracts, managerial reports and receipts. Clearly, AQI struggled to sustain itself on limited funds. Attempts to fundraise locally, including through coercion, were not only unsuccessful: they were counterproductive. Extorting money is inconsistent with winning hearts and minds. AQI's expenses included weapons and equipment (38.3 percent of their budget), personnel (19.6 percent), logistics (18.4 percent) outgoing transfers (13.6 percent) and other (10 percent). The expenses related to equipment included weapons and ammunition (roughly 60 percent of those outlays) along with binoculars, cell phones and vehicles. The personnel and logistic outlays represented the costs of bringing foreign fighters into Iraq and sustaining them. Money is clearly critical infrastructure for AQI as a terrorist group; as in any organization, there is a need to husband scarce resources. Managers everywhere maintain ledgers, track expenses and revenues to manage their financial affairs. For a terrorist organization, such expense claims and receipts for donations represent massive operational risk: the documentation identifies individual operatives and exposes the entire cell of the organization. The need

to manage money trumped the security risk; the presence of extensive documentation supports the contention that for AQI at least money is the lifeblood of a terrorist operation.

Multilateral initiatives and terrorism financing

Prior to the tragic events of 9/11, CFT paled in priority in the USA compared to the concerted American effort to address money laundering (Levitt and Jacobsen, 2008; Simser, 2008). Internationally, the UN Security Council had passed a 1999 resolution respecting Al-Qaeda's presence in Afghanistan (Resolution 1267). Resolution 1267 had teeth: an air travel ban and an asset freeze were imposed on the Taliban. The resolution was adopted under Chapter VII making it a mandatory obligation of Member States under international law. As will be seen below, the European Union (EU) courts took some issue with what "mandatory" in fact meant. The General Assembly passed a Convention for the Suppression of Financing of Terrorism in 1999 (Resolution 54/109) and urged states to become parties to it. Following attacks on the USS Cole, a more robust resolution was passed (1333). Following 9/11, there was a flurry of enactments respecting terrorist financing, including UN Resolutions 1373 and 1390, both adopted under the mandatory provisions of the UN Charter[4]. The US Patriot Act and the eight special recommendations of the Financial Action Task Force were put forward (Gurale, 2008, pp. 3-10). In January of 2009, a working group of multilateral organizations reviewed CFT measures and noted that:

- Funds sustain an organization and support specific attacks.
- Following the money yields "valuable intelligence that may be unavailable from other sources".
- When moved electronically, money leaves a trail.
- Targeted measures respecting groups like Al-Qaeda have been effective but need to be balanced with intelligence imperatives. If a network is shut down or sent to ground, the intelligence opportunity is lost.
- The CFT regime needs to contain adequate procedural safeguards.

This latter point, CFT safeguards, arises in two contexts. The challenge associated with listed individuals associated with terrorism is discussed in detail below. Second, the report notes that any CFT measure needs to be accompanied by typologies. This is an area where particularly multilateral bodies could do further work. As financial institutions know more about patterns of activity, they are better placed to make informed choices proportionate to risk (The World Bank, 2009).

The Canadian approach

Following the tragic events of 9/11, Canada made a number of changes respecting terrorist financing. We reformed our security apparatus: the Department of Public Safety and Emergency Preparedness was created; the Communications Security Establishment (CSE) were given new powers of intercept; an Integrated Threat Assessment Centre was created. Canada spends roughly $25 billion a year on national security (Stoffman, 2009, pp. 34-5). We also amended our criminal law on CFT by adding Part II.1 to the Criminal Code[5]. The Code's CFT provisions revolve around two definitions: terrorist activity and terrorist group. Terrorist activities include acts

or omissions in or outside of Canada that relate to offences under certain international protocols and conventions[6] signed between 1970 and 1999 (ranging from hijacking to CFT issues) or that meet a very specific definition. Under this latter provision, an act or omission, in or outside of Canada, is terrorist activity if:

(1) There is or in part a political, religious or ideological purpose or cause (although this has been read out of the definition by the courts and likely does not apply)[7].

(2) Committed "in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security" (which includes economic security and includes acts intended to compel someone to do something or refrain from doing something).

(3) The act or omission must intentionally:
   - cause death or serious bodily harm to a person by the use of violence; or
   - endanger a person's life.

Additionally:

- If there is property damage or serious interference or disruption caused as a likely result of the three international acts, that will constitute terrorist activity.
- The definition goes on to include conspiracy, attempt or threat to commit, accessory after the fact and counselling to commit.
- The definition excludes acts committed in an armed conflict to the extent they are governed by other rules of international law.

The second pivotal definition in Part II.1 is "terrorist group" which consists of either a listed entity or an entity that has as one of its purposes or activities facilitating terrorist activity[8].

The financing of terrorism is criminalized in a number of ways. Anyone who, directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out:

- Terrorist activity in violation of one of the listed international protocols or conventions.
- "Any other act or omission intended to cause death or serious bodily harm to a civilian or any other person not taking an active part in the hostilities in a situation of armed conflict". The purpose of such an act not be, by its name, to intimidate the public or compel a government or international organization to do or refrain from doing an act[9].

The penalty upon conviction is up to ten years imprisonment.

There are also provisions that prohibit and criminalize making property available for terrorist purposes[10] as well as using or procession property for terrorist purposes[11].

Canada's FIU

To investigate terrorism financing offences, law enforcement have a number of tools available to them. Canada's FIU or Financial Investigation Unit, FINTRAC, was created in 2000. FINTRAC's mandate is to collect financial information, usually in the form of

currency and suspicious transaction reports, conduct analysis and if appropriate share intelligence with law enforcement (police services, the Canadian Security Intelligence Service (CSIS), CSE, as well as foreign FIU's). Banks and other financial entities[12] in addition to their anti-money laundering work must file reports on terrorist property holdings. The obligation to file arises when the institution knows or believes a terrorist or terrorist group controls the property. That knowledge and belief may come from the institution's own knowledge of their client or from a reference to a listed entity[13].

FINTRAC receives over one-million filings, almost all in electronic form, every month; while that number includes both CFT and AML filings, financial institutions are clearly (and understandably) making protective filings (Flemming, 2009; Gordon, 2009). FINTRAC data mine the 12 million or so filings to produce disclosures (only FINTRAC has access to the database). In 2007-2008, this produced 210 case disclosures, 29 of which were related to terrorist financing (FINTRAC, 2008, p. 16)[14]. Those 29 reports merely provide raw data based on currency and suspicious transaction reports filed by financial institutions and others. They can be used as intelligence, particularly by agencies like CSIS. If a prosecution is desired, further investigation is necessary. Law enforcement can build a case using old-fashioned police work: surveillance, interviews, public record checks and so on. Police can also seek production orders as well as search warrants[15]. Wiretaps can be judicially authorised under Part VI of the Code.

FIU's can play an important role in respect of financial institutions and CFT. There are some useful typologies produced by multilateral bodies like FATF[16]. However, in Canada, the suspicious activity report system in Canada tends to flow in one direction only: financial institutions file the mandated reports; FINTRAC conducts analysis on some of those reports; law enforcement may see the product but financial institutions generally do not. While we impose a proscriptive burden on financial institutions, we do not treat them as partners and could do a better job of providing them with the tools to make effective risk-based choices.

Asset forfeiture

The criminal law process normally invoked for proceeds of crime and offence-related property does not apply in Canada for terrorist assets. The Code instead applies a process akin to civil or non-conviction-based forfeiture. A law enforcement officer may, on an *ex parte* basis, go before the judge of a federal court and with affidavit evidence stating there are reasonable and probable grounds to believe that property exists for which a forfeiture order might be sought under s. 83.14(1). If the court is satisfied on a balance of probabilities that the property was owned or controlled by or on behalf of a terrorist group, it shall be forfeited. Similarly, property that has or will be used to carry out terrorist activity can be forfeited[17].

There are some challenges with this process[18]. The federal court was originally created to deal with tax matters, although its mandate has increased and grown. Unlike courts of originating jurisdiction, however, the federal court's rules are not ideally suited to civil *in rem* forfeiture proceedings. The provisions of Part II.1 do not set out a detailed procedure to follow; in contrast Part VI, wiretaps, is very proscriptive and an officer is told explicitly what their underlying affidavit must attest to[19]. The federal court is permitted to seal an order, although there are two processes that have not been perfectly reconciled. Federal court rules of procedure, specifically Rules 151 and 152[20], require a motion to seal a file; the court must weigh the public interest in open and accessible court

proceedings against the need for confidentiality. The Code process, established under s. 487.3 requires the court to consider very different factors: would the ends of justice be subverted by disclosure and is the importance of access to information outweighed? The Code process is specific and mandated by statute; as such, it likely trumps the procedural rules of the court; ultimately those rules could do with amendment.

The knowledge challenge

Under the Code, no one in Canada, including a financial institution, can knowingly deal with assets belonging to a terrorist group. Financial institutions are in fact protected from civil liability if they take reasonable steps like closing an account, when confronted with the knowledge that there is a terrorist activity implication[21]. In a KYC world, where know your client is the standard expectation for financial institutions, knowledge of a terrorist link compels the institution to take certain action. When does a financial institution have knowledge? For example, if police serve the bank with a production order seeking terrorist financing-related information, does the bank have an obligation to immediately close the account? In many cases, law enforcement need the account to stay open and to operate as they conduct their inquiries. This is particularly true if intelligence gathering is a priority. The Code provides for a ministerial exception whereby financial institutions will be permitted to continue operating the account[22]. Of course, anyone who has worked in government knows getting a Minister of the Crown to sign a comfort letter in the world of real-time investigations is never going to be easy or happen quickly[23].

The list-based approach

The EU, like many jurisdictions, has used a list-based approach to CFT. UN resolution 1267 was one in a series of resolutions designed to address Al-Qaeda, bin Laden and terrorist financing. The EU adopted regulations pursuant to their common foreign and security policy that prescribed the freezing of funds for listed entities. Two parties affected by the regulation challenged: Mr Kadi, a Saudi national and the Al Barakaat International Foundation; a charity created in Sweden. At first instance, the courts rejected the challenge; however, the Grand Chamber of the European Court of Justice struck the regulation. At first, instance the courts found that as the basis for the EU regulation lay in international law, specifically a UN resolution binding on Member States, it could not be challenged. On appeal, the court refused to be bound by the terms of Resolution 1267 and found that as a sovereign entity, any EU regulation of this nature could be the subject of curial review. On appeal, the court also accepted the contention of the two affected parties that their rights had been violated; indeed the court found that their rights had "patently not been respected". The court did give the EU a brief window during which the regulations could be made human rights compliant. In response, the freezing orders and restrictions against the affected parties were retained; however, the affected parties were given a brief narrative of the rationale behind those orders; further complaints by the affected parties were rejected (Shapiro and Byman, 2006; Lehnardt, 2007)[24]. The EU has, for the time being, treated that notice and response as an adequate human rights protection.

There is a second problem with the list-based approach. A list is only going to work if it is properly maintained and kept current. The UN consolidated list has seen a diminishing number of names added each year: in 2001, there were 278 listings; in 2007

there were only eight names added. Further, each year fewer assets are being restrained pursuant to this process (Gurale, 2008). Any self-respecting listed terrorist will not transact financially in his or her own name. While at a certain level, that is the point of the list in the first place, there is an inherent limitation as to how effective the list can be. Someone who will kill innocent civilians will be supine about identity theft to evade the list. Finally, the UN list focuses on Al-Qaeda and the Taliban, not reaching Sikh militants, Tamil Tigers and the like. While financial institutions can rely on private sector databases like World-Check, one wonders how that interfaces with the court challenges that we have seen in Europe and might reasonable expect to see in countries like Canada.

CFT and the need for flexibility

A CFT regime that treats terrorist organizations as uniform and static entities is bound to fail. Consider Al-Qaeda and the many forms it has taken over the last 20 years. Al-Qaeda was created during the anti-Soviet era in Afghanistan. As an organization, Al-Qaeda was funded through charities, directly solicited donations from Saudi Arabia and other countries. It was also formed at a time when foreign governments, including the USA were providing weapons and financial support to anti-Soviet forces through intermediaries such as the Pakistan Inter-Services Intelligence. Following the Soviet withdrawal in 1989, bin Laden undertook a strategy of diversifying sources of money, retaining traditional patrons while adding business enterprises (both licit and illicit). When Al-Qaeda moved from Sudan to Afghanistan in 1996 they acquired a new state sponsor, the Taliban regime. In 1998, following the Nairobi and Dar es Salaam embassy bombings and a US asset freeze, Al-Qaeda apparently developed new ventures including the gem trade. By 2005, the international focus on CFT had an impact on Al-Qaeda; in an intercepted letter[25] Al-Qaeda's second-in-command concedes that money is tight as a result of the lines of finance being cut and indeed asks his AQI counterpart for $100,000. The London and the Madrid bombings appear to have been funded locally; in the case of Madrid, crime in Spain played a critical role in acquiring the necessary funds. The financing of Al-Qaeda has changed. International CFT barriers mean that the central funding of terrorist activities like 9/11 has given way to a cellular structure whereby terrorist activities are funded locally (Stoffman, 2009)[26].

Financial institutions and reputational risk

In 2005, US officials discovered that the Macau-based Banco Delta Asia (BDA) had been a conduit for money from the North Korean Government. Some of that money came from a company dealing in illicit narcotics. The US Treasury Department designated BDA as a primary money laundering concern under the US Patriot Act. That designation created a serious financial impediment: BDA could not transact normally in US dollars. There was a graver implication: other financial institutions simply did not want to transact with BDA. North Korea's Government demanded the return of the money in the BDA accounts. Macau was happy to see the money go. Eventually, a deal was brokered whereby roughly $25 million flowed through the US federal reserve system into the Bank of Russia and eventually found its way to the North Korean regime through a small bank in Russia's far east (Loeffler, 2009, p. 101).

Financial institutions invest heavily in their image of probity and reliability; given recent events some institutions are trying to recover reputations undermined by the

credit crisis; those institutions can ill afford to be implicated in a terrorist financing scheme. A recent report from Europol suggests that terrorist financing continues apace. The report notes that there are generally two sources of money: legitimate sources, like charities; a wide range of criminal activities ranging from fraud and counterfeiting to burglary, kidnapping and extortion (TE-SAT, 2009). Financial institutions are protected from a reputational perspective as long as they run a compliant CFT regime.

Class action

Financial institutions have to consider all risks that might affect their bottom line. Class actions to defer terrorism pose such a risk. On June 2, 2009, Bill C-35 was introduced in the federal parliament. Victims of terrorism can sue perpetrators of terrorism and their supporters. A financial institution that transacts for a terrorist organization not only violates sections of the code including 83.02 and 83.03, they could be named in a class action lawsuit if C-35 becomes law. Recently, similar legislation was considered in a New York State case involving Arab Bank PLC. Victims of suicide bombings in Israel sued Arab Bank under the Anti-Terrorism Act[27]. In 2005 and 2007, the Arab Bank's motions to dismiss the action on the grounds that the bank had no knowledge of the suicide bombs was discussed. In 2009, amongst the various allegations, the plaintiffs alleged that Arab Bank not only supported the infrastructure of groups like HAMAS, the bank also administered funds to the families of Palestinian martyrs, who each received $5,316.06. The litigation continues and a recent effort by Arab Bank to seek a contribution from Israeli banks was not successful[28].

CFT and displacement

As CFT measures are being felt around the world, there is a displacement effect. Recently, it seems unlikely that a known terrorist or terrorist organization would place money into its account and wire that money on to an operative. As noted above, Al-Qaeda recognizes that the old pathways for raising and moving money are gone. There are several new pathways. First, terrorist organizations can avail themselves of the techniques used by organized crime to launder money. That is, an imperfect solution to the extent that international anti-money laundering measures will interdict the activity. Second, organizations are moving to other methods of moving money: gem smuggling, bulk cash smuggling and cash couriers to move money. Trade-based money laundering is another technique. These methods entail costs and risks for a terrorist organization; in the case of cash smuggling, the risk of capture by law enforcement might actually be less than the risk of loss by theft or armed robbery. Terrorist organizations need to devote resources and personnel to move money, resources diverted away from efforts to plan and execute attacks. In the meantime, law enforcement needs to refine efforts to disrupt and dismantle terrorism.

Conclusions

In a press conference on December 19, 2005, President Bush lashed out at the *New York Times* who had published details on a secret NSA program. He told reporters that President Clinton had unimpeachable evidence in August of 1998 that bin Laden was personally behind the twin bombings of US embassies in Nairobi and Dar es Salaam. Clinton knew this because intelligence agencies in the USA and the UK had been monitoring bin Laden's satellite phone as well as a fax machine in France. The phone was

turned off after the media reported its use. In August 1998, US cruise missiles were fired at training camps and missed bin Laden's by only hours. A *Washington Post* reporter reported that President Bush's claims (which had been validated by the 9/11 commission) were in fact urban myth. According to the *Post*, the existence of the phone had already been reported to the press two years earlier, in 1996; the source of the information: the Taliban Government and possibly bin Laden himself (Kessler, 2005, p. A02).

For the purposes of this paper, the bin Laden satellite phone story may be true or an urban myth. Underlying the story is the notion that we need to think strategically about the tools available in the fight against terrorism, whether they be phones or financial records. Money is the lifeblood of a terrorist organization. As money moves electronically through our financial system, a trail is left. Policy makers have adapted AML techniques used in the financial sector to address CFT. Not only are there reporting obligations, financial institutions are at risk criminally if they knowingly transact on terrorist assets. The cost of this regulatory burden is significant to financial institutions. The burden is necessary. Terrorist organizations have had to change their method of operating, specifically as a result of these barriers. There is a benefit to financial institutions from compliance with this system and potentially heavy costs for non-compliance. Riggs Bank and BDA paid heavily in terms of reputation for being implicated in AML and CFT issues. The credit crisis of 2008 has harmed reputations generally in the financial services industry; a process that mitigates risk has unseen value.

What can be done to improve the CFT? If the desired end product is actionable intelligence, the system needs tweaking. There is every incentive for a financial institution to make as many protective filings as they can. There is little incentive for financial institutions to take risks and separate the extraordinary from the ordinary. Two things can change this. First, law enforcement can do a better job of sharing information. Bankers, by their profession, keep secrets. Surely there is a way of carefully providing information. Lists need to be updated. Risks need to be explained at some level. Second, if the flow of information is only in one direction, financial institutions are not really partners. If they are not partners, if they do not have a stake in the enterprise, as a group financial institutions will only be engaged to the extent that they compelled to do so.

One solution, in Canada at least, is to formalize an information sharing protocol whereby targeted intelligence can be shared with major financial institutions. Those institutions could in turn designate a relatively high-ranking official, like a compliance and anti-money laundering officer, to receive that information. The designated bank official could be subjected to security background checks; an audit process could be put into place to ensure that the information is used properly. If that is put in place, another question needs to be answered: why are we doing this? If it is for intelligence, then a better process needs to be put in place to protect financial institutions from liability (including liability from class actions). If the primary objective is prosecution, then other safeguards may be needed to ensure that the shared intelligence is actionable (HM Treasury, 2007, p. 56)[29].

Finally, policy makers need to think through why we have a CFT regime. There is a paucity of research and very little through which a CFT regime can be measured and evaluated (Levi, 2008). Further, the current CFT model has adapted the AML process for its needs. If the goal of policy makers is to prosecute terrorists and freeze their assets, that system, while imperfect, has merit. If the goals are different, if policy makers want intelligence to know who is who and what they are up to, the system has a number of

limitations. On the one hand, we do not want financial institutions transacting on terrorist assets; on the other, if a financial institution trying to avoid criminal liability shuts down an account, the intelligence opportunity is lost. Finally, as the experience with Al-Qaeda has shown, terrorist organizations evolve and change; as one pathway is shut down, the formal financial system, another is adopted like bulk cash smuggling. The very nature of the organizations themselves change too, from a command and control enterprise to a franchise enterprise in which operational control is devolved completely. A CFT system needs to be flexible and robust enough to address these challenges.

Notes

1. I am grateful for the assistance of Melany Doherty in the preparation of this paper and for the comments of Karim Rajwani, Frank Mauti and Michael DeFeo.
2. The Report of the Analytical Support and Sanctions Monitoring Team concluded that Al-Qaeda operations were not characterized by a high cost fee (www.un.org/sc/committees/1267/monitoringteam.html).
3. The documents were seized in a war zone and the locations were generally close to the Syrian border (Fishman, 2008). While the precise numbers are unknown, there appears to have been roughly 3,000 foreign fighters in Iraq at this time; records on 600 of those fighters seems to offer a decent sampling (Katzman, 2008).
4. Resolution 1373 required all states to take measures to freeze the assets of all terrorists and to criminalize terrorist financing. Resolution 1390 extended mandatory sanctions to include a travel ban, asset freeze and weapons prohibitions respecting members of Al-Qaeda, Usama bin Laden and the Taliban.
5. 2001, c. 41 (in force January 17, 2002). The provisions of this part are very complex and this paper only provides an overview. A forthcoming book on asset forfeiture by Simser and McKeachie (2012) will explore this provision more fully.
6. The Convention for the Suppression of Unlawful Seizure of Aircraft is signed at The Hague on December 16, 1970; the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation signed at Montreal on September 23, 1971; the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including diplomatic agents, adopted by the General Assembly (GA) of the UN on December 14, 1973; the International Convention against the Taking of Hostages (GA – December 17, 1979); Convention on the Physical Protection of Nuclear Material (Vienna/New York: March 3, 1980); Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (as supplemented, Montreal, February 24, 1988); Protocol for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Rome – March 10, 1988); Protocol for the Suppression of Unlawful Acts again the Safety of Fixed Platforms located on the continental shelf (Rome – March 10, 1988); International Convention for the Suppression of Terrorist Bombings (GA – December 15, 1997); International Convention for the Suppression of the Financing of Terrorism (GA – December 9, 1999).
7. *R.* v. *Khawaja* (2006), 214 CCC (3d) 399 (Ont. SCJ) leave to appeal refused by the SCC 216 CCC (3d) iv.
8. 83.01(1) defines terrorist group.
9. 83.02.
10. 83.03.
11. 83.04.

12. Which include life insurance companies, securities dealers, money service businesses, real estate brokers, casinos and dealers in precious stones and metals. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c. 17 at s. 5.
13. The area is complicated to navigate. See for example: United Nations Al-Qaeda and Taliban Regulations SOR/99-444; Regulations Establishing a List of Entities SOR/2002-284 Order Recommending that Each Entity Listed as of July 23, 2004, in the Regulations Establishing a List of Entities Remain a Listed Entity SI/2004-155; Order Recommending that Each Entity Listed as of July 23, 2006, in the Regulations Establishing a List of entities Remain a Listed Entity; SI/2006-133; Order Recommending that Each Entity Listed as of July 23, 2008, in the Regulations Establishing a List of Entities Remain a Listed Entity SI/2008-143.The bank regulator in Canada offers some assistance; see for example: www.osfi-bsif.gc.ca/app/DocRepository/1/eng/issues/terrorism/reminders/01-11-22_e.html
14. FINTRAC's enabling legislation is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2000.
15. ss. 487.012 and 487.013 if the Code; warrants to search are covered by s. 487.
16. www.fatf-gafi.org
17. s. 83.14, particularly subsection (5) and (1).
18. I am grateful for the thoughts of Sgts. Hill and MacDonald at the 2009 Symposium on Money Laundering (Toronto: Osgoode Hall, March 7, 2009).
19. See for example s. 184.2(2).
20. Passed under the Federal Court Act, 1998 pursuant to SOR/98-106.
21. s. 83.08(2).
22. 83.09 of the Code.
23. A simple change to the delegation provisions of section 25.1 of the Code could fix this problem.
24. *Yassin Abdullah Kadi and Al Barakaat International Foundation* v. *Council of the European Union and Commission of the European Communi*ties, Joined cases C-402/05 P and C-415/05 P, September 3, 2008, (ECJ), (EUR-Lex) the comment on rights was made at para 334; the response of the commission can be found in *Official Journal L* 322, 02/12/2008, pp. 25-6; see also Cardwell *et al.* (2009) which considers the case from a public international law perspective.
25. Para 6 of Ayman al-Zawahiri's letter 2005 to Abu Musab al-Zarqawi: "The brothers informed me that you suggested to them sending some assistance. Our situation since Abu al-Faraj is good by the grace of God, but many of the lines have been cut off. Because of this, we need a payment while new lines are being opened. So, if you're capable of sending a payment of approximately one hundred thousand, we'll be very grateful to you". Accessed July 6, 2009: www.weeklystandard.com/Content/Public/Articles/000/000/006/203gpuul.asp?pg=2
26. See Chapter 13 of the Bierstecker book (Levitt and Jacobsen, 2008; Simser, 2008). Canada's experience with the Toronto 18 is consistent with this.
27. 18 USC J §2332 and Foreign Nationals sued under the Alien Tort Claims Act 28 USC 1350.
28. *Little* v. *Arab Bank PLC* (2009) 611 F. Supp (2d) 233 (Dist. Crt, EDNY).
29. In the UK, there are on-going efforts to engage the private sector. For example, details of stolen passports can assist banks to determine whether they have been used to accounts.

References

Cardwell, P., French, D., White, N. and European Court of Justice (2009), "Money laundering and terrorist financing overview", *Int'l and Comparative LQ*, Vol. 58, p. 229.

FINTRAC (2008), *FINTRAC Departmental Performance Report for the Period Ended March 31*, available at: www.fintrac-canafe.gc.ca

Fishman, B. (Ed.) (2008), *Bombers, Bank Accounts and Bleedout*, Harmony Project, Combating Terrorism Centre, West Point, NY.

Flemming, J. (2009), Presentation to the 11th Annual Auto Theft Export Summit, Ottawa, May 9.

Gordon, R. (2009), "Trysts or terrorists?", *Wake Forest LR*, Vol. 43, p. 699.

Gurale, J. (2008), *Unfunding Terror*, Edward Elgar, Cheltenham, pp. 3-10.

HM Treasury (2007), *The Financial Challenge to Crime and Terrorism*, Her Majesty's Stationery Office, London, p. 56.

Katzman, K. (2008), *Al-Qaeda in Iraq: Assessment and Outside Links*, Congressional Research Service, Washington, DC, August 15.

Kessler, G. (2005), "File the Bin Laden phone leaks under urban myths", *Washington Post*, December 22, p. A02.

Lehnardt, C. (2007), "European court rules on UN and EU terrorist suspect blacklists", *American Society of International Law*, Vol. 11, p. 1.

Levi, M. (2008), "Lessons for countering terrorist financing from the war on serious and organized crime", in Biersteker, T. and Eckert, S. (Eds), *Countering the Financing of Terrorism*, Chapter 12, Routledge, London.

Levitt, M. and Jacobsen, M. (2008), "The US campaign to squeeze terrorist's financing", *Journal of International Affairs*, Vol. 62 No. 1, p. 67.

Loeffler, R. (2009), "Bank shots", *Foreign Affairs*, Vol. 88, p. 101.

Mavin, D. (2008), "Buck on a wire", *Financial Post Magazine*, October, p. 40.

Shapiro, J. and Byman, D. (2006), "Bridging the transatlantic counterterrorism gap", *Washington Quarterly*, Vol. 29, p. 33.

Simser, J. (2008), "Money laundering and asset cloaking techniques", *Journal of Money Laundering Control*, Vol. 11, p. 15.

Smser, J. and McKeachie, J. (2012), *Civil Asset Forfeiture in Canada*, Canada Law Book, Toronto (in press).

Stoffman, D. (2009), "Are we safe yet?", *The Walrus*, Vol. 6 No. 4, pp. 34-5.

TE-SAT (2009), *EU Terrorism Situation and Trend Report*, TE-SAT, The Hague, p. 40.

(The) World Bank (2009), *International Monetary Fund and United Nations Office of Drugs and Crime Final Report of the Counter Terrorism Implementation Task Force*, The World Bank, Washington, DC, p. 6 (January).

Corresponding author
Jeffrey Simser can be contacted at: jeff.simser@ontario.ca