

VOLUME FIVE

TERRORIST FINANCING

CHAPTER III: THE ROLES OF FEDERAL DEPARTMENTS AND AGENCIES IN EFFORTS TO SUPPRESS TERRORIST FINANCING

Many federal departments and agencies¹ are involved in national security matters:

- Canada Border Services Agency (CBSA);
- Canada Revenue Agency (CRA);
- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment (CSE)²;
- Department of Finance (Finance Canada);
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);
- Department of Fisheries and Oceans/Canadian Coast Guard;
- Department of Foreign Affairs and International Trade (DFAIT);
- Department of Justice (DOJ);
- Department of National Defence (DND) and the Canadian Forces (CF);
- Integrated Threat Assessment Centre (ITAC);
- Office of the Superintendent of Financial Institutions (OSFI);
- Privy Council Office (PCO);
- Public Safety Canada (PS); and
- Royal Canadian Mounted Police (RCMP).³

The focus of this chapter is on the roles of many of these agencies in attempts to suppress terrorist financing (TF). The role of the Canada Revenue Agency (CRA) is examined separately in Chapter VI.

¹ To simplify the narrative in this chapter, the terms “department” and “agency” are used interchangeably. The use of one term includes the other where the context requires.

² The official acronym is now CSEC, but the acronym CSE is still commonly used.

³ The agencies are not necessarily listed in order of the importance of their role in TF matters. Other documents and reports describe the inner workings of these agencies; see, for example, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [*A New Review Mechanism for the RCMP's National Security Activities*].

3.1 The Department of Finance (Finance Canada)

Finance Canada is the lead department in the federal government's overall initiative to combat money laundering (ML) and TF.⁴ It was placed in charge of the National Initiative to Combat Money Laundering in 2000, and remained at the helm when the Initiative was renamed the Anti-money Laundering and Anti-terrorist Financing Initiative (AML/ATF Initiative) after the enactment of the *Anti-terrorism Act*⁵ (ATA) in 2001. Two sections of Finance – Financial Crimes Domestic and Financial Crimes International – are responsible for money laundering and TF matters. Both sections are located in the Financial Sector Division of Finance.⁶

The Minister of Finance is responsible to Parliament for FINTRAC and for the Office of the Superintendent of Financial Institutions (OSFI).⁷

Canada is not unique in having a department such as Finance Canada in a lead policy and coordination role for TF matters.⁸ Finance Canada has a broad range of responsibilities in regulating and overseeing the financial sector and in policy development. It assesses proposed security initiatives to evaluate their financial cost, efficiency and potential impact on the economy.⁹ As part of this function, the Department is responsible for developing policy relating to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*¹⁰ (PCMLTFA) and its regulations¹¹. The PCMLTFA and its regulations provide the framework for Canadian initiatives against TF and money laundering.¹²

Finance Canada is also responsible for coordinating the activities of the AML/ATF Initiative, including consultations with stakeholders.¹³ Its specific goal in the AML/ATF Initiative is to protect Canada's financial sector from illicit uses, thus protecting its integrity.¹⁴

The AML/ATF initiative is "horizontal," meaning that Finance Canada works with other agencies, many of which are funded by the Initiative for their work on money laundering and TF matters. The funding arrangements do not earmark funds specifically for money laundering or for TF.¹⁵ As a result, agencies can

⁴ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6752.

⁵ S.C. 2001, c. 41.

⁶ Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6750-6751.

⁷ *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, ss. 2, 42(1) [PCMLTFA]; *Office of the Superintendent of Financial Institutions Act*, R.S.C. 1985, c. 18 (3rd Supp.), Part I, ss. 3, 4(1) [OSFI Act].

⁸ Testimony of Diane Lafleur, vol. 54, p. 6752. For examples in the US and the UK, see Michael Jacobson, "Extremism's Deep Pockets: The growing challenge of fighting terrorist financing," online: The Politic <<http://thepolitic.org/content/view/91>> (accessed June 3, 2009).

⁹ *A New Review Mechanism for the RCMP's National Security Activities*, p. 210.

¹⁰ S.C. 2000, c. 17.

¹¹ *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184 [PCMLTFR].

¹² Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6752.

¹³ Exhibit P-227, Tab 3: Department of Finance Memorandum of Evidence on Terrorist Financing, February 28, 2007, para. 4.25 [Department of Finance Memorandum of Evidence on Terrorist Financing].

¹⁴ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6753.

¹⁵ Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6754-6755.

direct funds to either activity. With no specific allocation of funds for TF, there is a danger that agencies will use the funds primarily for anti-money laundering efforts, leaving anti-TF efforts under funded. The following chart¹⁶ shows the agencies funded by the Initiative:

**Anti- Money Laundering/Anti-Terrorist
Financing (AML/ATF) Initiative**

Funded Partners	Annual Funding (thousands)			
	2006-07	2007-08	2008-09	2009-10
Department of Finance	\$1,800	\$1,800	\$1,800	\$1,800
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	\$37,500	\$38,600	\$37,400	\$37,500
Royal Canadian Mounted Police (RCMP)	\$15,600	\$12,000	\$12,000	\$12,000
Canada Border Services Agency (CBSA)	\$7,800	\$7,700	\$7,700	\$7,700
Canada Revenue Agency (CRA)	\$2,200	\$2,200	\$2,200	\$2,200
Department of Justice & Public Prosecution Services of Canada	\$2,300	\$2,300	\$2,300	\$2,300

Other agencies participate in the Initiative but are not funded by it. These include DFAIT, Public Safety Canada, CSIS and OSFI.¹⁷ FINTRAC, DFAIT and Public Safety receive funding through a separate program – the Public Security and Anti-Terrorism (PSAT) initiative. CSIS also receives funding to deal with its expanded anti-TF activities.¹⁸

The activities of the Financial Action Task Force (FATF) and Finance Canada are intertwined. Member countries follow the FATF recommendations on money laundering and TF. For its part, Finance Canada assesses financial sectors to determine if there is a sufficient vulnerability to money laundering or TF to warrant applying anti-TF laws to them.

Finance Canada has no intelligence-gathering role, but it uses information from law enforcement and intelligence agencies for these assessments.¹⁹ It conducts regular media scans about TF activities around the world and obtains

¹⁶ Exhibit P-227, Tab 2: Department of Finance Presentation, slide 2 [Department of Finance Presentation].

¹⁷ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6755.

¹⁸ Exhibit P-439: Department of Finance Response to Supplementary Questions of the Commission, Question 1(c) [Department of Finance Response to Supplementary Questions of the Commission].

¹⁹ Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6788-6789.

information on TF through its connection with the FATF.²⁰ The Department has no investigative powers.²¹

In developing policy, Finance Canada conducts outreach to private sector reporting entities and refers to them as “partners.” Diane Lafleur, Director of the Financial Sector Division at Finance Canada, testified that these entities, as front line players, had a key role in the anti-TF program.²² She stated that the program could not be effective without their commitment and that Finance Canada works closely with them to develop policies that make sense in given business environments. This was to ensure that “... we are not creating wonderful rules that actually can’t be administered and therefore have no results and can’t be effective.”²³ Ms. Lafleur also saw FINTRAC as a key partner of Finance in policy development.²⁴

Finance Canada was responsible in 2004 for the coordination and response to reviews of the AML/ATF Initiative by EKOS, a social research body, and by the Auditor General. Following those reviews, Finance published a consultation paper on the future of the Initiative and on proposed legislative changes. It also consulted private sector reporting entities. With the help of other agencies, Finance headed the government’s participation in the five-year parliamentary review of the Initiative and guided the policy development process leading to the enactment of Bill C-25²⁵ in 2006.

The Department led the government’s efforts to have the FATF revise its initial 2008 criticisms of Canada’s anti-TF efforts as well as Canada’s response to the final conclusions and recommendations of the 2008 FATF Mutual Evaluation of Canada.

In short, Finance Canada has the lead in developing policy regarding Canada’s anti-TF program. As the lead in anti-TF and anti-money laundering policy development, Finance Canada is responsible for two interdepartmental committees that have mandates in those matters, and a Finance representative chairs both committees.²⁶ Finance Canada is also responsible for work on a “performance management framework” for the Initiative.

Finance Canada also has numerous international responsibilities. It is the lead department for the Canadian delegation to the FATF, the Caribbean Financial Action Task Force and the Asia/Pacific Group on Money Laundering. It is also responsible for the anti-TF issues of concern to other international bodies, including the G-7, G-8, G-20, the International Monetary Fund, the World Bank,

²⁰ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6788.

²¹ Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6751, 6785.

²² Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6752-6753.

²³ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6756.

²⁴ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6786.

²⁵ *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act*, S.C. 2006, c. 12 [Bill C-25].

²⁶ The committees are the Financial Crimes Interdepartmental Coordinating Committee (ICC) and the Financial Crimes Interdepartmental Steering Committee (ADM Steering Committee).

the United Nations, the Organization of American States, the Inter-American Drug Abuse Control Commission, the Commonwealth Secretariat, all FATF-style regional bodies and organizations, and other international AML/ATF organizations.²⁷

3.2 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

3.2.1 Role, Goals, Structure and Overview

The Financial Transactions and Reports Analysis Centre (FINTRAC) is Canada's Financial Intelligence Unit (FIU).²⁸ FIUs have three main functions:

- to serve as a centralized repository for financial information;
- to analyze the information; and
- to facilitate the dissemination of the results.²⁹

FIUs can also monitor compliance by AML/ATF programs with FATF requirements, block transactions and freeze bank accounts, and train those in the financial sector, research and public education.³⁰

FINTRAC is an intelligence agency that receives financial information from private sector entities and government agencies and then produces financial intelligence.³¹ FINTRAC is the product of Canada's attempt to comply with Recommendation 26 of the FATF's "40 Recommendations" on Money Laundering:

Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of [Suspicious Transaction Reports] and other information regarding potential money laundering or terrorist financing.³²

FINTRAC is one of many federal agencies that Parliament has established to fight TF. FINTRAC's evidence of success is that it has produced valuable information

²⁷ Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.27.

²⁸ Much of Canada's legislation dealing with terrorist financing was examined earlier in this volume, but an important part of this legislation, specifically the *PCMLTFA*, is reserved for FINTRAC's work. The finer points of the *PCMLTFA* are therefore discussed in this section.

²⁹ Jae-myong Koh, *Suppressing Terrorist Financing and Money Laundering* (Berlin: Springer, 2006), p. 54 [Koh, *Suppressing Terrorist Financing and Money Laundering*].

³⁰ Koh, *Suppressing Terrorist Financing and Money Laundering*, p. 54.

³¹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6950.

³² FATF's "40 Recommendations" can be found online: Financial Action Task Force <http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html> (accessed September 14, 2009).

and identified links between individuals, organizations and transactions that help law enforcement and security intelligence agencies further their investigations.³³ FINTRAC believes that its activities help to create a hostile environment and a deterrent for those who want to use legitimate financial channels to launder money or finance terrorism³⁴ and that, without FINTRAC, the RCMP and CSIS would face greater difficulties in obtaining information and financial intelligence.³⁵

In 1997, a FATF evaluation criticized Canada's anti-money laundering program, in part due to the absence of an FIU. In response to the evaluation and to the FATF's "40 Recommendations," Canada established FINTRAC in July 2000 through the *Proceeds of Crime (Money Laundering) Act*. FINTRAC's initial operations were targeted solely at money laundering. In 2001, the ATA added TF to FINTRAC's mandate. The Act regulating FINTRAC was accordingly renamed the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

FINTRAC began operating in October 2001.³⁶ It is a young agency.³⁷ FINTRAC's TF work is even more recent. In addition, the implementation of its roles and responsibilities, both legal and operational, has occurred in stages.

FINTRAC's mission is to assist in combatting financial crime, whether generated by money laundering or TF. It is often involved in reviews of Canada's anti-TF program, including the 2008 FATF Mutual Evaluation of Canada. FINTRAC receives significantly more than half of the federal funds dedicated each year to the AML/ATF Initiative.

In general terms, FINTRAC's role is as follows:

...as Canada's financial intelligence unit (FIU)...to safeguard Canada's financial system by contributing to the creation of a more hostile environment for money laundering and terrorist activity financing in Canada; by supporting the public safety and national security of Canadians; and by upholding personal privacy.³⁸

³³ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.

³⁴ Financial Transactions and Reports Analysis Centre of Canada, *Report on Plans and Priorities For the years 2007-2008 to 2009-2010*, p. 7, online: Treasury Board of Canada Secretariat <<http://www.tbs-sct.gc.ca/rpp/0708/fintrac-canafe/fintrac-canafe-eng.pdf>> (accessed June 3, 2009) [FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10]; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6952.

³⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6979.

³⁶ UN CTC Report Submitted by Canada pursuant to Security Council resolution 1373 (2001), S/2004/132, p. 3, online: United Nations Security Council Counter-Terrorism Committee <<http://daccessdds.un.org/doc/UNDOC/GEN/N06/297/90/PDF/N0629790.pdf?OpenElement>> (accessed September 17, 2009).

³⁷ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6967.

³⁸ Financial Transactions and Reports Analysis Centre of Canada, *Departmental Performance Report For the Period ending March 31, 2007*, p. 6, online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/DPR/2007/DPR-eng.pdf>> (accessed September 14, 2009) [FINTRAC 2006-07 Departmental Performance Report].

The *PCMLTFA* sets out the objects of FINTRAC, calling it an independent agency that does the following:

- (a) acts at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information;
- (b) collects, analyses, assesses and discloses information in order to assist in the detection, prevention and deterrence of money laundering and of the financing of terrorist activities;
- (c) ensures that personal information under its control is protected from unauthorized disclosure;
- (d) operates to enhance public awareness and understanding of matters related to money laundering; and
- (e) ensures compliance with Part 1 of the *PCMLTFA* [which sets out the obligations of the reporting entities].³⁹

The FINTRAC 2008 Annual Report describes the activities of the agency as follows:

- Receiving financial transaction reports in accordance with the legislation and regulations and safeguarding personal information under our control.
- Ensuring compliance of reporting entities with the legislation and regulations.
- Producing financial intelligence on suspected money laundering, terrorist activity financing and other threats to the security of Canada.
- Researching and analyzing data from a variety of information sources that shed light on trends and patterns in financial crime.
- Enhancing public awareness and understanding of money laundering and terrorist activity financing.⁴⁰

The Department of Finance Memorandum of Evidence on Terrorist Financing offers a slightly fuller description of FINTRAC's responsibilities. They are to:

- receive and analyze financial transaction reports submitted by reporting entities in accordance with the *PCMLTFA* and its regulations, reports on the cross-border movement of currency

³⁹ *PCMLTFA*, s. 40.

⁴⁰ Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2008 Annual Report*, page following cover page, online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/ar/2008/ar-eng.pdf>> (accessed February 24, 2009) [FINTRAC 2008 Annual Report].

or monetary instruments, and information from international and domestic partners and from the general public;

- provide domestic police forces and foreign financial intelligence units (FIUs) (with which it has concluded an agreement to exchange information) with financial intelligence that it suspects would be relevant to the investigation or prosecution of money laundering and terrorist activity financing offences;
- provide the Canadian Security Intelligence Service (CSIS) with financial intelligence that it suspects would be relevant to threats to the security of Canada, including information on suspected terrorist activity financing;
- provide information to the CRA on suspected cases of terrorist financing involving charities, pursuant to an amendment made to the *PCMLTFA*,⁴¹ and
- help fulfill Canada's international commitments to participate in the fight against transnational crime, particularly money laundering and terrorist financing.⁴²

FINTRAC identified its three key priorities in its *Report on Plans and Priorities for the years 2007-2008 to 2009-2010*:

- deliver timely and high quality financial intelligence to law enforcement, security and intelligence agencies, and foreign financial intelligence units;
- ensure compliance with the *PCMLTFA*; and
- disseminate strategic information on money laundering and terrorist activity financing to partners, stakeholders, and the general public.⁴³

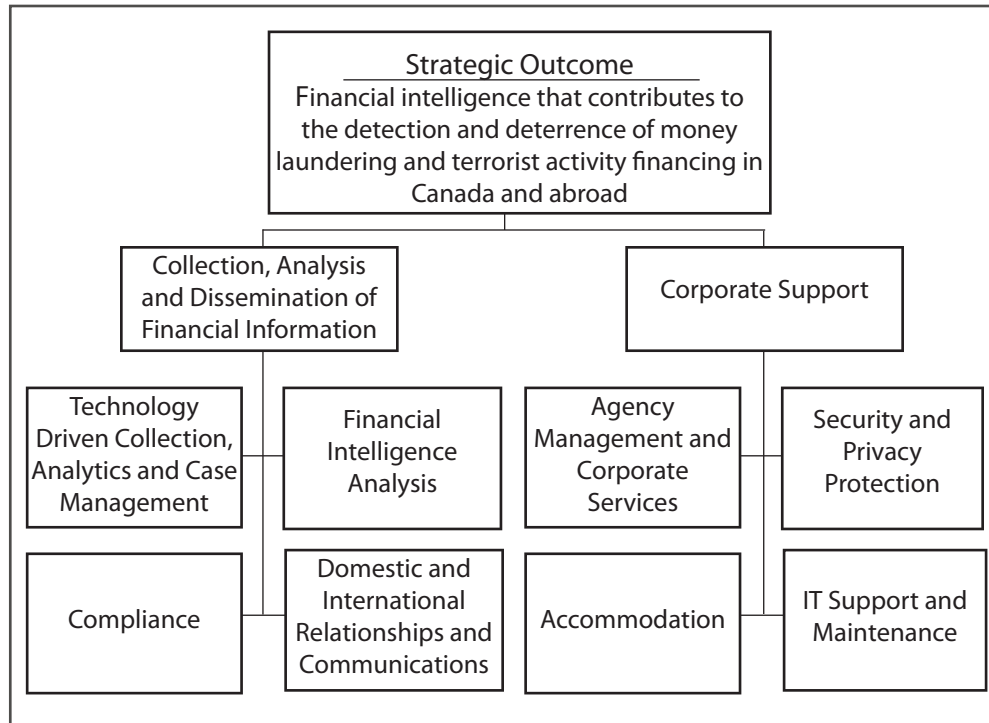
FINTRAC's work products are (i) disclosures of information (based on its analysis of the information it holds or receives about financial transactions) to agencies such as the RCMP, CSIS, CRA, CSE and CBSA and (ii) the production of macro-analyses and research documents on money laundering and TF. FINTRAC's "program activity architecture" is illustrated below:⁴⁴

⁴¹ This was an amendment introduced by Bill C-25.

⁴² Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.29.

⁴³ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 6.

⁴⁴ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 26.



The Minister of Finance is responsible for FINTRAC and reports to Parliament on its activities.⁴⁵ It might have made sense to put FINTRAC, the central agency under the *PCMLTFA*, under the umbrella of Public Safety Canada since other agencies under that umbrella have significant responsibilities in terrorism matters. However, Finance Canada, with its regulatory responsibility for many parts of the financial sector, is better suited for dealing with reporting entities from the financial world.

FINTRAC operates as an agent of the Crown⁴⁶ and acts "...at arm's length from law enforcement agencies and other entities to which it is authorized to disclose information."⁴⁷ At least part of the rationale for having Finance take on oversight was to avoid real or perceived conflicts of interest that might arise if FINTRAC were housed in a department or agency that might benefit from FINTRAC disclosures. Under Finance's umbrella, FINTRAC stands at arm's length from law enforcement.⁴⁸

Besides reporting to Parliament through the Minister of Finance, FINTRAC maintains a close working relationship with the Department of Finance itself.⁴⁹

⁴⁵ *PCMLTFA*, ss. 2, 42(1).

⁴⁶ *PCMLTFA*, s. 41(2).

⁴⁷ *PCMLTFA*, s. 40(a).

⁴⁸ Testimony of Diane Lafleur, vol. 54, September 28, 2007, pp. 6760-6761.

⁴⁹ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6786.

However, Finance officials are not involved in FINTRAC operations, and have no access to data provided to FINTRAC by reporting entities.⁵⁰

FINTRAC also maintains relationships with several branches of the federal and provincial governments,⁵¹ as well as with international organizations and foreign agencies.⁵²

FINTRAC is an “administrative” FIU – the most common FIU model internationally.⁵³ Among other things, this means that it is separate from law enforcement and intelligence agencies and from other bodies that receive information from it. It also means that FINTRAC is a stand-alone administrative and regulatory agency responsible for ensuring that reporting entities comply with the *PCMLTFA* and for analyzing the information received from them. Other, less common FIU models are the “law enforcement” model, where the FIU is part of a larger law enforcement apparatus, and the “prosecutorial” model, where the FIU falls under the jurisdiction of a public prosecutor’s office.

Each model has merits. Some argue that the administrative model is more trusted by private sector reporting entities, since the FIU acts as a buffer between the entities and law enforcement agencies, and it permits more efficient information exchanges with foreign FIUs. However, an administrative model FIU does not have the same range of powers as the other two models, and may not be able to get information into the hands of law enforcement agencies as efficiently as an FIU where the law enforcement function is an integral part of the FIU itself.⁵⁴

Mark Potter, Assistant Director for Government Relationships at FINTRAC, testified about the importance of FINTRAC’s international connections in anti-TF matters:

I think we all recognize we’re part of a global network and that money launderers, terrorist financiers, will seek the weakest link. So to the extent we can cooperate, both at a policy and standard-setting level, through groups like the FATF and at an operational level, through groups like [the Egmont Group of

⁵⁰ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6787; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7003.

⁵¹ These include national and provincial financial regulators, the RCMP and provincial and municipal police forces, CBSA, CRA, Department of Finance, Department of Justice, PSEPC, DFAIT, PCO and Treasury Board: Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2006 Annual Report*, p. 7, online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/ar/2006/ar-eng.pdf>> (accessed June 3, 2009) [FINTRAC 2006 Annual Report].

⁵² Including foreign financial intelligence units (FIUs), The Egmont Group of FIUs, FATF, the World Bank, the International Monetary Fund and the United Nations Global Programme against Money Laundering (UNGPM): FINTRAC 2006 Annual Report, p. 7.

⁵³ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7006-7007.

⁵⁴ For the pros and cons of the various models, see International Money Fund and World Bank, *Financial Intelligence Units: An Overview*, pp. 9-17, online: International Monetary Fund <<http://www.imf.org/external/pubs/ft/FIU/fiu.pdf>> (accessed August 8, 2008) [IMF and World Bank Overview of FIUs]. See also Koh, *Suppressing Terrorist Financing and Money Laundering*, pp. 54-55.

Financial Intelligence Units], in being able to share information efficiently, in sharing best practices with respect to training, with respect to information technology, helps us all reach a similar level of capacity to be able to – to combat global money laundering and terrorist financing.⁵⁵

Since June 2002, FINTRAC has been a member of the Egmont Group of Financial Intelligence Units (the Egmont Group), an international organization founded in 1995 to foster communication and improve the exchange of information, intelligence and expertise, with a worldwide membership of more than 100 FIUs. The Egmont Group's purpose is to "...enhance cooperation and information exchange in support of member countries' anti-money laundering and terrorist financing regimes."⁵⁶ FINTRAC saw joining the Egmont Group as a milestone since it "...allows us to strengthen relationships with FIUs from around the globe and will facilitate the establishment of bi-lateral information exchange agreements that will assist domestic and global efforts to detect, deter and prevent money laundering and terrorist financing."⁵⁷

FINTRAC collaborates with foreign FIUs individually in addition to relying on formal cooperation channels. For example, in 2006-07, FINTRAC worked with its Australian counterpart, AUSTRAC,⁵⁸ on technology upgrades and to improve data capture and data analysis capabilities.⁵⁹

3.2.2 Reporting Entities and Their Obligations

The *PCMLTFA* imposes reporting obligations on entities from many sectors of the financial world.⁶⁰ Reporting entities are required to provide FINTRAC with information on certain financial transactions involving them. These entities include federally-regulated banks, provincially-regulated *caisses populaires* and credit unions, Money Services Businesses (MSBs) and securities dealers.

⁵⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7006.

⁵⁶ Financial Transactions and Reports Analysis Centre of Canada, "FINTRAC is a member of the Egmont Group," online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/inter/egmont-eng.asp>> (accessed December 7, 2007).

⁵⁷ FINTRAC's then Director was the chair of the Transition Sub-committee of Egmont in 2005-06 to "lead the group towards becoming a more sustainable and permanent institution": FINTRAC 2006 Annual Report, p. 5.

⁵⁸ Prof. Martin Rudner has stated that "the Australian Financial Intelligence Unit is regarded as the gold standard, much more robust and much more capable in the prosecution, in both senses of the word, of people engaged in terrorism finance": Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12232.

⁵⁹ Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC 2007 Annual Report*, pp. 2, 25, online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/ar/2007/ar-eng.pdf>> (accessed June 3, 2009) [FINTRAC 2007 Annual Report]; FINTRAC 2006-07 Departmental Performance Report, p. 14.

⁶⁰ Although reporting entities are mostly from the private sector, s. 5(l) of the *PCMLTFA* also requires "departments and agents of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities, that sell money orders to the public or that sell prescribed precious metals, while carrying out the activities described in regulations made under paragraph 73(1)(c)" to report.

Reporting entities are not a part of FINTRAC but critically aid its work. They provide most of the information received by FINTRAC⁶¹ and have become the “eyes and ears” of the Centre.

Section 5 of the *PCMLTFA* identifies the entities required to report:

- (a) authorized foreign banks within the meaning of section 2 of the *Bank Act* in respect of their business in Canada, or banks to which that Act applies;
- (b) cooperative credit societies, savings and credit unions and caisses populaires regulated by a provincial Act and associations regulated by the *Cooperative Credit Associations Act*;
- (c) life companies or foreign life companies to which the *Insurance Companies Act* applies or life insurance companies regulated by a provincial Act;
- (d) companies to which the *Trust and Loan Companies Act* applies;
- (e) trust companies regulated by a provincial Act;
- (f) loan companies regulated by a provincial Act;
- (g) persons and entities authorized under provincial legislation to engage in the business of dealing in securities, or to provide portfolio management or investment counselling services;
- (h) persons and entities engaged in the business of foreign exchange dealing;
- (i) persons and entities engaged in a business, profession or activity described in regulations...;
- (j) persons and entities engaged in a business or profession described in regulations...while carrying out the activities described in the regulations;
- (k) casinos, as defined in the regulations, including those owned or controlled by Her Majesty;
- (l) departments and agents of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities or that sell money orders to the public, while carrying out the activities described in regulations...; and

⁶¹ *PCMLTFA*, s. 54.

(m) for the purposes of section 7 [which sets out the obligation to report certain transactions], employees of a person or entity referred to in any of paragraphs (a) to (l).

Sections 5(i) and 5(j) make it possible to add new reporting entities by way of regulation. The following organizations have been added: legal counsel and legal firms,⁶² British Columbia notaries public and notary corporations, accountants and accounting firms, dealers in precious metals and stones, and real estate developers.

FINTRAC monitors reporting sectors to identify appropriate additions to the list of reporting entities. For example, in its 2007 Annual Report, FINTRAC stated that it had noticed a stronger presence of Internet payment systems and “white label” ATMs in its disclosures of financial intelligence to other agencies.⁶³ The ability to add new financial sectors is particularly important if those who finance terrorism shift their fundraising activities to sectors that may still not be subject to reporting requirements.

3.2.3 Collection or Receipt of Information

FINTRAC receives information from three main sources: (i) private sector reporting entities, (ii) foreign FIUs and (iii) federal government agencies such as the RCMP, CSIS and the CBSA.⁶⁴ It must retain any reports received or information collected for a minimum of 10 years.⁶⁵ Identifying information contained in a report must be destroyed after 15 years if, during that time, the report has not been disclosed to certain bodies (for example, CSIS or the RCMP) identified in the *PCMLTFA*.⁶⁶

3.2.3.1 The Arm’s-Length Arrangement

FINTRAC does not have the legal authority to compel other agencies to provide information to it.⁶⁷ Nor can other agencies compel FINTRAC to provide information to them, except by obtaining a production order, discussed below. This is because FINTRAC stands at arm’s length from other agencies.

⁶² However, the obligation to report contained in ss. 7 and 9 of the *PCMLTFA* does not apply to legal counsel or legal firms when they are providing legal services: *PCMLTFA*, s. 10.1. Furthermore, s. 11 of the *PCMLTFA* states that nothing in Part 1 of the Act (which deals with record keeping, verifying identity, reporting of suspicious transactions and registration) requires a legal counsel to disclose any communication that is subject to solicitor-client privilege.

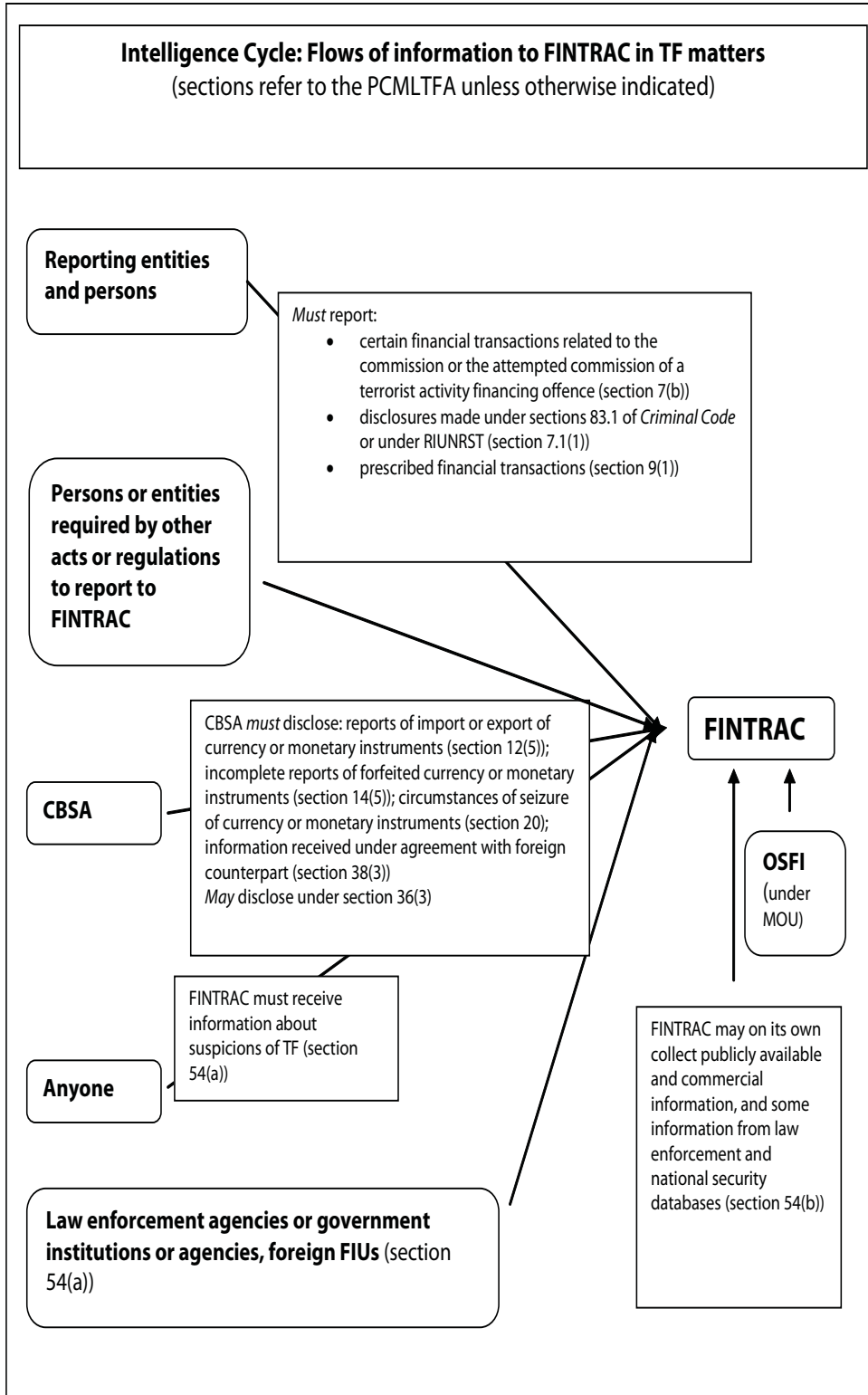
⁶³ FINTRAC 2007 Annual Report, p. 24. “White label” ATMs dispense cash, but are not affiliated with a bank.

⁶⁴ Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.31.

⁶⁵ *PCMLTFA*, s. 54(d). The retention requirement is subject to s. 6 of the *Privacy Act*, R.S.C. 1985, c. P-21, which sets out requirements for the retention and disposal of personal information collected by federal government institutions.

⁶⁶ *PCMLTFA*, s. 54(e).

⁶⁷ Exhibit P-382: Dossier 4: Terrorist Financing, December 13, 2007, p. 40 [Terrorist Financing Dossier].



3.2.3.2 Information Received from Reporting Entities

Under the *PCMLTFA*, reporting entities must do more than simply report certain transactions to FINTRAC. They have specific obligations about record-keeping, verifying clients' identities, complying with other legislation besides the *PCMLTFA*, and reporting suspicious and other transactions.⁶⁸

Reporting entities must provide information to FINTRAC about the following:

- suspicious transactions (through Suspicious Transaction Reports (STRs)) related to the possible commission of a money laundering or terrorist activity financing offence;⁶⁹
- the possession or control of property by listed entities (Terrorist Property Reports (TPRs));⁷⁰
- cash transactions of \$10,000 or more,⁷¹ or two or more cash transactions within 24 hours that amount to \$10,000 or more (Large Cash Transaction Reports),⁷² other than withdrawals;⁷³ and
- electronic funds transfers of \$10,000 or more, or two or more transactions within 24 hours that amount to \$10,000 or more, where the sender or the recipient is located outside Canada (Electronic Funds Transfer Reports (EFTRs)).⁷⁴

All the reports described above are submitted to FINTRAC on standardized forms. Reports are typically made using FINTRAC's electronic online system, known as F2R.⁷⁵

Reporting entities have no specific legal authorization to report any transactions that could be considered a threat to the security of Canada.⁷⁶ Still, reporting entities, unsurprisingly, are not prohibited from reporting these types of transactions.

⁶⁸ *PCMLTFA*, ss. 6-11.1.

⁶⁹ *PCMLTFA*, s. 7.

⁷⁰ Section 7.1 was added to the *PCMLTFA* in 2001 as part of the *Anti-terrorism Act*, S.C. 2001, c. 41 [*Anti-terrorism Act*] and requires a person or entity who is required to make a disclosure under s. 83.1 of the *Criminal Code*, R.S.C. 1985, c. C-46 [*Criminal Code*] to file a report with FINTRAC if that person or entity is subject to the *PCMLTFA*. Bill C-25 amended the provision by adding the obligation for a person or entity who is required to report under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, S.O.R./2001-360 [RIUNRST] and who is subject to the *PCMLTFA*.

⁷¹ *PCMLTFR*, s. 12(1)(a).

⁷² *PCMLTFR*, s. 3(1).

⁷³ *PCMLTFR*, s. 12(1)(a).

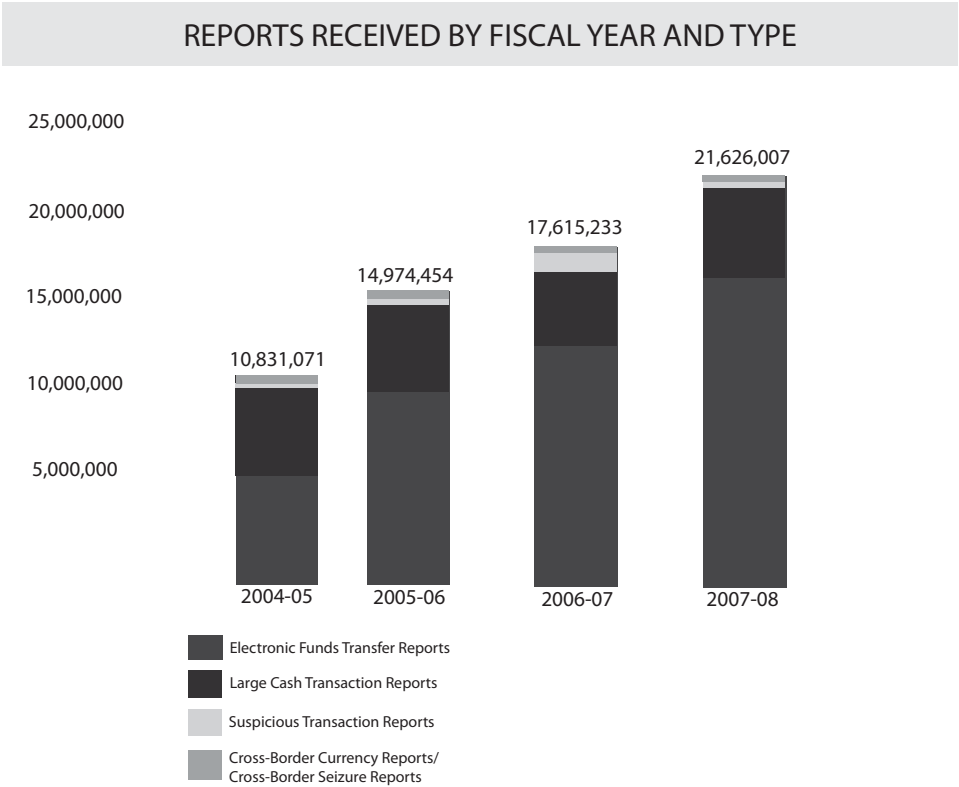
⁷⁴ *PCMLTFR*, ss. 12(1)(b), 12(1)(c), 3(1).

⁷⁵ FINTRAC presented a demonstration of the F2R system to Commission Counsel during the course of the Inquiry.

⁷⁶ A document prepared by FINTRAC also mentions this: see Exhibit P-233, Tab 11: Reasonable Grounds to Suspect, p. 1 [FINTRAC Response on Reasonable Grounds to Suspect].

Amendments to section 7 of the *PCMLTFA* came into force in June 2008. They require a reporting entity to report to FINTRAC when it has reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence.⁷⁷ Before, there was no obligation to report attempted transactions.

In fiscal year 2007-08, FINTRAC received slightly more than 21.6 million reports, a substantial increase over the previous year, and about twice as many reports as it received in 2004-05. However, only a very small percentage of reports to FINTRAC in recent years have been Suspicious Transaction Reports. The vast majority have been Electronic Funds Transfer Reports, followed by Large Cash Transaction Reports. The following chart⁷⁸ illustrates the breakdown of the reports received by FINTRAC, by fiscal year and type:



Although FINTRAC has over the years received relatively few STRs as a proportion of the total reports, STRs are particularly important because reporting entities have applied their financial experience to flag these transactions as problematic. Mark Potter testified that the STR is "...often one of the richest and most useful types of reports for getting at particularly the terrorist financing side of things."⁷⁹

⁷⁷ The amendments were introduced by Bill C-25, s. 5.

⁷⁸ FINTRAC 2008 Annual Report, p. 17.

⁷⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7029.

Unlike STRs, other reports are triggered mechanically, without analysis by the reporting entity, when an objective threshold is met – cash transactions of \$10,000 or more, for example.

“Objective threshold” reports also supply useful information.⁸⁰ For example, FINTRAC documents state that 93 per cent of its disclosures of information to other agencies about TF or threats to the security of Canada contained at least one EFTR, based on objective thresholds.⁸¹ Even so, FINTRAC’s own statistics show that Voluntary Information Records⁸² (VIRs) provided by government agencies, along with STRs, are the most common sources of information leading to investigations.⁸³

Section 7 of the *PCMLTFA* requires “...every person or entity [to] report to [FINTRAC] ... every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to...” the commission, or the attempted commission, of a money laundering offence or a terrorist activity financing offence. There is no definition in the *PCMLTFA* of “suspicious transaction,” but FINTRAC has issued a guideline.⁸⁴ According to FINTRAC, the omission of a definition from the Act was deliberate, thereby leaving it up to the reporting entities, which were in the best position to make the determination.⁸⁵ There is no monetary limit below which STRs are not required.⁸⁶ The guideline indicates that “reasonable grounds to suspect” is “...determined by what is reasonable in your circumstances, including normal business practices and systems within your industry.”⁸⁷ Furthermore, the guideline offers broad parameters for determining when a transaction might qualify as suspicious:

As a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

⁸⁰ Exhibit P-438: FINTRAC Response to Supplementary Questions of the Commission, January 9, 2008, Question 3(a) [First FINTRAC Response to Supplementary Questions of the Commission].

⁸¹ First FINTRAC Response to Supplementary Questions of the Commission, Question 3(b). This is consistent with the international nature of terrorism. See also Financial Action Task Force, *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism, Canada*, February 29, 2008, para. 101, online: Financial Action Task Force <<http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf>> (accessed April 1, 2009) [2008 FATF Mutual Evaluation of Canada].

⁸² As discussed below, the RCMP and other government agencies can voluntarily provide information to FINTRAC through Voluntary Information Records.

⁸³ Exhibit P-233, Tab 14: FINTRAC Originators Chart [FINTRAC Originators Chart].

⁸⁴ Financial Transactions and Reports Analysis Centre of Canada, “Guideline 2: Suspicious Transactions” (December 2008), online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp>> (accessed July 10, 2007) [FINTRAC Guideline on Suspicious Transactions].

⁸⁵ FINTRAC Response on Reasonable Grounds to Suspect, p. 1.

⁸⁶ FINTRAC Guideline on Suspicious Transactions, para. 6.1.

⁸⁷ FINTRAC Guideline on Suspicious Transactions, para. 3.1.

The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. You should evaluate transactions in terms of what seems appropriate and is within normal practices in your particular line of business, and based on your knowledge of your client. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.⁸⁸

The guideline also identifies indicators of suspicious transactions relating to TF,⁸⁹ stating that these indicators resemble and complement indicators of suspicious transactions in money laundering cases. The guideline states that it can be difficult to distinguish between a suspicion of money laundering activity and a suspicion of TF activity.⁹⁰ For FINTRAC, the important point is whether the entity has suspicions, not whether the suspicions relate to money laundering or TF.⁹¹ FINTRAC stated that most STRs that form the basis of disclosures to other agencies about possible TF were originally brought to FINTRAC's attention for their suspected relation to money laundering.⁹²

The guideline notes that TF often involves smaller amounts than money laundering cases.⁹³ Entities are urged to provide as many details as possible, "... including anything that made you suspect that it might be related to terrorist financing, money laundering, or both."⁹⁴

The guideline identifies more than 100 indicators that, alone or together, might point to suspicious activity.⁹⁵ Many are general, while others relate to specific activities or industries. Specific indicators are provided for financial sector entities, securities dealers, real estate brokers, non-profit organizations (NPOs) and Money Service Businesses (MSBs), among others. Below are several examples of indicators contained in the guideline:

⁸⁸ FINTRAC Guideline on Suspicious Transactions, para. 6.1.

⁸⁹ FINTRAC Guideline on Suspicious Transactions, paras. 7, 8.

⁹⁰ FINTRAC Guideline on Suspicious Transactions, para. 6.2.

⁹¹ FINTRAC Guideline on Suspicious Transactions, para. 6.2.

⁹² Exhibit P-440: FINTRAC Response to Supplementary Questions of the Commission, February 5, 2008, Question 2(m)(i) [Second FINTRAC Response to Supplementary Questions of the Commission].

⁹³ Janet DiFrancesco also testified that TF transactions are more difficult to identify than money laundering transactions because they involve "much smaller amounts of money": Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6956.

⁹⁴ FINTRAC Guideline on Suspicious Transactions, para. 6.2.

⁹⁵ The guideline clearly states that: "These indicators were compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations. They are not intended to cover every possible situation and are not to be viewed in isolation.": FINTRAC Guideline on Suspicious Transactions, para. 6.3.

- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client is quick to volunteer that funds are “clean” or “not being laundered.”
- Client appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.
- Client refuses to produce personal identification documents.
- All identification documents presented appear new or have recent issue dates.
- Client presents uncounted funds for a transaction. Upon counting, the client reduces the transaction to an amount just below that which could trigger reporting requirements.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Cash is transported by a cash courier.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Unusually large cash deposits by a client with personal or business links to an area associated with drug trafficking.

- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Client and other parties to the transaction have no apparent ties to Canada.
- Transaction crosses many international lines.
- Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- The non-profit organization appears to have little or no staff, no suitable offices or no telephone number, which is incompatible with their stated purpose and financial flows.
- The non-profit organization has operations in, or transactions to or from, high-risk jurisdictions.
- Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to hold funds in its account for a very long period.⁹⁶

FINTRAC has compiled some of the most common reasons for sending STRs to FINTRAC:

- Customer known to authorities;
- Unusual business activity;
- Unable to ascertain source of funds;
- Multiple deposits at different branches;
- Many third party deposits, appears to be operating MSB through the account.⁹⁷

Below is a chart⁹⁸ showing the number of STRs, by sector, that FINTRAC received in TF matters between 2001 and mid-2007.

⁹⁶ FINTRAC Guideline on Suspicious Transactions, paras. 7, 8.

⁹⁷ These and other reasons are found at Exhibit P-233, Tab 22: FINTRAC, "Tactical Financial Intelligence," pp. 18-20 [FINTRAC Presentation on Tactical Financial Intelligence].

⁹⁸ Exhibit P-233, Tab 6: STRs Received by Sector, 2001-07.

**FINTRAC'S RESPONSE TO AN INQUIRY
REQUEST FOR DISCLOSURE OF DOCUMENTS
TRANCHE 1**

Q. Statistics regarding "suspicious transactions" reports linked to TF that FINTRAC has received from all financial institutions:

A. See chart below.

STRs Received by Sector						
	2001-2002	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007*
Accountant	7	20	20	40	20	12
Bank	576	3623	4077	5665	12084	5174
Caisse Populaire	1045	3357	1946	3151	4918	5185
Canada Post	87	127	73	19	35	249
Casino	143	498	360	390	420	223
Co-op Credit Society	20	29		1	6	0
Foreign Exchange Dealer	938	6188	3221	2109	963	429
Legal Counsel	5	2	3	0	0	0
Life Insurance Broker or Agent	1	1	11	2	4	0
Life Insurance Company	10	30	52	29	32	78
Money Services Business	182	647	1871	4048	7092	5148
Provincial Savings Office	5	61	17	202	336	114
Real Estate Broker/Sales Representative	2	8	6	6	12	42
Savings & Credit Unions	639	2415	2767	2905	2837	1336
Securities Dealer	42	169	80	74	83	48
Trust & Loan Company	31	37	64	214	438	388
Unknown	39	146	226	258	87	5

Note: statistics for 2006-07 are for the first two quarters only.

Potter testified that banks provide a preponderance of the financial transaction reports submitted to FINTRAC,⁹⁹ including the most STRs, but that MSBs also contribute a significant number. The relatively large number from MSBs is surprising because of the small size of the MSB sector in Canada and the absence, until Bill C-25 was enacted, of requirements for such entities to register with FINTRAC. The new registration requirements for MSBs should produce more and better reports from that sector.¹⁰⁰

⁹⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6975. In fact, banks were the first institutions to be subjected to the reporting obligations under the FATF's original 40 Recommendations. Although non-bank financial institutions were also included in principle, no list of such institutions was provided: IMF and World Bank Overview of FIUs, p. 35.

¹⁰⁰ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6973-6974.

Several detailed guidance documents are also available to reporting entities to help them report properly.¹⁰¹ These documents are updated as circumstances and legislation change.

The 2008 FATF Mutual Evaluation of Canada explained that federal officials felt that asking for further information would violate section 8 of the *Charter*,¹⁰² although no court has yet made such a finding. Nonetheless, FINTRAC officials indicated that FINTRAC does go back to reporting entities to ask for additional information about an individual or a transaction.¹⁰³

Many private sector reporting entities see the reporting system as complex and as imposing considerable responsibilities on them, especially because of the numerous reporting obligations, including client identification rules (also sometimes referred to as “customer due diligence”). The inherent complexity of the financial world and its myriad types of transactions further complicate matters. Some reporting entities complain in particular about the one-way flow of information that leaves them wondering whether their reporting efforts were at all useful.

3.2.3.3 Other Sources of Information for FINTRAC

The CBSA must send a Cross-Border Currency Report (CBCR) to FINTRAC for any cross-border movement of currency or monetary instruments of \$10,000 or more.¹⁰⁴ CBSA also reports seizures of currency or monetary instruments via a Cross-Border Seizure Report (CBSR).¹⁰⁵ In addition, CBSA may provide information to FINTRAC if it has reasonable grounds to suspect that such information would be of assistance in the detection, prevention or deterrence of money laundering or financing of terrorist activities.¹⁰⁶

The RCMP and other municipal or provincial police forces, CSIS, CSE, ITAC, CBSA, CRA, DFAIT and other agencies can all (if their governing legislation permits) provide information to FINTRAC by way of a form entitled a Voluntary Information Record (VIR). FINTRAC must also receive reports that are made to it by foreign

¹⁰¹ These guidelines are more technical than substantive. They include Guideline 3A: Submitting Suspicious Transaction Reports to FINTRAC Electronically, Guideline 3B: Submitting Suspicious Transaction Reports to FINTRAC by Paper, Guideline 5: Submitting Terrorist Property Reports, Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically, Guideline 7B: Submitting Large Cash Transaction Reports to FINTRAC by Paper, Guideline 8A: Submitting Non-SWIFT Electronic Funds Transfer Reports to FINTRAC Electronically, Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC and Guideline 8C: Submitting Non-SWIFT Electronic Funds Transfer Reports to FINTRAC by Paper: see Financial Transactions and Reports Analysis Centre of Canada, “FINTRAC Guidelines,” online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/guide/guide-eng.asp>> (accessed July 10, 2008).

¹⁰² 2008 FATF Mutual Evaluation of Canada, para. 402.

¹⁰³ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6987-6989.

¹⁰⁴ *A New Review Mechanism for the RCMP's National Security Activities*, p. 186; *PCMLTFA*, ss. 12(1), 12(5); *Cross-border Currency and Monetary Instruments Reporting Regulations*, S.O.R./2002-412, s. 2(1) [*Cross-border Currency and Monetary Instruments Reporting Regulations*].

¹⁰⁵ *PCMLTFA*, ss. 18, 20.

¹⁰⁶ *PCMLTFA*, s. 36(3).

FIUs as well as other information voluntarily provided to it about suspicions of TF.¹⁰⁷ In addition, FINTRAC can collect information stored in databases maintained by the federal and provincial governments for law enforcement or national security purposes, such as the Canadian Police Information Centre (CPIC).¹⁰⁸ FINTRAC also relies on open source information – information available in the public domain, such as corporate registries. FINTRAC expressed concern, however, that it could not obtain access to CSIS databases.¹⁰⁹

Media scans concerning money laundering, TF and possible threats to the security of Canada are reviewed daily by FINTRAC analysts. This open source information is then matched against FINTRAC's database. Such a process was used in the recent case of the "Toronto 18."¹¹⁰

FINTRAC also reviews past and present TF cases around the world to enhance its own research and analysis.¹¹¹

3.2.3.4 The Voluntary Information Record (VIR) Process

VIRs may relate to investigations of money laundering or TF offences.¹¹² Federal officials spoke of their importance. For example, James Galt of CSIS testified that his first reflex on handling a new TF file would be to determine whether FINTRAC had been consulted. He stated that he could not think of a reason why the information in a file should not be sent to FINTRAC.¹¹³ RCMP Superintendent Rick Reynolds testified that, in TF matters, "...we provide...as many voluntary information reports as we feel appropriate and our resources allow."¹¹⁴ Once it receives a VIR, FINTRAC's TF Unit assesses the information to determine if it can produce an analysis for the agency that submitted the VIR.¹¹⁵

As noted, the VIR is usually sent to FINTRAC using a standardized form.¹¹⁶ Potter stated that the form was developed because the information FINTRAC was receiving before then was of "mixed quality."¹¹⁷ The form, developed with FINTRAC's partners, speeds up the analysis process within FINTRAC.¹¹⁸ During testimony, FINTRAC officials showed the Commission a "sanitized" case of actual TF activity. They also explained the content of the VIR in that case.

¹⁰⁷ *PCMLTFA* s. 54(a).

¹⁰⁸ *PCMLTFA* s. 54(b); Terrorist Financing Dossier, p. 39.

¹⁰⁹ Exhibit P-442: Summary of Meeting between Commission Counsel and FINTRAC, April 10, 2008, p. 3 [Summary of Meeting with FINTRAC].

¹¹⁰ Exhibit P-233, Tab 20: FINTRAC Response to Various Questions of the Commission, p. 1. The informal name of the case has changed several times, as charges were dropped against some of the defendants. The term "Toronto 18" is used here.

¹¹¹ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7009-7010.

¹¹² Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.

¹¹³ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6941.

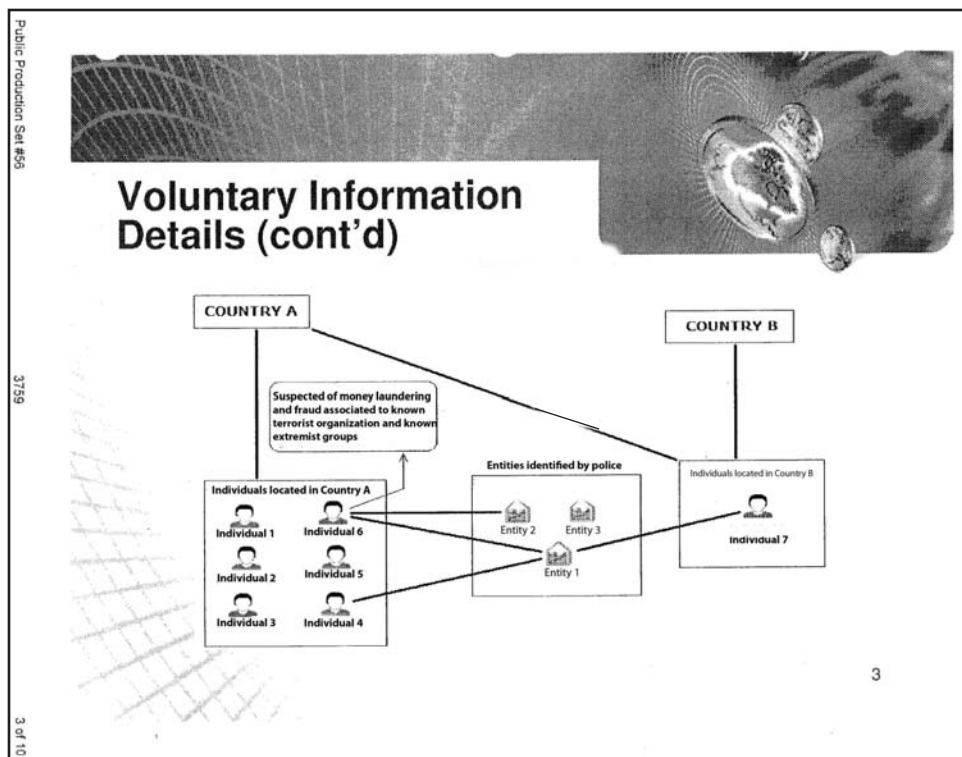
¹¹⁴ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6886.

¹¹⁵ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.

¹¹⁶ English and French versions of a VIR form were entered into evidence: see Exhibit P-233, Tab 9.

¹¹⁷ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6960.

¹¹⁸ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6961.



[Exhibit P-233, Tab 21, p.3 (Public Production 3759)]

The preparation of VIRs in agencies such as the RCMP and CSIS is centralized, with at least one senior staff member tasked with overseeing the information provided in the VIRs.¹¹⁹ There is no coordination between the RCMP and CSIS in preparing VIRs.

FINTRAC documents indicate that if a VIR is received from an agency such as CSIS, and if FINTRAC concludes that it meets the threshold for disclosing the information to law enforcement as suspected TF activity, it would seek permission from CSIS before such disclosure. Similarly, it would seek permission from a law enforcement agency before disclosing information to CSIS.¹²⁰ James Galt of CSIS stated that VIRs prepared by CSIS often contain an authorization to release the information to another agency.¹²¹ CSIS documents indicate that this is done with about half of VIRs. For the remainder, FINTRAC would need to seek permission and CSIS would decide on a case-by-case basis.¹²²

This arrangement whereby FINTRAC must seek permission from CSIS potentially conflicts with FINTRAC's legal obligation under the *PCMLTFA* to

¹¹⁹ Testimony of Jim Galt, vol. 55, October 1, p. 6917;

¹²⁰ Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).

¹²¹ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6920.

¹²² Exhibit P-441: CSIS Response to Supplementary Questions of the Commission, March 5, 2008, Question 2 [CSIS Response to Supplementary Questions of the Commission].

disclose designated information to a relevant agency when the threshold for disclosure is met. For example, section 55(3) of the *PCMLTFA* obliges FINTRAC to disclose information to “the appropriate police force” if FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating a terrorist activity financing offence. Even if CSIS had provided information in confidence, FINTRAC would be obliged to disclose it to the police if the information, combined with other information, gave FINTRAC “reasonable grounds to suspect.” Thus, the conflict arises between FINTRAC’S agreement with CSIS and its obligations under the *PCMLTFA*.

FINTRAC officials have stated that, in most cases where they have not received prior authorization, they do receive it after they approach the agency that submitted the VIR. The two principal situations where the agency refuses permission are when the VIR contains information from a foreign FIU or information about undercover sources.¹²³

FINTRAC gives priority to possible TF cases, regardless of the size of the operation.¹²⁴ Responding to VIRs submitted in TF matters is important to FINTRAC because of the possibility of loss of life from terrorist incidents.¹²⁵

The amounts of money at issue in TF, typically smaller than in money laundering cases, make it more difficult for FINTRAC to generate TF leads on its own. Janet DiFrancesco, Assistant Director for Macro-Analysis and Integration within the Operations Sector at FINTRAC, gave evidence that the smaller number of independent TF investigations generated by FINTRAC was primarily due to the nature of TF cases: “...[T]ypically we’re dealing with much smaller amounts of money moving.”¹²⁶

Unlike money laundering, where the large sums involved may arouse FINTRAC’S suspicion, the small amounts sometimes involved in TF may give FINTRAC no reason to become suspicious. As a result, FINTRAC has difficulty identifying possible TF by relying solely on its internal analysis. Galt testified that FINTRAC had identified cases on its own three times in the last few years.¹²⁷ In most cases, it must rely on others – reporting entities or agencies such as the RCMP or CSIS – who are reporting their own suspicions to FINTRAC. FINTRAC can then add value through its analysis of the information that comes into its possession.

About 90 per cent¹²⁸ of the possible TF cases that come to FINTRAC’S attention do so because FINTRAC has received law enforcement or CSIS VIRs. FINTRAC then responds to these VIRs, which can be viewed as unofficial requests for

¹²³ Summary of Meeting with FINTRAC, p. 1.

¹²⁴ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6962; Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(b).

¹²⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6962.

¹²⁶ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6956.

¹²⁷ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6920.

¹²⁸ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007 at p. 6956. Mark Potter could not give a number for the operations of FIUs in other countries: see Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6965.

information from FINTRAC – requests made by way of VIRs – by searching its own databases, analyzing the combined information and, if the legal criteria for disclosure are met, disclosing designated information to the appropriate agency.

Ms. DiFrancesco testified that FINTRAC identifies additional links, entities, individuals or accounts in regard to a particular investigation or matter. As well, to further advance the investigation, FINTRAC verifies links that law enforcement agencies have already made.¹²⁹ Because FINTRAC has information about electronic funds transfers (EFTs), information that law enforcement agencies usually do not hold, FINTRAC is well-positioned to identify links with foreign countries.¹³⁰ Potter testified that the VIR process also helped to maintain an appropriate relationship with other agencies:

...[P]articularly with law enforcement and CSIS, it allows us to balance two things: on the one hand being able to respond to the investigative priorities of those agencies by receiving VIRs from them on targets and entities of interest to them, and on the other hand to balance the need to maintain an arm's-length relationship and not have direct access to our database by those agencies and ensure that any cases we do ultimately disclose in which a VIR is a factor, reach our threshold of reasonable grounds to suspect. So there is a balance that is achieved through the use of that mechanism and that piece of information.¹³¹

During 2005-06, FINTRAC received 47 VIRs that it classified as relating to national security. This represented nine per cent of the total VIRs received. During the same period, FINTRAC made 33 disclosures to other agencies relating to TF or threats to national security. Recipients made seven follow-up requests and FINTRAC responded by providing additional information for six of the seven. The 33 disclosures were not necessarily the product of the 47 VIRs received during 2005-06 because some disclosures could have been the result of VIRs from previous years.¹³²

The 2008 FATF Mutual Evaluation of Canada spoke of FINTRAC's excessive reliance on VIRs for its TF work, stating that "...[t]his raises serious concern with respect to the capability of FINTRAC to generate new ML/TF cases independent from existing investigations."¹³³ The number of FINTRAC disclosures on TF matters which could lead to new investigations by other agencies should

¹²⁹ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.

¹³⁰ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957. In fact, FINTRAC is one of several FIUs in the world to receive EFTs, which puts it in a good position in Canada's fight against TF and ML: FINTRAC 2007 Annual Report, p. 24.

¹³¹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6959.

¹³² Exhibit P-233, Tab 10: FINTRAC Response on Voluntary Information Record Statistics, p. 1.

¹³³ 2008 FATF Mutual Evaluation of Canada, para. 21.

increase in coming years because the FINTRAC database is becoming more fully populated. Potter gave an example of a possible lead initiated by a FINTRAC review of media reports about terrorist activities. That information would then be combined with information in FINTRAC's database and analyzed.¹³⁴

3.2.4 Analysis of Information Received by FINTRAC

Section 54(c) of the *PCMLTFA* provides that FINTRAC must analyze and assess the reports and information it receives. The analysis process consists of assembling all relevant information from various sources, trying to identify connections between various parties and, finally, trying to identify transactions that could be linked to either TF or money laundering.¹³⁵

FINTRAC's 2008 Annual Report described the two general categories of financial intelligence that FINTRAC produces: "The first is information about specific suspicious transactions, that is, those that suggest movements of illicit money. The second is information showing overall patterns and trends as they emerge in the ever-evolving world of money laundering and terrorist financing."¹³⁶

Each of FINTRAC's four Tactical Financial Intelligence Units, part of its Operations section, plays a role in the analysis process:

- One unit deals with VIRs, performing a general triage function and handling less complicated cases, as needed;
- One unit deals with money laundering;
- One unit deals with TF and queries from foreign FIUs; and
- One unit deals with STRs and open source information which might feed into the money laundering and TF units.¹³⁷

Ms. DiFrancesco testified in 2007 that the TF unit at that time had a staff of approximately ten.¹³⁸ (The 2007 FINTRAC Annual Report stated that FINTRAC had 264 employees in total).¹³⁹ Employees in other units may also work on TF matters. FINTRAC's 2008 Annual Report stated that staffing increased to 329 employees during that year, but did not indicate how many devoted their time wholly or partly to TF matters.¹⁴⁰ The 2008 Annual Report spoke of how the efficiency of its electronic systems avoided the need to hire many more employees:

¹³⁴ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6963-6964.

¹³⁵ FINTRAC Presentation on Tactical Financial Intelligence, p. 8.

¹³⁶ FINTRAC 2008 Annual Report, p. 7.

¹³⁷ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6953-6955.

¹³⁸ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6955-6956.

¹³⁹ FINTRAC 2007 Annual Report, p. 30.

¹⁴⁰ FINTRAC 2008 Annual Report, p. 21.

Annually, [FINTRAC's] powerful systems collect, capture, cleanse, and move 20 million reports into appropriate databases, all within two hours of receipt. Because of this, we have been able to cut down our use of paper files drastically, and we are saving immeasurable amounts of staff time. (Indeed, if we had to key in these reports manually, we would need another thousand employees.) We then scan these huge volumes of reports – using analytical tools designed specifically for FINTRAC's unique requirements – and quickly zero in on patterns of possible suspicious transactions.¹⁴¹

The 2008 Annual Report stressed the utility of these systems:

...FINTRAC benefits from being one of the few FIUs that has developed electronic systems that permit the automated receipt of high volumes of financial reports and the rapid and precise mining of information from the millions of reports of various types in our databases.

...

We receive more than twenty million reports annually. Thirty years ago, the processing of this data would have required an army of sorters, filers and compilers to collect and analyze such volumes, as well as an airplane hangar in which to store the records. Today however, FINTRAC is up to the task at hand thanks to the advanced technological infrastructure – electronic systems that we constantly revamp and upgrade – that lies at the core of our operations.¹⁴²

The Annual Report claimed that FINTRAC's technology and analysis provided considerable benefits for police and other recipients of FINTRAC disclosures:

FINTRAC's sophisticated data mining techniques are able, for example, to look for links among transaction reports received from a multiplicity of different reporting entities. In so doing they can uncover the trail left by money launderers who typically use several banks – sometimes more than a dozen in widely dispersed locations – to try to evade detection.... [H]alf of our case disclosures this past year were based on reports from six or more reporting entities.

...

¹⁴¹ FINTRAC 2008 Annual Report, p. 21.

¹⁴² FINTRAC 2008 Annual Report, p. 7.

[T]he financial intelligence that FINTRAC discloses takes a variety of forms and is derived through many different methods. Often information provided to us by law enforcement and intelligence agencies leads us to comb through our databases to find connections that would otherwise elude investigators. What we are then able to disclose gives the investigators a valuable return on that initial lead.

In other instances, our automated technology will find suspicious patterns of financial transactions, and these enable our analysts to construct a case that is wholly new to police and other disclosure recipients. Common to all cases, however, is the scope and detail of the intelligence that FINTRAC is able to provide.¹⁴³

In analyzing the information it holds, FINTRAC looks at a broad array of indicators of TF. The following are examples:¹⁴⁴

- Sending or receiving funds by international transfers from and/or to locations of specific concern;
- Atypical business/account behaviour;
- Charity/relief organization linked to transactions;
- Media coverage of account holder's activities;
- Ongoing investigation; and
- Large and/or rapid movement of funds;

The 2008 FATF Mutual Evaluation of Canada criticized FINTRAC because of the indicators it used to determine whether a transaction was related to TF. The FATF concluded that the indicators were solely based on FATF typologies (examples of trends and methods) and indicators, as well as those of the Egmont Group and other FIUs, rather than developed by FINTRAC. The FATF concluded that, the list based on TF trends identified by FINTRAC itself spots "relatively basic and unsophisticated indicators."¹⁴⁵

FINTRAC officials presented to the Commission a "sanitized" TF scheme. The scheme is complex, as the diagrams below show. This and other cases of such complexity may require FINTRAC to perform a very sophisticated analysis.¹⁴⁶

¹⁴³ FINTRAC 2008 Annual Report, p. 11.

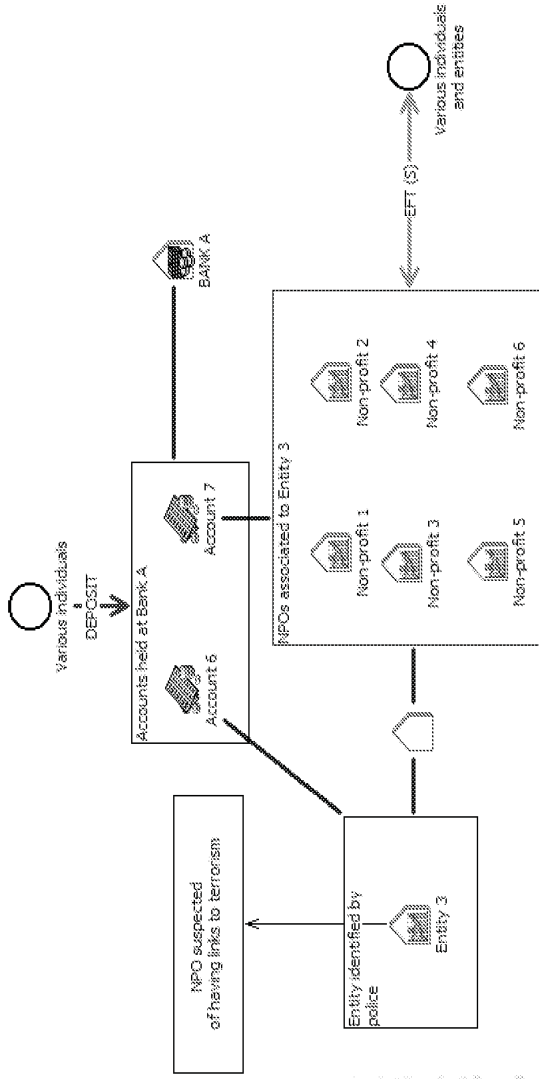
¹⁴⁴ The FINTRAC Presentation on Tactical Financial Intelligence includes a more complete list: see pp. 21-24.

¹⁴⁵ 2008 FATF Mutual Evaluation of Canada, para. 378.

¹⁴⁶ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6989-6995.



Analysis (cont'd)

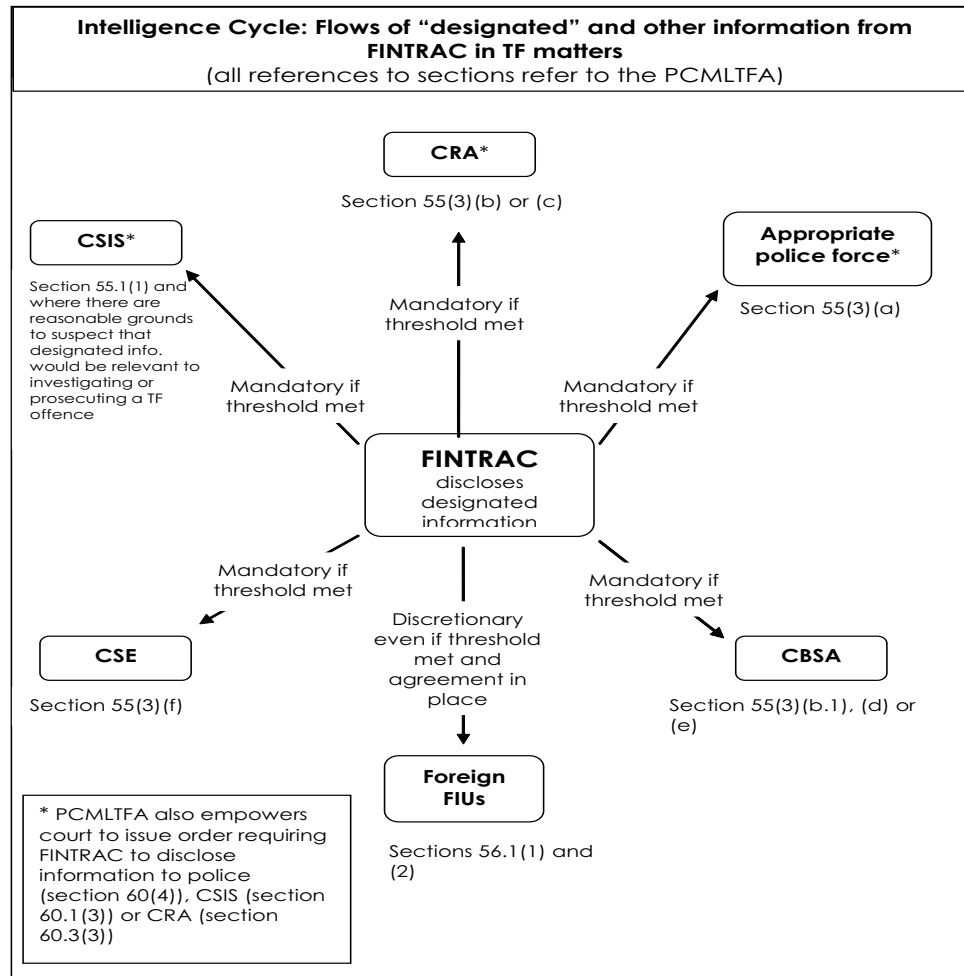


[Exhibit P-233, Tab 21 pp. 6 and 8 (Public Production # 3759)]

3.2.5 Disclosure of Information

3.2.5.1 Conditions for FINTRAC Disclosures

After completing its analysis,¹⁴⁷ FINTRAC must or may, if the legal threshold is met, disclose “designated information” to specific agencies. The following chart¹⁴⁸ explains the different tests for disclosure by FINTRAC:



¹⁴⁷ PCMLTFA, s. 54(c).

¹⁴⁸ Some provisions were in place before the *Anti-terrorism Act* – for example, in the *Proceeds of Crime (Money Laundering) Act* in regard to money laundering. The purpose of this chart is to differentiate between the provisions contained in Bill C-25 and those in place before in regard to TF. Anything which preceded Bill C-25 is labelled “ATA.” Likewise, since agencies such as the Canada Customs and Revenue Agency and the Department of Citizenship and Immigration have changed, disclosure rules that may have been modified to apply to different recipients were not identified as “new” in the chart. For example, the previous s. 55(3)(b) was amended and disclosure can now be made to two agencies instead of one because of organizational changes. As such, the “new” provisions are still labelled as originating in the *Anti-terrorism Act*.

1 st Test	2 nd Test	Recipient	PCMLTFA	Since
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	None.	Police	55(3)(a)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada;	None.	CSIS	55.1(1)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to an offence of obtaining or attempting to obtain a rebate, refund or credit to which a person or entity is not entitled, or of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue;	CRA	55(3)(b)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also has reasonable grounds to suspect that the information is relevant to determining whether a registered charity, as defined in subsection 248(1) of the <i>Income Tax Act</i> , has ceased to comply with the requirements of that Act for its registration as such;	CRA	55(3)(c)(i)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also has reasonable grounds to suspect that the information is relevant to determining whether a person or entity that the Centre has reasonable grounds to suspect has applied to be a registered charity, as defined in subsection 248(1) of the <i>Income Tax Act</i> , is eligible to be registered as such;	CRA	55(3)(c)(ii)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to an offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Agency;	CBSA	55(3)(b.1)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to determining whether a person is a person described in sections 34 to 42 of the <i>Immigration and Refugee Protection Act</i> or is relevant to an offence under any of sections 117 to 119, 126 or 127 of that Act;	CBSA	55(3)(d)	ATA
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to investigating or prosecuting an offence of smuggling or attempting to smuggle goods subject to duties or an offence related to the importation of goods that are prohibited, controlled or regulated under the <i>Customs Act</i> or under any other Act of Parliament;	CBSA	55(3)(e)	C-25
If FINTRAC has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence;	If FINTRAC also determines that the information is relevant to the mandate of the Communications Security Establishment referred to in paragraph 273.64(1)(a) of the <i>National Defence Act</i> .	CSE	55(3)(f)	C-25
If FINTRAC has reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence [and has a MOU in place];	In response to a request made by the institution or agency [FIU].	Foreign FIU	56.1(1) or (2) and 56.1 (2.1)	ATA
If FINTRAC has reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence [and has a MOU in place];	In order to perform its functions, FINTRAC may direct queries to an institution or agency [FIU] and in doing so it may disclose designated information.	Foreign FIU	56.1(1) or (2) and 56.1 (3)	ATA

Using an example from the chart, FINTRAC is required to disclose designated information to a law enforcement agency or CSIS if it meets the first test described in the chart – that FINTRAC has “...reasonable grounds to suspect that designated information *would be* relevant...” The conditions for disclosing to agencies other than CSIS and the RCMP are stricter. FINTRAC must satisfy not only the first test, but a second test as well. For example, the *PCMLTFA* requires FINTRAC to disclose designated information to the CRA under section 55(3)(b) of the *PCMLTFA*, but only if FINTRAC satisfies two tests:

- It has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, and
- It determines that the information is relevant to an offence of obtaining or attempting to obtain a rebate, refund or credit to which a person or entity is not entitled, or of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue.

Potter explained the reason for a more stringent test when FINTRAC deals with the CRA:

I think the intent of the original legislation and the way we were put together was, we're a money laundering/terrorist financing financial intelligence unit, so that's our core focus. There are other agencies, like CRA that deal with tax evasion most directly. So I think there was a concern that might – at a minimum, there would be the perception that somehow this new agency was created and was going to be looking at your taxes.¹⁴⁹

There is no definition of “reasonable grounds to suspect” in the *PCMLTFA* and no case law about its interpretation in the context of that legislation.¹⁵⁰ FINTRAC therefore relies on the case law interpreting the expression in other contexts.¹⁵¹

Based on [various courts' interpretations of similar phrases], it would appear clear that FINTRAC would have “reasonable grounds to suspect” that information it would be disclosing would be relevant to investigating or prosecuting a terrorist

¹⁴⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6970-6971.

¹⁵⁰ FINTRAC Response on Reasonable Grounds to Suspect, p. 3.

¹⁵¹ FINTRAC Response on Reasonable Grounds to Suspect, p. 3. See pp. 4-5 of the same document for jurisprudence on this subject.

activity financing offence when police provide FINTRAC with voluntary information regarding individuals and businesses of interest to them in the context of a particular investigation.¹⁵²

The *PCMLTFA* requires FINTRAC to disclose designated information to CSIS if FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada.¹⁵³ One FINTRAC document provided to the Commission states that any “terrorist activity financing offence,” as defined in the *PCMLTFA*, would constitute a “threat to the security of Canada” as defined in the *Canadian Security Intelligence Service Act (CSIS Act)*.¹⁵⁴ Accordingly, if the FINTRAC interpretation is accurate, when FINTRAC has reasonable grounds to suspect that financial intelligence would be relevant to investigating a terrorist activity financing offence, this would also constitute reasonable grounds to suspect that the intelligence would be relevant to “threats to the security of Canada.” FINTRAC would be obliged to disclose the information to CSIS as well as whichever other agency to which the *PCMLTFA* requires disclosure. In short, if FINTRAC finds information that could be relevant to investigating or prosecuting a TF offence – barring possible limits on disclosure contained in VIRs sent to FINTRAC – FINTRAC must disclose information to CSIS as well as to other recipients.

However, the converse is not necessarily true. “Threats to the security of Canada” can take many forms that do not involve TF. If FINTRAC has reasonable grounds to suspect that designated information would be relevant to a threat to the security of Canada that does not involve TF – espionage, for example – FINTRAC must disclose the information only to CSIS.

FINTRAC has the discretion to disclose information to foreign FIUs with which it has a memorandum of understanding (MOU) on grounds similar to those for which it is obliged to disclose information to Canadian law enforcement agencies.¹⁵⁵ These MOUs must be approved by the Minister of Finance¹⁵⁶ and are limited in scope.¹⁵⁷ Before entering into an MOU with a foreign FIU, FINTRAC assesses the country’s legal regime, relying on input from local partners.¹⁵⁸ FINTRAC seeks assurances that the country has adequate privacy measures to

¹⁵² FINTRAC Response on Reasonable Grounds to Suspect, p. 5. This does not appear to be far removed from direct access by recipients of FINTRAC information to FINTRAC’s database, notwithstanding the prohibition to do so.

¹⁵³ *PCMLTFA*, s. 55.1.

¹⁵⁴ Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).

¹⁵⁵ *PCMLTFA*, s. 56.1(2); Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7010-7012. The Terrorist Financing Dossier notes that, “When FINTRAC decides whether to enter into an information-sharing agreement with a foreign financial intelligence agency, it considers the country’s willingness and ability to protect the information that FINTRAC provides and to honour the restrictions that FINTRAC places on the information”: p. 41, note 188. For a list of FINTRAC’s MOU Partners as of July 2007, with the name of each FIU and the date of signature, see Exhibit P-233, Tab 18: FINTRAC MOU Partners.

¹⁵⁶ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7010; *PCMLTFA*, s. 56(2). The Minister may also enter into MOU agreements: see *PCMLTFA*, s. 56(1).

¹⁵⁷ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.

¹⁵⁸ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.

protect the information sent to its FIU.¹⁵⁹ Privacy concerns are one reason for FINTRAC's reluctance to sign MOUs with some foreign FIUs:

Ideally, FINTRAC would be able to exchange information with every FIU in the world in pursuit of the money trail, without reservations, wherever that trail may lead. Practically, however, this desire to obtain information must be balanced with the need to ensure that FINTRAC is exchanging information with partners who will safeguard that information from unauthorized disclosure.¹⁶⁰

In its 2007 Annual Report, FINTRAC stated that it had agreements with FIUs from 45 countries.¹⁶¹ The 2008 Annual Report stated that FINTRAC signed agreements with two new FIU partners in Sweden and the island of St. Kitts and Nevis.¹⁶²

When asked why none of the FIUs with whom FINTRAC had signed MOUs are located in countries that are "hotspots" of terrorism, FINTRAC offered two main explanations:

- FINTRAC's selection of MOU partners does not exclusively focus on TF, but also on money laundering. The MOU may be directed at money laundering alone and reflect the fact that a country is a money laundering "hotspot," but not a significant source of terrorism or TF; and
- Many jurisdictions that could be considered terrorism "hotspot" may have FIUs, but the FIUs may be in the early stages of development and they may not yet be members of the Egmont Group. All Egmont members undergo an operational evaluation before admission to ensure that they are able to maintain an agreed level of standards and practices. [The implication of this response by FINTRAC is that FINTRAC is reluctant to make an agreement with an FIU that has not passed the Egmont evaluation.]¹⁶³

FINTRAC did note, however, that it had MOUs with countries that have been targets of terrorist acts, including Spain, France, Israel, Indonesia, Colombia, the US and the UK.¹⁶⁴ After MOUs are in place, FINTRAC continues to monitor foreign countries' legal frameworks.¹⁶⁵

¹⁵⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7011.

¹⁶⁰ Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a)(i).

¹⁶¹ FINTRAC 2007 Annual Report, p. 27. FINTRAC had MOUs with 30 FIUs in 2006 and 20 in 2005: see

FINTRAC 2007 Annual Report, "FINTRAC Highlights 2005-2007," on the page following the report cover.

¹⁶² FINTRAC 2008 Annual Report, p. 20.

¹⁶³ Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a).

¹⁶⁴ Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(a).

¹⁶⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7011-7012. As of January 2008, FINTRAC had conducted outreach visits to the FIUs of Australia, Bahamas, Barbados, Belgium, Cayman Islands, Hong Kong, Israel, Italy, Mexico, Netherlands, Spain and the United States: Second FINTRAC Response to Supplementary Questions of the Commission, Question 6(d).

3.2.5.2 What FINTRAC Discloses

FINTRAC discloses only “designated information.” The *PCMLTFA* defines “designated information” in three places,¹⁶⁶ and the applicable definition depends on the identity of the proposed recipient. Before the changes introduced by Bill C-25, only limited information – basically raw data¹⁶⁷ – could be disclosed, limiting the potential value of FINTRAC disclosures. As a result, recipients often had to do their own analysis of the information they received, causing delay and wasting resources.

Bill C-25 added new categories of information to what constituted “designated information” in the *PCMLTFA*. FINTRAC’s 2008 Annual Report spoke of how this enhanced the value of FINTRAC’s disclosures to other agencies:

With the new provisions, our case disclosures can include a greater range of information relating to financial transactions, and the number of agencies to which we are authorized to make them has increased. Consequently, because our financial intelligence is enriched, its value in investigations is enhanced. Feedback from the law enforcement and intelligence communities already reflects this enhancement.¹⁶⁸

The same report spoke of the more general “products” of FINTRAC’s analysis that it discloses:

In 2007-08, we produced and disseminated a wide range of well-received strategic analysis products to our partners. Among these were “The Watch”, an environmental scan focused on money laundering and terrorist activity financing issues; “Backgrounders”, which present a general overview of emerging trends and typologies; and financial intelligence “Briefs” which provide a more in-depth assessment of our reports and disclosures. As in the past, “Perspectives” were also produced to offer a retrospective of our disclosures and reports, and to identify typologies and patterns of transactions in relation to a particular subject or theme.¹⁶⁹

The chart below shows the expanded categories of information included in the definition of “designated information” (the definitions in sections 55(7), 55.1 and 56.1 are identical at present).

¹⁶⁶ *PCMLTFA*, ss. 55(7), 55.1(3), 56.1(5).

¹⁶⁷ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6918.

¹⁶⁸ FINTRAC 2008 Annual Report, p. 4.

¹⁶⁹ FINTRAC 2008 Annual Report, p. 8.

	PCMLTFA on December 1 st , 2006 Section 55(7)	PCMLTFA on June 13 th , 2008 Section 55(7)
(a)	the name of the client or of the importer or exporter, or any person acting on their behalf;	the name of any person or entity that is involved in the transaction, attempted transaction, importation or exportation, or any person or entity acting on their behalf;
(b)	the name and address of the place of business where the transaction occurred or the address of the customs office where the importation or exportation occurred, and the date the transaction, importation or exportation occurred;	the name and address of the place of business where the transaction occurred or the address of the customs office where the importation or exportation occurred, and the date the transaction, importation or exportation occurred;
(c)	the amount and type of currency or monetary instruments involved or, in the case of a transaction, if no currency or monetary instruments are involved, the value of the transaction or the value of the funds that are the subject of the transaction;	the amount and type of currency or monetary instruments involved or, in the case of a transaction, if no currency or monetary instruments are involved, the value of the transaction or the value of the funds that are the subject of the transaction;
(d)	in the case of a transaction, the transaction number and the account number, if any;	in the case of a transaction, the transaction number and the account number, if any;
(e)*	any other similar identifying information that may be prescribed for the purposes of this section.	<i>*similar section is now at (f) in the current PCMLTFA*</i>
(e)*		the name, address, electronic mail address and telephone number of each partner, director or officer of an entity referred to in paragraph (a), and the address and telephone number of its principal place of business;
(f)		any other similar identifying information that may be prescribed for the purposes of this section;
(g)		the details of the criminal record of a person or entity referred to in paragraph (a) and any criminal charges laid against them that the Centre considers relevant in the circumstances;
(h)		the relationships suspected by the Centre on reasonable grounds to exist between any persons or entities referred to in paragraph (a) and any other persons or entities;
(i)		the financial interest that a person or entity referred to in paragraph (a) has in the entity on whose behalf the transaction was made or attempted, or on whose behalf the importation or exportation was made;
(j)		the name of the person or entity referred to in paragraph (a) suspected by the Centre on reasonable grounds to direct, either directly or indirectly, the transaction, attempted transaction, importation or exportation;
(k)		the grounds on which a person or entity made a report under section 7 about the transaction or attempted transaction and that the Centre considers relevant in the circumstances;
(l)		the number and types of reports on which a disclosure is based;
(m)		the number and categories of persons or entities that made those reports;
(n)		indicators of a money laundering offence or a terrorist activity financing offence related to the transaction, attempted transaction, importation or exportation.

As the chart shows, Bill C-25 brought a significant increase in the information qualified as designated information. FINTRAC now discloses links between the various parties identified in the disclosures, as well as the indicators of suspicious activity and the original grounds for an STR. Still, FINTRAC cannot of its own accord disclose its analysis in a specific case or the written justification for its disclosures.¹⁷⁰ FINTRAC explained that "...[t]he decision to allow disclosure of strictly factual information was, once again, a deliberate one to counterbalance the fact that FINTRAC would be making its disclosures based on the 'reasonable grounds to suspect' threshold, which is the least onerous legal standard possible that is not entirely subjective."¹⁷¹

Although Bill C-25 added new categories to the information that FINTRAC discloses, law enforcement agencies or CSIS may still need to analyze the information – in essence, repeating the analysis that FINTRAC has already done. Law enforcement agencies, CRA and CSIS can obtain a FINTRAC analysis (as opposed to designated information) only by obtaining a production order.¹⁷²

The 2008 FATF Mutual Evaluation of Canada stated that 14 production orders had been sought to that point by law enforcement.¹⁷³ It is not known whether any of these orders related to TF, but the main point is the relatively small number of orders, even if all had related to TF.

3.2.5.3 How FINTRAC Discloses

FINTRAC has a rigorous internal case approval process that aims to ensure that the required threshold for disclosures is met.¹⁷⁴ The final decision to disclose rests with FINTRAC's Disclosure Committee, chaired by the Director of FINTRAC. If the disclosure package is approved, it is provided to recipients. The process can extend over a few weeks in a money laundering case, a period which may be reasonable since such an investigation is essentially reactive and the circumstances of the case do not generally threaten lives. In TF cases, however, lives can be at immediate risk and there may be a need to disclose information promptly. FINTRAC assured the Commission that the turnaround time in TF cases from receipt of a VIR to disclosure to an agency can be as fast as 24 hours and that FINTRAC gives TF disclosures priority.¹⁷⁵

FINTRAC disclosures are made without any caveat on the use of the information. It is expected that the recipient will use the information to further its investigations.¹⁷⁶ The information disclosed by FINTRAC could potentially become public if a prosecution proceeds or if the recipients decide for any other reason to make the information public.

¹⁷⁰ FINTRAC Response on Reasonable Grounds to Suspect, p. 2.

¹⁷¹ FINTRAC Response on Reasonable Grounds to Suspect, p. 2.

¹⁷² Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 7016; *PCMLTFA*, ss. 60, 60.1, 60.3.

¹⁷³ These numbers are probably current as of the time of the FATF on-site visit, which occurred early in 2007.

¹⁷⁴ See Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6983-6984 for an explanation of the process.

¹⁷⁵ Second FINTRAC Response to Supplementary Questions of the Commission, Question 4(a). See also 2008 FATF Mutual Evaluation of Canada, para. 375.

¹⁷⁶ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6994.

FINTRAC's 2008 Annual Report stated that FINTRAC made 210 disclosures of cases during the year under review. Of this total, 171 were associated with money laundering, 29 with TF and other "threats to Canada's safety," and 10 with both money laundering and TF.¹⁷⁷ The 2008 Annual Report did not state the value of the disclosures. However, the 2007 Annual Report indicated that there were roughly \$10 billion in suspicious transactions,¹⁷⁸ of which about \$208 million related to suspected TF or threats to the security of Canada.¹⁷⁹

The amounts involved in individual disclosures are generally much smaller in TF cases than in money laundering cases. In 2005-06, the biggest single disclosure in a TF case involved about \$98 million, with the average being \$919,000 and the smallest being under \$10,000. In contrast, the amounts involved in money laundering disclosures were at least \$10,000, with the largest being \$886 million.¹⁸⁰ The following chart shows the range in value of FINTRAC disclosures related to suspected TF:¹⁸¹

Threats and/or Terrorist Financing (Number of Cases)		
	2005-06	2006-07
0 - \$1M	17	18
\$1M - \$10M	13	10
\$10M - \$50M	1	4
\$50M - \$100M	2	1
\$100M - \$500M	0	0
\$500M - \$1B	0	0
\$1B +	0	0
Total Number of Disclosures	33	33

¹⁷⁷ FINTRAC 2008 Annual Report, p. 9.

¹⁷⁸ FINTRAC 2007 Annual Report, p. 8.

¹⁷⁹ Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(e); FINTRAC 2007 Annual Report, p. 8. In 2005-06, FINTRAC made 168 case disclosures involving slightly more than \$5 billion in suspect financial transactions. Of these disclosures, 33 were for suspected terrorist activity financing and/or other threats to the security of Canada. One disclosure involved both suspected money laundering and suspected terrorist activity financing and/or threats to the security of Canada. Of the roughly \$5 billion in suspicious transactions, approximately \$256 million related to suspected terrorist activity financing and other threats to the security of Canada: FINTRAC 2006 Annual Report, p. 8.

¹⁸⁰ Exhibit P-233, Tab 13: FINTRAC Disclosure Value Chart, p. 1.

¹⁸¹ Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(i).

The number and dollar value of FINTRAC disclosures has steadily increased over the years for both TF and money laundering. According to FINTRAC, the increase in the value of disclosures flows from its strategy of focusing on large cases, its deeper knowledge of trends, more experienced staff, improved computer systems, and its growing database.¹⁸²

In its 2007 Annual Report FINTRAC stated that the demand for its intelligence attested to its quality. The report also stated that feedback from law enforcement offered a clear indication of the value of the financial intelligence it provided.¹⁸³ As noted above, however, the 2008 Annual Report provided no indication of the dollar value of FINTRAC's disclosures for the period covered by the report.

FINTRAC officials explained that the dollar value of disclosures did not indicate the actual amount of TF taking place. This was because FINTRAC only needs to *suspect* that certain transactions are relevant to investigating a TF offence for it to disclose information. Even so, it included the value of these transactions in the total value of its disclosures.

One FINTRAC document stated that the value of a particular transaction is "...not necessarily the most relevant piece of the intelligence puzzle," adding that, for example, names of individuals and account numbers may have more intelligence value.¹⁸⁴

3.2.6. Relationships between FINTRAC and Other Agencies

3.2.6.1 In General

As noted earlier, FINTRAC stands at arm's length from other agencies.¹⁸⁵ The arm's-length relationship is intended to address privacy concerns. A central issue is how to achieve a workable compromise between investigative efficiency and privacy rights. The objects of the *PCMLTFA* are relevant in searching for this compromise, since they include responding to the needs of law enforcement "...while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves."¹⁸⁶

The 2008 FATF Mutual Evaluation of Canada described the justification advanced for the arm's-length relationship:

The decision to provide police and other recipients with designated information only when FINTRAC reaches its threshold, rather than to provide unrestricted access to FINTRAC's data holdings, reflects the fact that FINTRAC receives

¹⁸² FINTRAC 2007 Annual Report, p. 9.

¹⁸³ FINTRAC 2007 Annual Report, pp. 4, 10.

¹⁸⁴ Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(b).

¹⁸⁵ The term "arm's length" is used in the *PCMLTFA*: see s. 40(a).

¹⁸⁶ *PCMLTFA*, s. 3(b).

a large amount of varied financial information on persons and entities, the vast majority of which is legitimate and not relevant to any investigation or prosecution.¹⁸⁷

Janet DiFrancesco of FINTRAC testified that standing at arm's length from other bodies is an advantage:

[O]ur regime...was created to be consistent with the *Charter of Rights*, and it does of course consider privacy laws but I think one of the advantages that FINTRAC does have, having been created at arm's length, is that we are also able to collect what we call more objective reports, prescribed transactions in terms of international wire transfers and large cash transaction reports.¹⁸⁸

The relationship between FINTRAC and Finance Canada was described earlier in this chapter. Potter testified that FINTRAC's relationship with both CSIS and the RCMP, the most typical recipients of its disclosures, was "positive."¹⁸⁹ He described the relationship as follows:

We would work with them...in a number of [areas other than disclosures], whether it be policy and legal development, whether it be research on new methods being used, typologies work; so there are a number of ways in which we would interact with the RCMP and CSIS beyond just the core relationship of providing disclosures.¹⁹⁰

Potter described FINTRAC's relationship with CBSA as less close, since CBSA is a recipient of FINTRAC disclosures under different conditions from those that exist for the RCMP and CSIS.¹⁹¹ FINTRAC continues to work on understanding and clarifying the conditions for disclosure to CBSA.

In 2004, the Auditor General¹⁹² reported reluctance among law enforcement agencies to share information with FINTRAC. However, Ms. DiFrancesco testified that there was no longer any reluctance to share.¹⁹³

FINTRAC also gives its partners macro-analyses (not to be confused with its analyses in individual cases, which it cannot disclose unless compelled by a

¹⁸⁷ 2008 FATF Mutual Evaluation of Canada, para. 382.

¹⁸⁸ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6967-6968.

¹⁸⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 7004-7005.

¹⁹⁰ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7004.

¹⁹¹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 7005.

¹⁹² *Report of the Auditor General of Canada to the House of Commons*, November 2004, Chapter 2: "Implementation of the National Initiative to Combat Money Laundering," para. 2.25, online: Office of the Auditor General of Canada <<http://www.oag-bvg.gc.ca/internet/docs/20041102ce.pdf>> (accessed January 16, 2009) [2004 Auditor General Report on Money Laundering].

¹⁹³ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7018-7019.

production order) and research documents on money laundering and TF. In 2006-07, it provided macro-analyses to ITAC and to the Criminal Intelligence Service Ontario.¹⁹⁴ FINTRAC also contributed to assessments and studies by the RCMP and CSIS.¹⁹⁵ One FINTRAC document provided to the Commission stated that, during recent years, "...strategic information has been provided on FINTRAC's drug, fraud, and FIU query related disclosures and on the use of NPOs and internet payment systems."¹⁹⁶

FINTRAC has specialized staff – Law Enforcement Liaison Officers – responsible for delivering disclosure packages to and obtaining feedback from law enforcement agencies. These officers also assist law enforcement agencies when they provide VIRs to FINTRAC.

Privacy concerns may arise from using secondments between FINTRAC and other agencies because of a fear that employees seconded from FINTRAC may use their FINTRAC connections to obtain information for the agency to which they are seconded, even if FINTRAC is not legally allowed or required to disclose the information.

3.2.6.2 Feedback to FINTRAC from Recipients of Disclosures

FINTRAC was criticized in the past for not disclosing sufficient information. Bill C-25 expanded the types of information that FINTRAC can or must disclose.

The Auditor General's November 2004 report found that police forces did not "give much weight" to unsolicited disclosures by FINTRAC.¹⁹⁷ RCMP Superintendent Reynolds assured the Commission that this was not the case, at least for the TF portion of the RCMP's work.¹⁹⁸

FINTRAC provides voluntary Disclosure Feedback Forms with all of its disclosures. It has been encouraging disclosure recipients to complete the form and to identify leads that the FINTRAC information may have produced. FINTRAC receives some, though not regular, feedback. FINTRAC does not view such feedback as a necessity, but admits that it is useful to learn about the impact of its work.¹⁹⁹ In some cases, FINTRAC does receive follow-up information from law enforcement agencies about ongoing investigations.

FINTRAC officials indicated that the issue of feedback from disclosure recipients will be addressed in the "performance management framework" that is being developed under Finance Canada's leadership. This framework will involve all of the partners in the federal government's AML/ATF Initiative.

¹⁹⁴ FINTRAC 2007 Annual Report, p. 24.

¹⁹⁵ Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).

¹⁹⁶ Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).

¹⁹⁷ 2004 Auditor General Report on Money Laundering, para. 2.25.

¹⁹⁸ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6885.

¹⁹⁹ Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 6994-6995.

As of January 2007, feedback to FINTRAC about the value of its disclosures produced the following results.²⁰⁰ The disclosures:

- related to persons/business/entity of interest: 79%
- were useful for intelligence purposes: 75%
- provided names/leads on previous unknowns: 62%
- were a major contribution: 24%
- were a minor contribution: 23%²⁰¹

Ms. DiFrancesco agreed with one counsel that feedback has a double benefit. If it is negative, it forces FINTRAC to make the appropriate changes. If it is positive, it can act as a morale booster.²⁰²

In addition to the voluntary feedback form, and in compliance with the Auditor General's recommendation encouraging FINTRAC to expand exchanges of information with other agencies, FINTRAC has initiated more frequent meetings with disclosure recipients. Meetings with the RCMP provide an opportunity to meet with RCMP investigators at both senior and working levels.²⁰³

Obtaining feedback through meetings and feedback forms is an ad hoc approach to evaluating the usefulness of FINTRAC. It is not required by law. As a result, meetings and feedback forms do not help to measure FINTRAC's performance systematically.

3.2.7 Interaction between FINTRAC and the Private Sector

Ms. Lafleur testified that FINTRAC and the anti-TF program are dependent on reporting entities.²⁰⁴ Millions of transaction reports are sent to FINTRAC every year, producing an ever-growing database.²⁰⁵ The *FINTRAC Report on Plans and Priorities For the years 2007-2008 to 2009-2010* noted that "...[t]he production of timely, high quality financial intelligence is dependant on reporting entities fulfilling their obligations to report and ensuring that the reported data is of high quality."²⁰⁶ In short, if FINTRAC does not receive reports of sufficient quality, its own analysis suffers.²⁰⁷ This in turn impedes the work of those to whom it discloses information.

²⁰⁰ See FINTRAC Disclosure Feedback Form, section 1, for the various categories. Disclosure recipients can select more than one answer.

²⁰¹ Exhibit P-233, Tab 17: FINTRAC Disclosure Feedback Statistics.

²⁰² Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, pp. 7014-7015.

²⁰³ Testimony of Mark Potter, vol. 56, October 2, 2007, pp. 6997-6998.

²⁰⁴ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6756.

²⁰⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6950. At the time of the Commission's hearings, the database was said to contain around 60 million reports: see Testimony of Janet DiFrancesco, vol. 56, October 2, 2007, p. 6957.

²⁰⁶ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 9.

²⁰⁷ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

3.2.7.1 FINTRAC Measures to Ensure Compliance by Private Sector Reporting Entities

FINTRAC has the obligation to ensure that reporting entities comply with the *PCMLTFA* and its regulations.²⁰⁸ A budget of \$16.2 million was designated for FINTRAC's compliance efforts during the 2007-08 fiscal year.²⁰⁹ FINTRAC's compliance examinations continue to demonstrate that the vast majority of reporting entities want to, and do in fact, comply with their legislative obligations.²¹⁰

FINTRAC cannot oversee compliance by all reporting entities because of their numbers. Instead, compliance focuses "...primarily [on] those sectors and entities that are most at risk for non-compliance."²¹¹ Compliance efforts consist of the following: awareness activities; monitoring data quality; questionnaires; on-site examinations; and taking appropriate remedial action when non-compliance is detected.²¹²

FINTRAC has begun to refocus its compliance activities to invest more resources in examining reporting entities. Entities are selected using a risk-based approach, focusing on reporting entities at highest risk of non-compliance.²¹³ The FINTRAC 2008 Annual Report stated that, in 2007-08, FINTRAC conducted 277 examinations, and the national and provincial regulatory agencies with which FINTRAC had a memorandum of understanding conducted 257 examinations. FINTRAC disclosed five cases of suspected non-compliance with reporting obligations to law enforcement for investigation and prosecution.²¹⁴

The FINTRAC 2008 Annual Report did not identify the deficiencies that examinations revealed. However, the 2007 Annual Report, covering 2006-07, identified the deficiencies found during that period:²¹⁵

²⁰⁸ *PCMLTFA*, s. 62.

²⁰⁹ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 13.

²¹⁰ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 15.

²¹¹ Exhibit P-233, Tab 7: FINTRAC's Risk-Based Approach, p. 1 [FINTRAC's Risk-Based Approach].

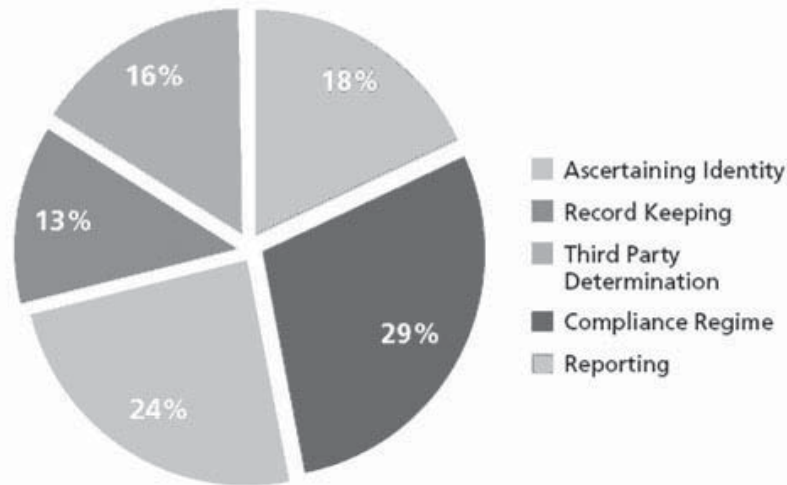
²¹² FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 13; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6986; FINTRAC's Risk-Based Approach.

²¹³ FINTRAC Report on Plans and Priorities for 2007-08 to 2009-10, p. 14.

²¹⁴ FINTRAC 2008 Annual Report, p. 17.

²¹⁵ FINTRAC 2007 Annual Report, p. 19.

Deficiencies Identified through Examinations



In performing compliance work, FINTRAC considers a wide range of factors, such as "...open source information, reporting volumes, observations gleaned from outreach activities, voluntary information which FINTRAC has received on non-compliance, results from compliance questionnaires completed by reporting entities, information received from regulators, quality and quantity assurance reviews, and the results of compliance examinations."²¹⁶ FINTRAC assigns a general risk level to reporting sectors based on these factors, although risk-based assessments of individual entities within the various reporting sectors are also done.²¹⁷

Compliance questionnaires, which FINTRAC considers an effective tool for monitoring compliance, are widely used. As a result, FINTRAC can cover many reporting entities at low cost.²¹⁸ In 2007-08, more than 6,000 questionnaires were sent to reporting entities.²¹⁹

Bill C-25 introduced a requirement for reporting entities to establish and implement a compliance program in addition to their reporting duties. The program is "risk-based," since it must include "...the development and application of policies and procedures for the person or entity to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity

²¹⁶ FINTRAC's Risk-Based Approach, pp. 1-2.

²¹⁷ FINTRAC's Risk-Based Approach, p. 2.

²¹⁸ Questionnaires assess compliance by reporting entities by asking about several subjects, such as the size and scope of the reporting entity's operation, the entity's business lines, the implementation of a compliance regime, compliance policies and procedures, review of compliance policies and procedures, and ongoing compliance training: see FINTRAC's Risk-Based Approach, p. 2.

²¹⁹ FINTRAC 2008 Annual Report, p. 17.

financing offence.”²²⁰ This risk-based approach is not designed to replace an approach based on simply complying with rules that require reporting (a “rules-based” approach). FINTRAC provides guidance on its website about setting up programs.²²¹

FINTRAC documents describe the risk-based approach for reporting entities in their compliance programs as consisting of the following elements:

- risk assessment of its business activities, using certain factors;
- risk-mitigation to implement controls to handle identified risks;
- keeping client identification and, if required for its sector, beneficial ownership information up to date; and
- ongoing monitoring of financial transactions that pose higher risks.²²²

One submission on behalf of the Indian Nationals proposed greater reliance on a risk-based approach.²²³

FINTRAC also consults with other agencies that have responsibility for regulating entities covered under the *PCMLTFA*.²²⁴ FINTRAC states that this facilitates its compliance work and can help minimize duplication of effort and the burden imposed upon reporting entities. As of March 2007, FINTRAC had MOUs with the following agencies:

- Office of the Superintendent of Financial Institutions (OSFI);
- Investment Dealers Association of Canada (IDA);
- Alberta Gaming and Liquor Commission (AGLC);
- Financial Institutions Commission of British Columbia (FICOM);
- Gaming Policy and Enforcement Branch (BC)(GPEB);
- Credit Union Deposit Guarantee Corporation of Manitoba (CUDGC);
- Brunswick Credit Union Federation Stabilization Board Limited (“Risk Management Agency” (RMA));
- New Brunswick Department of Justice and Consumer Affairs, Insurance Branch;

²²⁰ *PCMLTFA*, ss. 9.6(1), 9.6(2).

²²¹ Financial Transactions and Reports Analysis Centre of Canada, “Guideline 4: Implementation of a Compliance Regime” (December 2008), online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp>> (accessed July 18, 2008).

²²² Financial Transactions and Reports Analysis Centre of Canada, “Guideline 4: Implementation of a Compliance Regime” (December 2008), Chapter 6: “Risk-Based Approach,” online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp#66>> (accessed August 6, 2008).

²²³ Submissions of the Family Members of the Crew Victims of Air India Flight 182 and Indian Nationals, Air India Cabin Crew Association, Sanjay Lazar and Aleen Quraishi, p. 45.

²²⁴ FINTRAC’s Risk-Based Approach, p. 2; *PCMLTFA*, s. 65(2).

- Office de stabilisation de la Fédération des caisses populaires acadiennes;
- Credit Union Deposit Guarantee Corporation of Newfoundland and Labrador (CUDGC);
- Nova Scotia Environment and Labour, Alcohol and Gaming Division;
- Nova Scotia Credit Union Deposit Insurance Corporation (NSCUDIC);
- Alcohol and Gaming Commission of Ontario (AGCO);
- Deposit Insurance Corporation of Ontario (DICO);
- Autorité des marchés financiers (Québec) (AMF);
- Credit Union Deposit Guarantee Corporation (Saskatchewan); and
- Saskatchewan Liquor and Gaming Authority (SLGA).²²⁵

These MOUs allow FINTRAC to "...regularly exchange statistics, risk assessment information, examination results, and examination plans" with these agencies.²²⁶ The arrangements do not constitute a delegation of authority to ensure compliance, since FINTRAC still conducts examinations in reporting sectors that are covered by MOUs.²²⁷ FINTRAC has described the work of its MOU partners as providing "significant supervisory coverage":

The work done by regulators to assess risk, examine entities, identify deficiencies, require corrective action and possibly sanction entities under their own powers serves to provide significant supervisory coverage of financial intermediaries with [Anti-money Laundering/TF] requirements.²²⁸

Besides concern about the adequacy of reports from reporting entities – in 2006-07, FINTRAC identified over 1300 cases where transaction reports were sent back to the originator, for what were considered mostly substantive issues²²⁹ – there is concern that not all reporting entities are reporting to FINTRAC. FINTRAC uses various strategies to identify non-reporting. These include media scans of entities that provide financial services, complaints from other reporting entities, identification by compliance officers or law enforcement agencies and information provided voluntarily by the public.²³⁰ FINTRAC also does a comparative analysis of reporting volumes among activity sectors.²³¹ As well, when it knows the identities of entities that fail to report, it contacts them in order to "bring them into the fold," and it undertakes on-site examinations in appropriate cases.²³²

²²⁵ FINTRAC 2007 Annual Report, p. 22.

²²⁶ FINTRAC's Risk-Based Approach, p. 3.

²²⁷ FINTRAC's Risk-Based Approach, p. 3.

²²⁸ FINTRAC's Risk-Based Approach, p. 3.

²²⁹ FINTRAC 2007 Annual Report, p. 18; First FINTRAC Response to Supplementary Questions of the Commission, Question 2(j).

²³⁰ Exhibit P-233, Tab 8: FINTRAC Determining and Dealing with "Non-Reporting," p. 1 [FINTRAC Determining and Dealing with "Non-Reporting"].

²³¹ FINTRAC Determining and Dealing with "Non-Reporting," p. 1.

²³² FINTRAC Determining and Dealing with "Non-Reporting," p. 1.

Amendments introduced by Bill C-25²³³ gave FINTRAC the authority to impose monetary penalties on entities that fail to comply with reporting requirements.²³⁴ Under the *PCMLTFA*, FINTRAC also has the authority to disclose non-compliance to the police.²³⁵ Fewer than 20 cases of non-compliance had been reported (as of the time of FINTRAC's 2008 Annual Report) to law enforcement agencies since the beginning of the compliance program in 2004.²³⁶ FINTRAC indicated that it disclosed non-compliance to law enforcement agencies when it saw little likelihood of compliance by an entity.²³⁷

Monetary penalties add flexibility to FINTRAC's compliance work. However, the Office of the Privacy Commissioner of Canada argued that if reporting entities become fearful of the penalties and the attendant negative publicity, they could try to minimize the risk and over-report to ensure compliance as a result.²³⁸ This would expand FINTRAC's databases to the point of allowing it to compile information on an even greater number of perfectly lawful transactions.

Other factors might lead to under-reporting of suspect transactions. For example, the lack of feedback by FINTRAC to reporting entities might lead the entities to conclude that the STRs they provide have little value in countering TF; as a result, the entities may become less vigilant and less likely to submit STRs, although they would still presumably report transactions that exceed a given monetary threshold.

3.2.7.2 Outreach and Guidance Tools

FINTRAC offers information sessions for reporting entities about changes in legislation,²³⁹ as well as to help them comply with their reporting obligations. Private sector reporting entities are reminded regularly how important it is to provide reliable information to FINTRAC.²⁴⁰

²³³ Bill C-25, s. 40, introducing ss. 73.1-73.5 to the *PCMLTFA*; 2008 FATF Mutual Evaluation of Canada, p. 311.

²³⁴ The IMF and World Bank Overview of FIUs mentions that: "To obtain compliance with the AML/CFT reporting obligations, there needs to be in place a set of measures intended to foster improvements in the flow and quality of reports without resort to sanctions, such as awareness raising and training," but that "...[a]fter an outreach program has been in place for a certain length of time, the FIU needs to consider the case of entities that fall below the level of reporting of the sector as a whole [...] [a]n array of administrative sanctions may be set out in the legislation to deal with non-compliant entities, and the application of the sanction varies according to the gravity of the offense": pp. 53-54.

²³⁵ *PCMLTFA*, ss. 65(1), 65(2).

²³⁶ FINTRAC 2008 Annual Report, p. 17.

²³⁷ First FINTRAC Response to Supplementary Questions of the Commission, Question 2(l)(i).

²³⁸ Exhibit P-278, Tab 5: Office of the Privacy Commissioner of Canada, Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, "Canada's Financial Monitoring Regime," September 2007, p. 4.

²³⁹ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

²⁴⁰ See, for example, Financial Transactions and Reports Analysis Centre of Canada, "Feedback on Suspicious Transaction Reporting: Banking Sector," para. 1.2, online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/FOR/2007-04-04/bsf-eng.asp#112>> (accessed October 3, 2008).

In 2007-08, FINTRAC employees delivered 370 presentations and seminars to reporting entities, reaching over 18,000 individuals. Among these were 24 information sessions in 10 cities about the new requirements of the *PCMLTFA* brought about by Bill C-25.²⁴¹ FINTRAC's 2008 Annual Report acknowledged that financial institutions and intermediaries subject to the *PCMLTFA* were "undoubtedly" in a "challenging period" as they prepared for changes to their legal obligations under the *PCMLTFA*.²⁴²

In addition, FINTRAC operates a call centre to answer general inquiries about FINTRAC's operations, as well as more specific questions about reporting requirements.²⁴³ In 2006-07, information officers answered 3,206 inquiries and the FINTRAC website received more than 600,000 "hits."²⁴⁴ The website contains guidance on several topics for reporting entities and the public. In addition, FINTRAC employees publish articles in trade journals and newsletters.²⁴⁵

FINTRAC also has on its website a section for "Feedback on reporting," where several topics are explored, such as suspicious transactions in the banking sector.²⁴⁶ The section offers several examples of typologies.

3.2.7.3 Views of Private Sector Reporting Entities about the Anti-TF Program

This Commission used various tools to learn the views of parties involved in the current anti-TF program. These included a survey of a group of private sector reporting entities conducted by the Deloitte consultancy. Deloitte asked a selection of reporting entities from across Canada for their observations about the anti-TF program. The survey was designed to provide a snapshot of views by sector. Two aspects of the Deloitte report warrant particular mention:

- The report was not intended to serve as hard evidence of the deficiencies of the anti-TF program. It was to be seen as an advisory report on various themes to inform the Commission, and as an opportunity for the Commission to receive other views; and
- The financial services sector received particular attention, since banks provide most of the financial transaction reports submitted to FINTRAC.

The Deloitte report raised several issues facing the private sector reporting entities. The issues are summarized below.

²⁴¹ FINTRAC 2008 Annual Report, p. 16.

²⁴² FINTRAC 2008 Annual Report, p. 4.

²⁴³ Department of Finance Memorandum of Evidence on Terrorist Financing, para. 4.33.

²⁴⁴ FINTRAC 2007 Annual Report, p 28. The FINTRAC 2008 Annual Report provided no statistics on this point.

²⁴⁵ Exhibit P-233, Tab 23: FINTRAC, "Overview of Canada's Financial Intelligence Unit – FINTRAC," CFE Ottawa Chapter Professional Development Day, October 18, 2006, p. 11.

²⁴⁶ Online: Financial Transactions and Reports Analysis Centre of Canada <<http://www.fintrac.gc.ca/publications/general-general-eng.asp#1>> (accessed October 3, 2008).

A. Lack of Understanding of the Distinction between Money Laundering and TF²⁴⁷

The report concluded that private sector reporting entities lack an understanding of how terrorist organizations fund their operations. The report noted that very few practical examples of TF have been provided to reporting entities,²⁴⁸ although FINTRAC and other bodies have identified the indicators that should lead a reporting entity to prepare an STR in TF matters.

B. Lack of Prominence of the TF Issue

Representatives from some reporting entities who were interviewed by Deloitte suggested that TF and terrorism in general do not appear to be a concern in Canada. One representative offered an explanation:

I mean quite frankly the threat of terrorism, although we hear about it and we talk about it to some degree as a Canadian entity, it's not that high a profile. I think because nothing's happened in the country yet, that's my personal belief.²⁴⁹

C. Lack of Feedback from FINTRAC to Reporting Entities²⁵⁰

According to Deloitte, reporting entities viewed their information as being sent on a one-way trip to FINTRAC. At present, said one interviewee, "...it's difficult to keep staff motivated and interested in screening for [terrorism property matches] without them feeling that they're contributing to something."²⁵¹ The report continued:

Those interviewed would like to see more feedback from FINTRAC in terms of whether or not their reporting is assisting, is useful and is of a benefit based on the time, effort, energy and cost that each institution expends to comply with the legislation.²⁵²

The lack of feedback also meant that reporting entities did not know whether they should continue to do business with some of their clients whose activities they had reported. One representative stated:

One of the things we asked ourselves was, okay, well if we've identified suspicious activity and we report it and then it happens again and we report it again... at what point...do

²⁴⁷ Exhibit P-241, Tab 2: Deloitte, Report of Findings as a Result of the Interviews of Regulated Entities on the Topic of Terrorist Financing In, Through and Out of Canada, September 28, 2007, para. 5.1.1 [Deloitte Report on TF].

²⁴⁸ Deloitte Report, para. 5.1.4.

²⁴⁹ Deloitte Report, para. 5.1.12.

²⁵⁰ Deloitte Report, para. 5.1.3.

²⁵¹ Deloitte Report, para. 5.1.9.

²⁵² Deloitte Report, para. 5.1.3.

we look at this and say we really shouldn't be or we need to be looking at whether we want to be doing business with this particular firm or client or entity.²⁵³

The Deloitte report included suggestions for improving feedback from FINTRAC. Some reporting entities expressed interest in more regular contact with the agencies responsible for national security matters – the RCMP and CSIS.²⁵⁴

FINTRAC does face some constraints in providing feedback. FINTRAC cannot provide feedback on the results its use of the information that reporting entities provide. Another reason invoked for restricting feedback is the possibility of alerting the individuals or groups being investigated.²⁵⁵ As well, FINTRAC receives so many reports that it would be impossible to follow up with reporting entities on each report, even if it wanted to.

FINTRAC believed that its current approach of providing guidance, but not feedback, was appropriate. Mark Potter of FINTRAC testified that FINTRAC spends considerable time providing “feedback” (more like guidance) to the private sector:

[W]e spend a lot of time providing feedback to the reporting entities, their associations and individual members on the quality of reports we're seeing, how they can improve, ways we can work better with them in implementing system changes, ensuring that they have sufficient lead time to change their IT systems if necessary, getting their views on what are the best means to provide the reports to us....²⁵⁶

Potter could not say whether it would be more effective if FINTRAC had the discretion to advise reporting entities on how their information was applied:

I'm not sure. I think I'd step back and ask: What is the objective here? And if the objective is to get consistent, high quality reporting from these entities there are other ways we can achieve that objective, giving them some sort of feedback on their individual forms that they provide and the reports they provide to us and providing general feedback on the results of the initiative broadly.²⁵⁷

²⁵³ Deloitte Report, para. 5.1.3.

²⁵⁴ Deloitte Report, para. 5.1.5.

²⁵⁵ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6987.

²⁵⁶ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6986.

²⁵⁷ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6988.

D. Costs of Complying with the PCMLTFA

Private sector reporting entities bear the cost of reporting to FINTRAC. The federal government considers this appropriate.²⁵⁸ It also appears to be in line with the current FATF policy.

Some reporting entities examined in the Deloitte report argued that complying with the *PCMLTFA* was costly.²⁵⁹ One called for federal government financial assistance to help all entities acquire appropriate technologies,²⁶⁰ especially since this would help them comply more effectively with the *PCMLTFA* and because they are doing this for the government's benefit.

Some reporting entities also wanted a "level playing field" for reporting entities and "broadly similar compliance obligations" as banks in other countries.²⁶¹ They wanted all private sector entities to be required to submit reports to FINTRAC. They complained that the obligations imposed on them were sometimes not applied to other types of reporting entities.²⁶² They spoke of gaps in coverage by the *PCMLTFA*: "white label" ATMs (ATMs that are not affiliated with a bank), money services businesses (MSBs), provincial mortgage brokers, pre-paid credit cards, stored value cards, Internet clearing houses such as PayPal, Internet gaming, precious metals, the legal profession and various religious communities.²⁶³

Several of the problems with gaps in coverage were corrected by Bill C-25 or are currently being reviewed. For example, MSBs and precious metals dealers are now covered by the *PCMLTFA*. The federal government is weighing options for white label ATMs and stored value and pre-paid cards.

E. Ineffectiveness of the Listing System

Some reporting entities complained that the lists of individuals identified as being associated with terrorism contained little biographical data beyond individuals' names. The entities claimed that this produced many false matches when an individual's name was similar to that of someone on the list, and that this in turn created much additional work for the entities, with no corresponding benefit.²⁶⁴ Some entities also believed that having to report on "politically-exposed persons" (PEPs) would increase their workload. The FATF defines PEPs as "...individuals who are or have been entrusted with prominent public functions such as Heads of State, senior politicians, senior government, judicial or military

²⁵⁸ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

²⁵⁹ Deloitte Report, para. 5.1.8.

²⁶⁰ Deloitte Report, para. 5.1.16.

²⁶¹ Deloitte Report, para. 5.1.10; Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6985.

²⁶² Deloitte Report, para. 5.1.11.

²⁶³ Deloitte Report, para. 5.1.11.

²⁶⁴ Deloitte Report, para. 5.1.9.

officials, senior executives of state-owned corporations and important political party officials.”²⁶⁵

Many reporting entities criticized the listing process. However, many names that appear on the lists used in Canada are not entirely its responsibility. For example, the *United Nations Al-Qaida and Taliban Regulations*²⁶⁶ (UNAQTR) listings are made by the United Nations Security Council and then adopted by Canada through regulation.

One interviewee noted that, since the lists were public, there was little chance that a listed individual would open a bank account using a name as it appeared on a list.²⁶⁷ For that reason, the lists were of little value. Their only benefit could be rapid checks by reporting entities immediately after the listing of an individual, but before the individual learned of the addition of their name to the list. However, despite its limitations, Canada is bound by international instruments to participate in the listing process.²⁶⁸

This concern about the utility of the listing process in dealing with suspect individuals did not apply to the *Criminal Code*²⁶⁹ list, which identifies terrorist groups, not individuals.

F. Other Issues

One reporting entity called for financial entities to increase the exchange of information about money laundering and TF.²⁷⁰ Some entities, aware that charitable organizations can be used to finance terrorist activity, believed that such organizations should be more actively monitored.²⁷¹

²⁶⁵ Department of Finance, *Enhancing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, Consultation Paper, June 2005, p. 12, online: Department of Finance <http://www.fin.gc.ca/activity/pubs/enhancing_e.pdf> (accessed October 2, 2008). The Consultation Paper continues: "While the FATF Recommendation focuses on foreign PEPs, countries are increasingly expanding the coverage of their regimes to both foreign and domestic PEPs, in line with the requirements of the United Nations Convention against Corruption and other international agreements. There is international concern, particularly for some foreign jurisdictions, that PEPs constitute higher risk customers for financial institutions and intermediaries as they have potentially greater opportunities to engage in corrupt activities, and Canada will do its part in the global fight against corruption. To prevent the laundering of the proceeds of corruption, financial institutions and intermediaries should take additional steps to identify customers that are PEPs and apply enhanced due diligence measures."

²⁶⁶ S.O.R./99-444.

²⁶⁷ Deloitte Report, para. 5.1.9.

²⁶⁸ For other criticisms of the listing regime (from an international standpoint), see Koh, *Suppressing Terrorist Financing and Money Laundering*, pp. 103-106.

²⁶⁹ R.S.C. 1985, c. C-46.

²⁷⁰ Deloitte Report, para. 5.1.16.

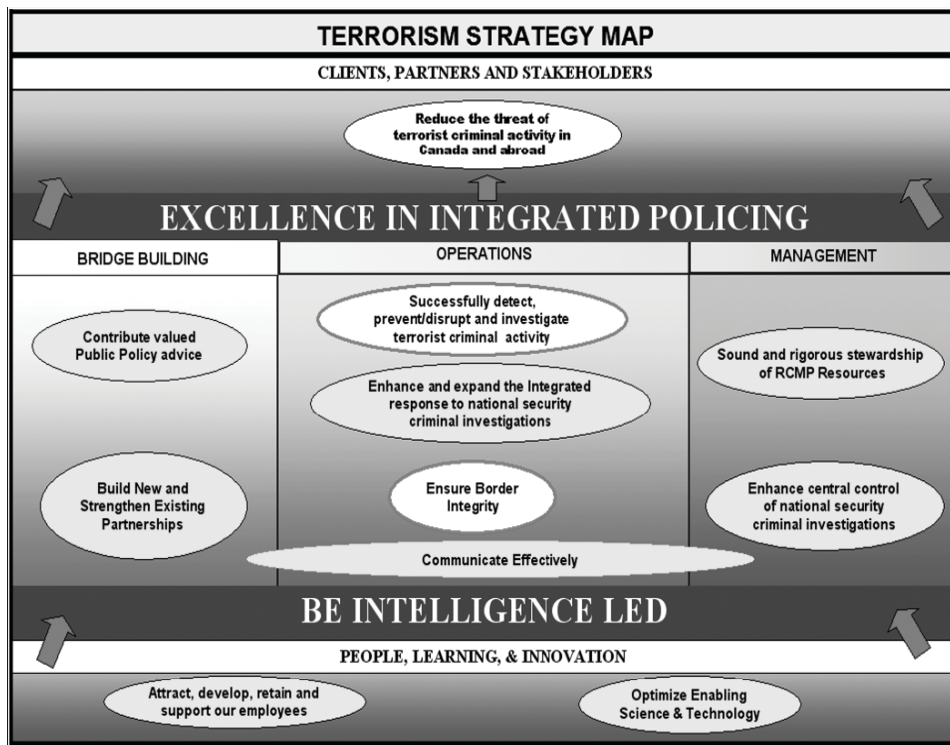
²⁷¹ Deloitte Report, para. 5.1.13.

3.3 Royal Canadian Mounted Police

3.3.1 Roles, Goals and Structure

As an agency in the portfolio of the Minister of Public Safety, the RCMP acts as Canada's national police force and as a contract provincial or local police force in several Canadian provinces, territories, municipalities and aboriginal communities.²⁷² The RCMP is considered to be the "default" law enforcement agency in TF matters.

A recent RCMP publication estimates that "...[a]s many as 50 terrorist organizations are present in some capacity in Canada, involved in a range of activities that include fundraising (with money sent abroad to finance terrorist efforts), weapons procurement, and human and commodity trafficking."²⁷³ The RCMP considers terrorism to be a priority. The RCMP's terrorism strategy is summarized in the following chart²⁷⁴ from its 2008-09 Report on Plans and Priorities:



²⁷² According to the RCMP's website, the RCMP provides a total federal policing service to all Canadians and policing services under contract to the three territories, eight provinces (except Ontario and Quebec), more than 190 municipalities, 184 aboriginal communities and three international airports: online: <<http://www.rcmp-grc.gc.ca/about-ausujet/index-eng.htm>> (accessed December 3, 2007).

²⁷³ Royal Canadian Mounted Police, *Royal Canadian Mounted Police Report on Plans and Priorities 2008-2009*, p. 47, online: Treasury Board Secretariat of Canada <<http://www.tbs-sct.gc.ca/rpp/2008-2009/inst/rcm/rcm-eng.pdf>> (accessed June 3, 2009) [RCMP 2008-09 Report on Plans and Priorities].

²⁷⁴ RCMP 2008-09 Report on Plans and Priorities, p. 48. A chart dealing with the Economic Integrity Strategy is found at p. 57.

The RCMP participates in the federal government's AML/ATF Initiative. The 2008 FATF Mutual Evaluation of Canada describes the RCMP's involvement in national security and TF matters:

469. The RCMP has an integrated model for responding to National Security Investigations (NSI), which forms part of the overall Public Safety Anti-Terrorism (PSAT) initiative. The NSI centrally coordinates and directs all national security investigations, intelligence and policy. At the operational level in each province of Canada, NSI serves as the policy centre for the Integrated National Security Enforcement Teams (INSETs) and the National Security Investigation Sections (NSIS).

470. The NSI includes a unit in Ottawa called the Anti-Terrorist Financing Team which consists of the RCMP and CRA. The team is responsible for (1) monitoring and coordinating major ongoing investigational projects related to terrorist organizations focusing primarily on their financial and procurement infrastructures and (2) liaising on a routine basis with partner agencies such as FINTRAC, CSIS and CRA Charities Directorate. The unit has also hosted terrorist financing courses in 2005 and 2006.

471. National Security Operations Branch (NSOB) supports and coordinates all national security field operations by reviewing, analyzing and disseminating information from all sources, including international partners, the CSIS, third parties and RCMP field investigations. NSOB also prepares subject profiles, case briefs and briefing notes for senior management, ensures compliance with RCMP policy, and tasks RCMP liaison officers in support of RCMP National Security investigations.

472. The Anti-Terrorist Financing Team (ATFT) supports counter-terrorism strategies with respect to financial intelligence investigations, enforcement, and the listing process in respect to Terrorist Entities.²⁷⁵

The RCMP created an Anti-Terrorist Financing Task Force in October 2001, making the Task Force permanent under its Financial Intelligence Branch in April 2002:

This intelligence/investigative body was established to support national security efforts to identify financial intelligence and enforcement opportunities related to terrorist financing, as well as to provide direction and support to field units. An Internet investigation team was established as part of the branch to investigate terrorist fundraising on the Internet.²⁷⁶

²⁷⁵ 2008 FATF Mutual Evaluation of Canada, paras. 469-472.

²⁷⁶ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.

Since October 2006, RCMP responsibilities in TF matters have fallen under the National Security Investigations Branch (NSI). The NSI is supervised by its own Assistant Commissioner, who reports to the Deputy Commissioner, Operations.²⁷⁷ One component of the NSI, the Anti-Terrorist Financing Team (ATFT), is dedicated to TF matters. The tasks of the ATFT are as follows:

- Monitor and coordinate major national security ongoing investigations (and projects) in terrorist matters, more specifically on the financing and procurement sides;²⁷⁸
- make recommendations based on the analysis of financial information received from various sources in matters related to TF offences;
- liaise with other anti-TF partners in Canada;²⁷⁹
- support the listing process.²⁸⁰

The ATFT consists of the RCMP and the CRA.²⁸¹ The RCMP also sends liaison officers to some countries to assist in the fight against money laundering and TF, and to perform other roles.²⁸²

3.3.2 Activities Aimed at Fighting TF

For about 18 months after TF offences appeared in the *Criminal Code* in late 2001, RCMP activity on terrorism matters as a whole remained focused on preventing attacks²⁸³ rather than on “following the money.” RCMP Superintendent Reynolds testified that this was because it takes time after legislation is adopted to put resources in place and to do investigations and gather evidence.²⁸⁴

Superintendent Reynolds also testified that the RCMP saw TF investigations as “highly complex” and lengthy. Simply gathering the evidence in a single case could take three years.²⁸⁵ He stated that every significant national security investigation includes a TF component.²⁸⁶ TF investigations address matters such as raising and moving funds and the procurement of materials.²⁸⁷ As of March 31, 2006, there were 90 active intelligence investigations and four major project investigations with respect to TF.²⁸⁸

²⁷⁷ Exhibit P-230, Tab 2: RCMP Organizational Chart.

²⁷⁸ 2008 FATF Mutual Evaluation of Canada, para. 470. The FATF Mutual Evaluation contains a description of the structure of the RCMP and other law enforcement agencies in regard to TF matters: see paras. 460-480.

²⁷⁹ 2008 FATF Mutual Evaluation of Canada, para. 470.

²⁸⁰ 2008 FATF Mutual Evaluation of Canada, para. 472.

²⁸¹ 2008 FATF Mutual Evaluation of Canada, para. 470.

²⁸² 2008 FATF Mutual Evaluation of Canada, paras. 179, 1554.

²⁸³ This is also described as “chasing the bomber.”

²⁸⁴ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6819.

²⁸⁵ Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6819-6820.

²⁸⁶ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.

²⁸⁷ Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6820-6821.

²⁸⁸ *Royal Canadian Mounted Police Departmental Performance Report for the period ending March 31, 2006*, p. 62, online: Treasury Board of Canada Secretariat <<http://www.tbs-sct.gc.ca/dpr-rmr/2005-2006/rcmp-grc/rcmp-grc-eng.pdf>> (accessed May 13, 2009).

When the RCMP receives information or intelligence relating to TF, it first determines whether a criminal investigation is warranted.²⁸⁹ In all TF investigations, RCMP Headquarters provides direction, international liaison, and central coordination with other agencies such as CRA and FINTRAC.²⁹⁰ Investigative teams gather the necessary intelligence.²⁹¹ The RCMP also relies to a great extent on Integrated National Security Enforcement Teams (INSETs) to investigate TF cases. The work of the INSETs is described later in this chapter.

Reynolds testified that the priority of the RCMP in TF investigations is always to prevent the loss of life, and that prevention and disruption of terrorist activities as a whole are by-products of TF investigations.²⁹² He testified that, although disruption can prevent individual terrorist incidents, it does not stop the desire to raise funds.²⁹³ Reynolds explained that another key goal of investigations is to understand the reach and capacity of organizations and identify the persons involved with the activities.²⁹⁴

Significant resources are devoted to the investigation of potential TF offences.²⁹⁵ Reynolds identified two main areas of concern: (i) micro-financing in respect of operations in support of individual terrorist actions and (ii) macro-financing to support certain organizations. He testified that investigations cannot be focused solely on the “bomber” (the terrorist act). They must focus as well on the larger organization behind the terrorist act.²⁹⁶ He stated that the RCMP does not have the capacity to investigate all potential TF matters.²⁹⁷

The RCMP also provides information to the CRA to help the Charities Directorate review applications for charitable status and assess whether existing charities comply with the *Income Tax Act*.²⁹⁸

The RCMP is the main recipient of FINTRAC’s disclosures of designated information.²⁹⁹ The *PCMLTFA* does not specifically require FINTRAC to disclose information to the RCMP, requiring disclosure only to “the appropriate police force.”³⁰⁰ However, the *Criminal Code* specifically identifies the RCMP when setting out the obligations of reporting entities. These entities must disclose to the RCMP Commissioner the existence of property in their possession that is connected to a terrorist group.³⁰¹

289 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.

290 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6825-6826.

291 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6890.

292 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.

293 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6824.

294 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6823.

295 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6880.

296 Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6827-6828.

297 Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6839.

298 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36; FINTRAC 2008 Annual Report, p. 11.

299 According to the Department of Finance, “The RCMP, through its money laundering and terrorist financing units, is the major recipient of disclosures from FINTRAC”: Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.

300 *PCMLTFA*, s. 55(3)(a).

301 *Criminal Code*, s. 83.1(1).

As well, in both money laundering and TF matters, the RCMP receives information from the CBSA, private sector reporting entities, other RCMP units, CSIS,³⁰² foreign partners and the public.³⁰³

The RCMP is involved in training and raising awareness among AML/ATF Initiative partners and the private sector, as well as police forces abroad. The Department of Finance Memorandum on Terrorist Financing noted that "...the RCMP has provided direct technical assistance and training to police forces in developing countries to help them conduct anti-money laundering and anti-terrorist financing investigations and enhance their investigative techniques."³⁰⁴ The ATFT also offers a course on TF,³⁰⁵ including Internet TF.

The RCMP participates in several domestic and international groups dealing with TF matters, such as the Financial Action Task Force, the G8 Law Enforcement Projects Subgroup (Roma/Lyon Group), the International Working Group on Terrorist Financing, the Terrorist Financing Working Group of the Canadian Bankers Association, the Five Eyes Terrorist Financing Working Group, and the Bi-lateral (US-Canada) Anti-Terrorist Financing Working Group.³⁰⁶

3.3.3 Resources

Superintendent Reynolds testified that in 2001 the RCMP had projected a need for about 126 individuals to cover both intelligence and investigations.³⁰⁷ That year, the RCMP acquired 17 positions for TF matters, of which three were assigned to three separate INSETs and 14 were assigned to RCMP Headquarters in Ottawa. Existing personnel in some INSETs were taken off other duties and assigned to TF matters. In 2006, the RCMP received additional funding. As a result, 33 new positions were created, for a total of 50 positions on TF matters.³⁰⁸

According to Reynolds, the resources challenge extended beyond proper funding. It took time to develop employees with the required skills for TF investigations. There were also problems with retaining employees because of competition for the same candidates within the private and public sectors. As well, not everyone in law enforcement was attracted to financial investigations.³⁰⁹ Reynolds testified that "court time" also took time away from investigations:

So, there has been an increase in the amount of court time, which isn't criticism by any standpoint but bearing in mind, as we spend more time authoring court processes, defending court processes or providing disclosure and responsibility to it,

³⁰² *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 19(2)(a) [CSIS Act].

³⁰³ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 36.

³⁰⁴ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.

³⁰⁵ 2008 FATF Mutual Evaluation of Canada, para. 470.

³⁰⁶ Exhibit P-383, Tab 7: Description of RCMP's Anti-Terrorist Financing Team.

³⁰⁷ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6838.

³⁰⁸ Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6824-6825.

³⁰⁹ Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6838-6841, 6892-6893.

that of course reduces the amount of time that could be spent on investigations.³¹⁰

The FATF addressed RCMP resources in its 2008 Mutual Evaluation of Canada:

[T]he RCMP lacks the resources that would allow it to focus on a larger spectrum of ML/TF investigations. The RCMP acknowledges that, due to resources constraints, it essentially dedicates its resources to large and complex ML investigations related to organised crime groups.³¹¹

The dissenting opinion of two MPs, Joe Comartin and Serge Ménard, who sat on the House of Commons subcommittee that reviewed the *Anti-terrorism Act* in 2007, described the importance of “operations” – intelligence and law enforcement efforts:

Terrorism cannot be fought with legislation; it must be fought through the efforts of intelligence services combined with appropriate police action. ...Therefore, one cannot expect that new legislation will provide the tools needed to effectively fight terrorism. Legislation can, however, be amended if police do not seem to have the legal means needed to deal with the new threat of terrorism.³¹²

Bromley emphasized in a paper for the Commission the need for law enforcement and other authorities to ask intuitive questions instead of relying on the analysis of complicated data.³¹³ Quiggin testified in support of being “on the ground” and on the front lines through community engagement.³¹⁴

³¹⁰ Testimony of Rick Reynolds, vol. 55, October 1, 2007, pp. 6842-6843.

³¹¹ 2008 FATF Mutual Evaluation of Canada, para. 517. See also 2008 FATF Mutual Evaluation of Canada, para. 468.

³¹² House of Commons Canada, Final Report of the Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act, Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues*, March 2007, p. 116, online: Parliament of Canada <<http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf>> (accessed May 25, 2009).

³¹³ Blake Bromley, “Funding Terrorism and Charities,” October 26, 2007, online: Benefic Group <<http://www.beneficgroup.com/files/getPDF.php?id=120>> (accessed May 12, 2009), p. 9.

³¹⁴ Testimony of Thomas Quiggin, vol. 91, December 7, 2007, p. 12078. Quiggin stated that, “.. in order to be effective in counterterrorism intelligence, you have to be literally on the ground with the people involved right out at the front lines; that means community engagement....If you have good community engagement programs, if you’re out working with people on the street day by day by day, you will be able to identify who the perpetrators are, who the radicals are.”

3.4 Canadian Security Intelligence Service (CSIS)

3.4.1 Role, Goals and Structure

CSIS is a civilian intelligence agency, established in 1984 and governed by the *Canadian Security Intelligence Service Act (CSIS Act)*.³¹⁵

CSIS investigates threats to the security of Canada, analyzes information and reports to and advises the Government of Canada about those threats. The CSIS website identifies the key threats that it investigates: terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure.³¹⁶ Terrorism is its main priority.³¹⁷ Neither the definition of “threats to the security of Canada” in the *CSIS Act* nor the description of the key threats investigated by CSIS specifically mention TF, but TF clearly forms part of the work of CSIS.³¹⁸ As noted earlier in this chapter, FINTRAC has concluded that the definition of “terrorist activity financing offence” in the *PCMLTFA* comes within the definition of “threats to the security of Canada” in the *CSIS Act*.³¹⁹

The ATA required FINTRAC to make disclosures to CSIS about threats to the security of Canada, whereas, before 2001, FINTRAC was focused solely on money laundering.³²⁰

The increase in concern about TF led CSIS to create a Terrorist Financing Unit (TFU) within its Counter Terrorism Branch in 2002, although CSIS had done some work on TF issues before then.³²¹ The mandate of the TFU is to identify and track financial structures which support terrorist organizations and to be a source of reliable intelligence for the Government of Canada.³²² A Security

³¹⁵ Canadian Security Intelligence Service, “History of CSIS,” online: Canadian Security Intelligence Service <<http://www.csis-scrs.gc.ca/hstrrtfcts/index-eng.asp>> (accessed September 15, 2009).

³¹⁶ Online: <<http://www.csis-scrs.gc.ca/bts/rfcs-eng.asp>> (accessed July 28, 2008). For more information on the various roles and responsibilities of CSIS, see the several background documents available online: <<http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/index-eng.asp>> (accessed August 8, 2008).

³¹⁷ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6912; Canadian Security Intelligence Service, “Backgrounder No. 8 – Counter-Terrorism,” online: Canadian Security Intelligence Service <<http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr08-eng.asp>> (accessed August 6, 2008) [CSIS Backgrounder on Counter-Terrorism], which states that: “Ensuring the safety and security of Canadians is one of the Government of Canada’s most important responsibilities. With this in mind, the government has identified counter-terrorism as the Canadian Security Intelligence Service (CSIS) number one priority.”

³¹⁸ Canadian Security Intelligence Service, *Public Report 2005-2006*, p. 5, online: Canadian Security Intelligence Service <<http://www.csis-scrs.gc.ca/pblctns/nlprpt/2005/rprt2005-eng.pdf>> (accessed July 28, 2008).

³¹⁹ Second FINTRAC Response to Supplementary Questions of the Commission, Question 1(d).

³²⁰ *PCMLTFA*, s. 55.1. Jim Galt of CSIS testified that “Money laundering is not part of CSIS mandate. It’s a criminal matter. If it came to our attention we’d immediately draw it to the attention of the RCMP but it’s not something that we look at. It’s not our -- as I say, it’s not our mandate.”: Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6921.

³²¹ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6939.

³²² Exhibit P-232, Tab 2: Security Intelligence Review Committee, *Review of the CSIS Investigation of Terrorist Financing Activities in Canada* (SIRC Study 2004-10), August 5, 2005, p. 5 [SIRC Study 2004-10].

Intelligence Review Committee (SIRC) study of a CSIS investigation of TF noted that, in 2002-03, a ministerial directive for the first time specifically directed CSIS to investigate and advise the Government of Canada about the threat arising from TF.³²³ The same SIRC study noted that the growing international focus on TF created the need for CSIS to focus more specifically on TF and to develop a level of expertise and continuity in this area.³²⁴

In May 2006, in a reorganization of CSIS operational branches, the TFU was moved from the Counter Terrorism Branch to the Human Sources/Operational Support Branch and renamed the Financial Analysis Unit (FAU).

The SIRC study described the CSIS approach to TF issues:

In February 2003, CSIS HQ issued a directional statement to explain the nature and objectives of the investigation into terrorist financing. According to this statement, its primary purpose was to collect and assess information in order to provide the Government of Canada with reliable intelligence on the extent and nature of terrorist financial support efforts in Canada, to provide assistance as required to law enforcement organizations, to respond as required under the [*Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*] and the *Anti-Terrorism Act*, and to fulfill other international commitments. The investigation was intended “to deter and disrupt the flow of funds to terrorists, thus hindering their ability to mount operations.”³²⁵

3.4.2 Activities Related to TF

Jim Galt, Director of the FAU at CSIS, testified that the FAU’s responsibility is to support the operational branches of CSIS through financial analysis. The FAU is the only unit of its kind at CSIS and it supports three major operational branches.³²⁶ Its mandate is to provide support to investigations with respect to financial aspects, and is not limited to TF.³²⁷ Besides using information in the CSIS database and open source information,³²⁸ the FAU receives reports that are sent to CSIS by private sector entities.³²⁹

Investigations are run by the operational unit that has conduct of and responsibility for a particular file.³³⁰ The FAU’s main responsibility is to view an operational file from a financial perspective to provide the operational branches

³²³ SIRC Study 2004-10, p. 6.

³²⁴ SIRC Study 2004-10, p. 9, referencing CSIS Counter Terrorism Program 2003-2004.

³²⁵ SIRC Study 2004-10, p. 13.

³²⁶ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6907.

³²⁷ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6906.

³²⁸ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6933.

³²⁹ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6927.

³³⁰ Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6906-6908.

with additional investigative leads, identify new targets or direct operational branches in other ways to further an investigation.³³¹ In his evidence, Galt stated that almost all CSIS operational files had a financial aspect.³³² The FAU brings together all the financial information received from FINTRAC or from regular CSIS investigations. Financial analysts on staff provide analysis of the information to the operational branches.³³³ The FAU's work may involve providing an operational branch with a quick analysis of a particular matter. In most cases, however, the FAU's work is part of an ongoing counterterrorism effort.³³⁴

CSIS sends VIRs, prepared by the FAU, to FINTRAC.³³⁵ Disclosure to FINTRAC was one of the first steps by the FAU after it receives a file.³³⁶ CSIS relies on section 12 of the *CSIS Act* to share information within government.

During fiscal year 2006-07, CSIS sent 30 to 40 VIRs to FINTRAC. In these VIRs, CSIS explains why a particular individual or group is considered a threat to the security of Canada.³³⁷ This helps FINTRAC to prepare its own analysis and its response to the VIR. FINTRAC must disclose "designated information"³³⁸ to CSIS if FINTRAC has reasonable grounds to suspect that the information would be relevant to threats to the security of Canada.³³⁹ CSIS is currently satisfied with the extent and quality of the disclosures from FINTRAC and finds the information it receives more detailed and useful than in the past.³⁴⁰

After obtaining approval from the Minister of Public Safety, CSIS can also apply to a judge for a production order requiring FINTRAC to disclose information – for example, information in addition to the designated information FINTRAC must disclose – to facilitate an investigation "in respect of a threat to the security of Canada."³⁴¹ CSIS does not maintain statistics on the usefulness of disclosures by FINTRAC. Galt testified that, like the RCMP, the FAU would prefer that the arm's-length relationship with FINTRAC become closer.³⁴²

Galt testified that the FAU now receives "some of their [FINTRAC's] analysis." There were some compatibility problems between CSIS and FINTRAC technology, leading to a less efficient transfer of information to the CSIS system.³⁴³ At the time of the Commission's hearings, discussions were underway to resolve this.³⁴⁴

331 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6908-6909.

332 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6909.

333 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6909.

334 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6921.

335 *PCMLTFA*, s. 54(a); *CSIS Act*, ss. 12, 19; Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6917.

336 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6941.

337 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6917.

338 For the purposes of disclosures to CSIS, "designated information" is defined in s. 55.1(3) of the *PCMLTFA*.

339 *CSIS Act*, s. 55.1.

340 CSIS Response to Supplementary Questions of the Commission, Question 3.

341 *PCMLTFA*, s. 60.1.

342 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6933.

343 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6918-6919.

344 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6919.

One of the main counterterrorism activities of CSIS is to provide information for Canada's listing process. In the process under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*,³⁴⁵ CSIS prepares an assessment for DFAIT and sits on the interdepartmental committee on listings.³⁴⁶ A CSIS background document on counterterrorism states that, since the creation of the list, CSIS has played a role in the listing of 40 entities, including Al Qaida, the Liberation Tigers of Tamil Eelam (LTTE) and Hezbollah.³⁴⁷ The FAU itself is not involved in this process.³⁴⁸

CSIS also has responsibility for making recommendations to the Minister of Public Safety regarding the issuance of a certificate under the *Charities Registration (Security Information) Act* (CRSIA) process – a process which can lead to denial of eligibility for charitable status or revocation of existing charitable status.³⁴⁹

The SIRC study mentioned above noted that efforts to combat TF required cooperation with domestic partners and that partners depended on CSIS for their enforcement actions. The study further stated that CSIS worked most closely with FINTRAC and the CRA's Charities Directorate in this regard.³⁵⁰ CSIS "liaised and cooperated closely with CRA in ongoing efforts to prevent the exploitation of registered Canadian charities to finance terrorist activity."³⁵¹ In fact, CRA often consults with CSIS before granting registered charity status, and Galt testified that CSIS would become involved as well in the process of issuing certificates under CRSIA.³⁵² The SIRC study stated that it had reviewed all CSIS exchanges of information with domestic partners and found that "with the exception of a few omissions in the use of tracking codes, they complied with the *CSIS Act*, Ministerial Direction, operational policy and relevant MOUs."³⁵³

SIRC also noted that CSIS respected its legal obligations, policies and MOUs in its dealings with foreign partners. SIRC observed that CSIS, during the period of its investigation, cooperated with more than 35 foreign partners on TF issues and that it gathered information on foreign legal frameworks that were aimed at fighting TF. CSIS representatives also attended several international conferences and presentations on TF.³⁵⁴

345 S.O.R./2001-360.

346 SIRC Study 2004-10, pp. 20-21.

347 CSIS Backgrounder on Counter-Terrorism.

348 Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6927.

349 *A New Review Mechanism for the RCMP's National Security Activities*, p. 190. The RCMP also makes recommendations to the Minister.

350 SIRC Study 2004-10, p. 15.

351 SIRC Study 2004-10, p. 17.

352 Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6929-6930, 6865.

353 SIRC Study 2004-10, p. 18.

354 SIRC Study 2004-10, p. 19.

3.4.3 Resources

When Galt testified before the Commission, the FAU had four permanent and three “borrowed” employees, occupied as follows:

- head;
- two contractual financial analysts (a chartered accountant and an RCMP officer formerly with the Integrated Proceeds of Crime unit);
- one individual seconded from CRA; and
- three intelligence officers.³⁵⁵

A tactical analyst position was not filled, at least in part because of a shortage of resources.³⁵⁶ CSIS as a whole had 2,449 full-time employees as of March 31, 2007.³⁵⁷ Galt testified that resources were a significant challenge³⁵⁸ and that he would have liked to see the FAU’s resources doubled or tripled.³⁵⁹ The lack of resources was limiting the service that the unit could provide:

[W]e are not able at this point to take on all operational files within the Service, mainly because of resourcing issues. So we have – we have gone through an exercise of creating a priority list of operational files that we look at, and with more resources obviously, I could expand that list. So resources are always an issue.³⁶⁰

CSIS made a request for 13 additional positions in 2008 to deal specifically with TF issues that had arisen since 2006. In addition, the February 2008 federal budget provided \$10 million between 2008-09 and 2009-10, to be shared by CSIS and CRA for their anti-TF efforts. CSIS stated that it will consider itself adequately financed on anti-TF matters if planned funding allocations are implemented.³⁶¹

3.5 Canada Border Services Agency

3.5.1 Role, Goals and Structure

The Canada Border Services Agency (CBSA), in the portfolio of the Minister of Public Safety, was created through a merger of departments. Since 2003, the

³⁵⁵ Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6909-6910.

³⁵⁶ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6915.

³⁵⁷ Canadian Security Intelligence Service, *Public Report 2006-2007*, p. 6, online: Canadian Security Intelligence Service <<http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2006/rprt2006-eng.pdf>> (accessed June 3, 2009).

³⁵⁸ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6922.

³⁵⁹ Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6910-6911.

³⁶⁰ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6910.

³⁶¹ CSIS Response to Supplementary Questions of the Commission, Question 1(b); Department of Finance, *The Budget Plan 2008, Responsible Leadership*, pp. 138, 140, online: Department of Finance <<http://www.budget.gc.ca/2008/pdf/plan-eng.pdf>> (accessed September 18, 2009). The budget allocation was intended to “bolster existing capacities”: p. 138.

CBSA has included the customs component of the former Canada Customs Revenue Agency, the enforcement/intelligence component of Citizenship and Immigration Canada and the enforcement component of the Canadian Food Inspection Agency. The *Canada Border Services Agency Act*³⁶² (*CBSA Act*) sets out the mandate of the CBSA, which includes the following:

...providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation, by

(a) supporting the administration or enforcement, or both, as the case may be, of the program legislation...

... and

(e) providing cooperation and support, including advice and information, to other departments and agencies of the Government of Canada to assist them in developing, evaluating and implementing policies and decisions in relation to program legislation for which they have responsibility.³⁶³

The FATF Special Recommendations on Terrorist Financing call for countries to have "...measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation." Furthermore, "...[c]ountries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed."³⁶⁴

Separate divisions of the CBSA deal with enforcement, intelligence and policy development. The activities and responsibilities of these divisions in TF matters are outlined below.

3.5.2 CBSA Activities

3.5.2.1 In General

CBSA's responsibilities in relation to terrorism and TF are to gather and disseminate intelligence in support of the administration and enforcement

³⁶² S.C. 2005, c. 38.

³⁶³ *Canadian Border Services Agency Act*, S.C. 2005, c. 38, s. 5(1).

³⁶⁴ See Special Recommendation IX of the FATF's "9 Special Recommendations (SR) on Terrorist Financing (TF)," online: Financial Action Task Force <http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_00.html#IXCashcourriers> (accessed February 11, 2009). The FATF has also published interpretive notes and best practices to help countries put in place the necessary regulations.

of the applicable rules regarding cross-border movements of currency and individuals.³⁶⁵ The CBSA is also in charge of the *Immigration and Refugee Protection Act* process involving foreign nationals or permanent residents who may have been involved in criminal activities such as TF, or who may pose a threat to the security of Canada.³⁶⁶ In short, the CBSA has two main “business lines” relating to terrorism and TF:

- detecting and monitoring the cross-border movement of currency and monetary instruments; and
- preventing the entry into Canada of persons who are not admissible because they may have been involved in terrorism or TF.³⁶⁷

Border Services Officers (BSOs) are trained to identify suspicious individuals as well as those who may be hiding contraband.³⁶⁸ The CBSA also uses “sniffer dogs” that can detect money,³⁶⁹ as well as scanners and other sophisticated equipment³⁷⁰ – technologies recently acquired in the fight against terrorism.³⁷¹ The Borders Enforcement Division of the CBSA provides guidance to BSOs in their anti-TF activities. Denis Vinette, Director of the CBSA Borders Enforcement Division, testified about how CBSA attempts to identify illegal activity among the large volume of individuals and vehicles entering Canada:

[We use] information we have in advance, either through our intelligence program [or] through our partnerships with other individuals, the training, the rigorous training our officers go through to prepare them to try and find those anomalies, either within individual behaviours, within documents, within patterns or trends...to try and deal with [the] significant challenge of finding that needle in the haystack.³⁷²

CBSA employees receive extensive training, including from the RCMP.³⁷³ Instead of creating a single unit charged with pursuing money laundering and TF, the CBSA has trained its 7,200 BSO officers across the country to deal with these matters.³⁷⁴ As a result, Vinette testified, “...[w]e didn’t get 40 or 50 or 100 resources that solely worked on this. We get the benefit of 7000.”³⁷⁵

³⁶⁵ Testimony of Tyson George, David Quartermain and Denis Vinette, vol. 56, October 2, 2007, pp. 7033-7035.

³⁶⁶ Testimony of Tyson George, vol. 56, October 2, 2007, pp. 7033, 7052-7053. See also the Department of Finance Memorandum of Evidence on Terrorist Financing, p. 37.

³⁶⁷ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7053.

³⁶⁸ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7036.

³⁶⁹ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7084.

³⁷⁰ 2008 FATF Mutual Evaluation of Canada, para. 585.

³⁷¹ For examples of the technologies, such as the “Snake Eye Camera” and the “Merlin Density Meter,” see 2008 FATF Mutual Evaluation of Canada, para. 588.

³⁷² Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7056-7057.

³⁷³ 2008 FATF Mutual Evaluation of Canada, para. 594.

³⁷⁴ Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7043-7044, 7049.

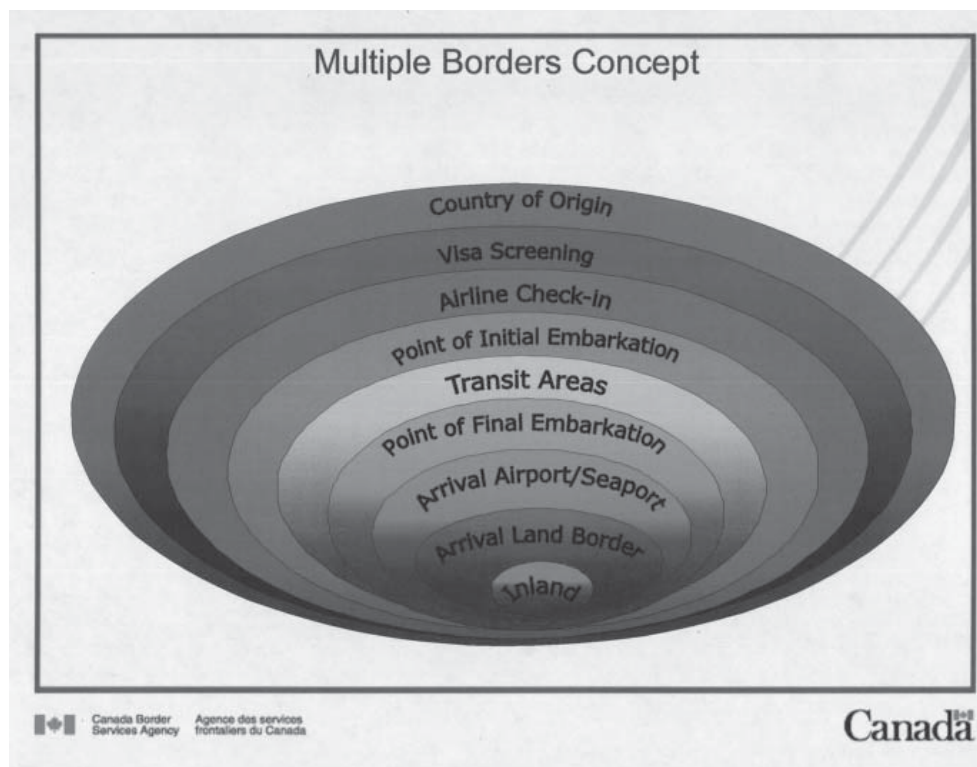
³⁷⁵ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7063.

CBSA's Strategic Intelligence Analysis Division has as its sole purpose producing analytical products on a number of topics, including TF and proceeds of crime.³⁷⁶ CBSA also collaborates with international partners in identifying TF cases.³⁷⁷

Within the Intelligence Directorate, the Borders Intelligence Division is charged with providing guidance to intelligence officers in the regions. The Division is the point of contact between headquarters and regional offices on TF matters. It has 44 "migration integrity officers" in 39 countries as well as three intelligence liaison officers overseas.³⁷⁸

3.5.2.2 The "Multiple Borders" Concept

The CBSA follows "multiple borders"³⁷⁹ concept to identify problematic behaviours or activities. This approach affords the CBSA multiple opportunities to identify individuals who may pose some threat to Canada. The concept is illustrated in the following chart³⁸⁰:



³⁷⁶ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7062.

³⁷⁷ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7062.

³⁷⁸ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7034.

³⁷⁹ Sometimes abbreviated to "multi borders," and also called a "layered safety net," or the "onion."

³⁸⁰ Exhibit P-235, Tab 7: Multiple Borders Concept Model [Multiple Borders Concept Model].

The outer layer of the “onion” is the country of origin of the person or activity being monitored. There are several components to this “outer layer”:

1. CBSA working with Citizenship and Immigration Canada visa officers;
2. CBSA's 44 Migration Integrity Officers, posted in various overseas locations, communicating with airline check-in staff. These officers act as liaison officers with local law enforcement agencies as well as with airline employees;
3. CBSA checking passenger lists (usually when a flight bound for Canada is in the air) against CBSA's database at its Risk Assessment Centre in Ottawa. This step allows CBSA to verify if there is a “look-out” (a mention in CBSA computers) or any other relevant information about a particular individual;
4. CBSA checks at transit areas in Canadian airports;
5. CBSA inspections at Canadian airports; and
6. The Inland Enforcement Program for cases where a potentially inadmissible person has managed to enter Canada.³⁸¹

This layered approach also largely applies to cargo traffic.³⁸²

There are many ways to inspect cargo and individuals seeking to enter Canada. Still, the sheer volume of individuals and vehicles entering Canada is a key operational challenge for CBSA. As Vinette testified, “...you couldn't inspect every shipment; the border would shut down essentially.”³⁸³ As a result, the CBSA must be efficient and creative in minimizing the risks of contraband and ill-intentioned individuals entering Canada.

3.5.2.3 Business Line 1: Cross-border Movements of Currency and Monetary Instruments

Part 2 of the *PCMLTFA*, Reporting of Currency and Monetary Instruments, deals with two components of CBSA's work on cross-border activities – administrative rules governing the process for making declarations when entering Canada, and search and seizure powers.³⁸⁴

It is not illegal for an individual entering or leaving Canada to carry money in cash or other instruments, but this must be reported in certain cases. At or above a certain amount (currently \$10,000) persons³⁸⁵ must declare the import

³⁸¹ For a description of the concept, see Testimony of David Quartermain, vol. 56, October 2, 2007, pp. 7057-7060.

³⁸² Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7060-7061.

³⁸³ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7075.

³⁸⁴ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7044.

³⁸⁵ The persons are defined in s. 12(3) of the *PCMLTFA* and include mainly exporters and people transporting money.

or export to an officer,³⁸⁶ usually a BSO.³⁸⁷ Designated persons must complete reports on both the import and export of currency, including import or export by mail, courier or any means of transportation.³⁸⁸ CBSA also watches for cross-border movements of gold and precious metals and stones.³⁸⁹

Vinette stated that some individuals may understandably be reluctant to report – for example, if they are not familiar with Canada’s border control system or come from a country where there is distrust of the authorities.³⁹⁰ All reports about movements of funds – legitimate or improper – are forwarded to FINTRAC as Cross-Border Currency Reports (CBCRs).³⁹¹ FINTRAC then adds the information to its database.

After a report is made, the person entering or leaving Canada must answer any questions posed by the BSO and must present the currency or monetary instruments if the BSO requests.³⁹²

If a BSO suspects on reasonable grounds that an individual is hiding on or about themselves currency or monetary instruments worth \$10,000 or more which has not been reported,³⁹³ the BSO may search a person within a reasonable time after the person arrives in Canada. A BSO may on the same grounds search a person about to leave Canada at any time before the person’s departure. BSOs also have the power to stop, board and search any means of transportation to determine if currency or monetary instruments of \$10,000 or more are on board and have not been reported.³⁹⁴ Similar powers exist to search baggage and mail.³⁹⁵ Documents on concealment methods are circulated regularly, and officers also have access to a database of information and analysis.³⁹⁶

³⁸⁶ The *PCMLTFA*, at s. 2, defines the term “officer” to have the same meaning as in subsection 2(1) of the *Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.) [*Customs Act*]. The *Customs Act* defines “officer” as “a person employed in the administration or enforcement of this Act, the *Customs Tariff* or the *Special Import Measures Act* and includes any member of the Royal Canadian Mounted Police.”

³⁸⁷ “Monetary instruments” is defined to include stocks, bonds, debentures, treasury bills, bank drafts, cheques, promissory notes, travellers’ cheques and money orders, other than warehouse receipts or bills of lading: *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 1(1). It appears that in around 90% of cases, currency is seized. See 2008 FATF Mutual Evaluation of Canada, para. 603. The Bank of Canada and several financial entities are exempt from reporting: *Cross-border Currency and Monetary Instruments Reporting Regulations*, ss. 15, 15.1; *PCMLTFA*, s. 12(1); *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 2(1). Section 2 of the *Regulations* provides that the amount is in Canadian currency or its equivalent and explains how to calculate it. Several exceptions to the reporting rules are specified.

³⁸⁸ *PCMLTFA*, s. 12(3).

³⁸⁹ Under the general provisions of s. 110 of the *Customs Act* and s. 489(2) of the *Criminal Code*. See 2008 FATF Mutual Evaluation of Canada, para. 583.

³⁹⁰ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7039.

³⁹¹ *PCMLTFA*, s. 12(5).

³⁹² *PCMLTFA*, s. 12(4).

³⁹³ *PCMLTFA*, s. 15; *Cross-border Currency and Monetary Instruments Reporting Regulations*, s. 2(1).

³⁹⁴ *PCMLTFA*, s. 16(1).

³⁹⁵ *PCMLTFA*, ss. 16(2), 17; Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7041. Officers do not have the authority to open mail that weighs 30 grams or less unless either the addressee or the sender agrees or is present: see *PCMLTFA*, ss. 17(2), 17(3). For other provisions specific to mail, see s. 21 of the *PCMLTFA*.

³⁹⁶ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7065.

Air passengers arriving from foreign countries must complete a Declaration Card.³⁹⁷ For outbound flights, CBSA relies on intelligence and random searches on targeted flights where individuals are asked whether they are transporting currency or monetary instruments worth \$10,000 or more.³⁹⁸ Similar controls are in place at other types of border points.

The CBSA allocates a large portion of its time and resources to incoming flights, mainly because couriers might use such flights to bring money into Canada for terrorist purposes. However, the CBSA plays a limited role with departing passengers, so currency or monetary instruments can easily escape detection on flights leaving Canada. Remedying this would require the CBSA to devote as many resources to departing passengers as it does to incoming passengers.

If a BSO has reasonable grounds to believe that reporting obligations were not followed, the currency or monetary instruments may be seized.³⁹⁹ Various “levels” of seizures are described in CBSA regulations, except for “Level 4” seizures (involving suspected proceeds of crime or TF funds, and the most serious of all seizures), which are described in the *PCMLTFA*. The seizure levels appear below:

³⁹⁷ Examples of declaration cards were entered into evidence: see Exhibit P-235, Tab 4: Declaration Card and Exhibit P-235, Tab 5: Family Declaration Card.

³⁹⁸ 2008 FATF Mutual Evaluation of Canada, para. 563.

³⁹⁹ *PCMLTFA*, s. 18(1). Various procedural obligations must be respected, as set out in ss. 18(2)-(4) of the *PCMLTFA*. The Minister of Public Works and Government Services receives the seized currency or monetary instruments: see *PCMLTFA*, s. 22(2).

Level	Circumstances	Prescribed Penalty	Reference
1	In the case of a person or entity who: <ul style="list-style-type: none"> i. has not concealed the currency or monetary instruments, ii. has made a full disclosure of the facts concerning the currency or monetary instruments on their discovery, and iii. has no previous seizures under the Act [PCMLTFA]; 	\$250	Regulations, section 18 (a)
2	In the case of a person or entity who: <ul style="list-style-type: none"> i. has concealed the currency or monetary instruments, other than by means of using a false compartment in a conveyance, or who has made a false statement with respect to the currency or monetary instruments, or ii. has a previous seizure under the Act, other than in respect of any type of concealment or for making false statements with respect to the currency or monetary instruments; 	\$2500	Regulations, section 18 (b)
3	In the case of a person or entity who: <ul style="list-style-type: none"> i. has concealed the currency or monetary instruments by using a false compartment in a conveyance, or ii. has a previous seizure under the Act for any type of concealment or for making a false statement with respect to the currency or monetary instruments; 	\$5000	Regulations, section 18 (c)
4	In the case of the officer having reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime within the meaning of subsection 462.3(1) of the <i>Criminal Code</i> or funds for use in the financing of terrorist activities.	No specific amount prescribed	PCMLTFA, section 18(2)
"Regulations" refers to the <i>Cross-border Currency and Monetary Instruments Reporting Regulations</i> , SOR/2002-412.			

When currency or monetary instruments are seized, the officer who made the seizure must without delay (using a Cross-Border Seizure Report (CBSR)) report the seizure to FINTRAC. The officer must also notify the President of the CBSA.⁴⁰⁰ If a foreign national or non-Canadian citizen is suspected of involvement in TF, the file is forwarded to CBSA's Organized Crime Section.⁴⁰¹ After the information is analyzed, the CBSA can request help from law enforcement agencies, CSIS and FINTRAC.⁴⁰²

After seizing currency or monetary instruments, the BSO refers to the information available to him or her to determine if the items are proceeds of crime or connected to money laundering or TF. With Level 4 seizures, this determination has already been made before the seizure, since Level 4 seizures occur only if an officer has reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime or funds for use in TF. No subsequent determination is therefore necessary.⁴⁰³

The 2008 FATF Mutual Evaluation of Canada reported that, between January 2003 and September 2006, CBSA filed 174,938 CBCRs and 5,322 CBSRs with FINTRAC.⁴⁰⁴ About 18 per cent of FINTRAC's disclosures to recipients contained information from a CBCR or CBSR.⁴⁰⁵

Numerous methods are used to smuggle money or goods into Canada.⁴⁰⁶ Several were explained to the Commission during the hearings. CBSA's Strategic Intelligence Analysis Division circulates information to help BSOs and other CSBA employees stay current on new concealment methods.⁴⁰⁷ Annual seizures are split about evenly between those at land border crossings and those at airports.⁴⁰⁸

Because of the potential seriousness of a Level 4 seizure, BSOs work with CBSA intelligence officers whenever such a seizure occurs.⁴⁰⁹ David Quartermain, Director of the Borders Intelligence Division of CBSA's Intelligence Directorate, testified that intelligence officers transfer this information and their analysis to an Integrated Proceeds of Crime Unit (IPOC) within the RCMP. The IPOC may in turn transfer the file to an Integrated National Security Enforcement Team (INSET) or elsewhere in the RCMP if there are suspicions of TF.⁴¹⁰ In all cases

400 *PCMLTFA*, s. 20.

401 2008 FATF Mutual Evaluation of Canada, para. 581.

402 2008 FATF Mutual Evaluation of Canada, para. 581.

403 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7045.

404 2008 FATF Mutual Evaluation of Canada, para. 596.

405 2008 FATF Mutual Evaluation of Canada, para. 597.

406 Exhibit P-235, Tab 8: CBSA Currency Concealment Presentation. See also Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7054-7055.

407 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7040.

408 Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7054-7055.

409 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7045; Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7048.

410 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7051.

involving a suspicion of money laundering or TF, the information is shared with law enforcement and intelligence agencies, including FINTRAC.⁴¹¹

Quartermain stated that amendments introduced by Bill C-25 helped address "...some of the information-sharing issues that [CBSA] had identified as gaps" with FINTRAC and other partners:

[I]n the past, the information flow was more from CBSA into FINTRAC, and now...we can obtain information back from FINTRAC if it is relevant to investigating or prosecuting a money laundering offence or terrorist activity, as it relates to smuggling goods or subject to duties or evading taxes.

Another issue was the exchange of information with foreign states. In the past, we couldn't do that. Now, amendments allow [sharing] information or disclosing seizure information that has been collected under Part II of the *PCMLTFA* with foreign agencies which have regimes similar to a centre such as FINTRAC. So I will use the example of the U.S. We're in the midst of negotiating with the various agencies in the United States ...which will allow us then to share [information with U.S. organizations] with respect to seizures.⁴¹²

Vinette testified that, between January 2003 and September 2007, CBSA had made about 900 seizures at border crossings involving suspected proceeds of crime, including TF. A total of roughly \$48 million was involved.⁴¹³ However, CBSA had no breakdown to show how much of that total involved suspected TF.

Quartermain testified that the CBSA does not receive feedback in all cases where it shares information about suspected TF funds with its partners, and he was uncertain if there was a way to find out what percentage of those funds could be related to TF. There was no legislated requirement for feedback.⁴¹⁴

CBSA provided the following Selected Commodities Seizure Report⁴¹⁵ to the Commission.

411 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7055. See also *PCMLTFA*, s. 36(2) which states: "An officer who has reasonable grounds to suspect that information referred to in subsection (1) would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence may disclose the information to the appropriate police force."

412 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7069.

413 Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7050.

414 Testimony of David Quartermain, vol. 56, October 2, 2007, pp. 7053-7056.

415 Exhibit P-235, Tab 10: CBSA Selected Commodities Seizure Report, January 1, 2003 to September 26, 2007.

Selected Commodities Seizure Report January 1, 2003 to September 28, 2007			
Commodity Group	Commodity Type	SeizureCount	Value
Currency or Monetary	Banker's Drafts	123	4,364,592.31
Currency or Monetary	Bonds	13	322,198.00
Currency or Monetary	Cheques	255	8,498,549.16
Currency or Monetary	Currency	6994	126,519,187.00
Currency or Monetary	Money Orders	73	1,170,021.79
Currency or Monetary	Oth. Instrmts. in Bearer Form	6	89,902.40
Currency or Monetary	Stocks	5	693,385.70
Currency or Monetary	Traveller's Cheques	382	5,196,208.00
Currency or Monetary	Treasury Bills	4	68,337.40
Suspected Proceeds of Crime	Banker's Drafts	4	96,280.00
Suspected Proceeds of Crime	Cheques	17	707,698.37
Suspected Proceeds of Crime	Currency	805	45,296,646.97
Suspected Proceeds of Crime	Money Orders	17	455,767.15
Suspected Proceeds of Crime	Oth. Instrmts. in Bearer Form	1	13,600.00
Suspected Proceeds of Crime	Recovery Entry	1	0.00
Suspected Proceeds of Crime	Traveller's Cheques	14	270,420.00
Totals		8,714	193,762,694.25

The *PCMLTFA* provides a review and appeal procedure for seizures by CBSA and also specifies the penalties for failing to report currency imports or exports as required by section 12(1).⁴¹⁶ The *PCMLTFA Act* permits a person from whom currency or monetary instruments have been seized, or the lawful owner, to ask the Minister of Public Safety to review the seizure.⁴¹⁷ Vinette confirmed that seven attempts, all unsuccessful, had been made to challenge Level 4 seizures in court.⁴¹⁸ At the time of the 2008 FATF Mutual Evaluation of Canada, 45 cases challenging Level 4 seizures were before the courts.⁴¹⁹ It is not known how many of these, if any, were related to TF.

⁴¹⁶ *PCMLTFA*, ss. 24-31. The *PCMLTFA* also sets out a procedure for third party claims: see ss. 32-35.

⁴¹⁷ *PCMLTFA*, s. 25.

⁴¹⁸ Testimony of Denis Vinette, vol. 56, October 2, 2007, p. 7049.

⁴¹⁹ 2008 FATF Mutual Evaluation of Canada, para. 601.

Information that CBSA gathers can be used in other ways.⁴²⁰ In addition to the information provided through CBCRs and CBSRs, a BSO may provide information to FINTRAC if the BSO has reasonable grounds to suspect that it would be of assistance to FINTRAC in the detection, prevention or deterrence of money laundering or the financing of terrorist activities – a sort of “catch-all” provision.⁴²¹

In turn, FINTRAC must disclose information to CBSA when FINTRAC concludes that any of the following conditions are met:

- (i) the information is relevant to an offence of evading or attempting to evade paying taxes or duties imposed under an Act of Parliament administered by the CBSA;⁴²²
- (ii) the information is relevant to determining whether a person is a person described in sections 34 to 42 of the *Immigration and Refugee Protection Act* or is relevant to an offence under any of sections 117 to 119, 126 or 127 of the Act;⁴²³ or
- (iii) the information is relevant to investigating or prosecuting an offence of smuggling or attempting to smuggle goods subject to duties or an offence related to the importation of goods that are prohibited, controlled or regulated under the *Customs Act* or under any other Act of Parliament.⁴²⁴

The 2008 FATF Mutual Evaluation of Canada gave Canada a “Compliant” rating for its cross-border procedures. The FATF noted as well that the monetary threshold (\$10,000 – explained below) triggering the need to make a currency declaration was even lower than that recommended by the FATF, and that Canada has implemented the border control measures outlined in the FATF Best Practices Paper.⁴²⁵

3.5.2.4 Business Line 2: The Immigration and Refugee Protection Act Process and Other Activities Related to TF

Besides monitoring the cross-border movement of currency and monetary instruments, the CBSA has a role in immigration matters. One of CBSA’s goals is to prevent individuals who may have been involved in TF from entering the country.⁴²⁶

⁴²⁰ Information in this context is that referred to in s. 36(1) of the *PCMLTFA* and consists of: (a) information set out in a report made under section 12(1) of the *PCMLTFA*, (b) any other information obtained for the purposes of Part 2 of the *PCMLTFA*, and (c) information prepared from information referred to in paragraph (a) or (b).

⁴²¹ *PCMLTFA*, s. 36(3).

⁴²² *PCMLTFA*, s. 55(3)(b.1).

⁴²³ *PCMLTFA*, s. 55(3)(d).

⁴²⁴ *PCMLTFA*, s. 55(3)(e).

⁴²⁵ 2008 FATF Mutual Evaluation of Canada, para. 585.

⁴²⁶ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7053.

Section 37(1) of the *Immigration and Refugee Protection Act*⁴²⁷ sets out the activities which make a permanent resident or a foreign national inadmissible to Canada on grounds of “organized criminality.” Tyson George, a Senior Analyst with the Organized Crime Section of the National Security Division of the CBSA, testified that TF could be one such activity.⁴²⁸

If Citizenship and Immigration Canada visa officers overseas have reason to believe that a person may be inadmissible under section 37, they send that information to the Organized Crime Section. The Section analyzes the information and, if it believes that there is a possibility of TF being involved, it consults its partner agencies, including FINTRAC. It may also submit a VIR to FINTRAC. FINTRAC in turn may disclose designated information to the Section. Based on any information it receives from FINTRAC and other agencies, and on its own analysis, the Section provides its opinion to the visa officers about whether the person is inadmissible.⁴²⁹

3.5.3 International Cooperation

The *PCMLTFA* allows the Minister of Public Safety, with the consent of the Minister of Finance, to enter into an agreement with a foreign state, or an institution or agency of that state, to allow for an exchange of information from reports about currency or monetary instruments between CBSA and a similar foreign counterpart.⁴³⁰ Information obtained by Canada under the agreement must also be sent to FINTRAC.⁴³¹

The 2008 FATF Mutual Evaluation of Canada described the exchanges of information allowed by a partnership agreement between Canada and the United States under the Shared Border Accord. The exchanges were to help both countries manage the flow of refugee claimants at their shared border (some of the information-sharing would also relate to TF):

- Advance Passenger Information and agreed-to Passenger Name Records on flights between Canada and the United States, including in-transit flights, in order to identify risks posed by passengers on international flights arriving in each other’s territory;
- Data related to customs fraud, and agreed-upon customs data pursuant to NAFTA, as well as any additional commercial and trade data, for national security purposes;
- Advance information on designated individuals and organizations for the purpose of freezing terrorist assets;
- Refugee and asylum claimants, in order to ensure that applicants are thoroughly screened for security risks;

⁴²⁷ S.C. 2001, c. 27.

⁴²⁸ Testimony of Tyson George, vol. 56, October 2, 2007, p. 7052.

⁴²⁹ Testimony of Tyson George, vol. 56, October 2, 2007, pp. 7052-7053.

⁴³⁰ *PCMLTFA*, s. 38(1).

⁴³¹ *PCMLTFA*, s. 38(3).

- Marine in-transit containers arriving in Canada and the United States; and
- Anti-terrorism efforts, through the Cross-Border Crime Forum and Project Northstar.⁴³²

As noted above, Quartermain told the Commission that negotiations were underway with various agencies in the United States to share information about seizures with US organizations.⁴³³

3.5.4 Funding

In 2006-07, the CBSA was allocated \$7.8 million under the AML/ATF Initiative and was allocated \$7.7 million for each of the subsequent three fiscal years.⁴³⁴

3.6 Department of Foreign Affairs and International Trade

The Department of Foreign Affairs and International Trade (DFAIT), through the Minister of Foreign Affairs, is responsible for matters relating to the conduct of the external affairs of Canada, including international trade and commerce and international development, where those matters have not been assigned to another federal department, board or agency.⁴³⁵ The *Department of Foreign Affairs and International Trade Act* requires the Minister to perform the following duties, among others:

- conduct all official communication between the Government of Canada and the government of any other country and between the Government of Canada and any international organization;
- conduct and manage international negotiations as they relate to Canada;
- coordinate the direction given by the Government of Canada to the heads of Canada's diplomatic and consular missions; and
- foster the development of international law and its application in Canada's external relations.⁴³⁶

Several sections of DFAIT play a role in TF matters. The Commission heard evidence from Keith Morrill, Director of the Criminal, Security and Treaty Law

⁴³² 2008 FATF Mutual Evaluation of Canada, para. 577.

⁴³³ Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7069.

⁴³⁴ Department of Finance Presentation, slide 1.

⁴³⁵ *Department of Foreign Affairs and International Trade Act*, R.S.C. 1985, c. E-22, s. 10(1) [*Department of Foreign Affairs and International Trade Act*].

⁴³⁶ *Department of Foreign Affairs and International Trade Act*, s. 10(2).

Division, part of the Legal Bureau at DFAIT.⁴³⁷ The Division helps address legal issues at the international and domestic levels. The Division has two goals:

- (i) to ensure that Canadian views are put forward at the international level and that its objectives are integrated at that level, as well as being consistent with Canadian domestic policy; and
- (ii) to ensure that Canadian foreign policy and the appropriate domestic legislation is in line with Canadian contributions at the international level in regard to terrorism, TF and other related issues.⁴³⁸

Two other groups within DFAIT also deal with these issues: the International Crime and Terrorism Division and the Economic Crime Section of the International Humanitarian and Human Rights Law Section.⁴³⁹

DFAIT coordinates Canada's international TF activities and "develops and advocates Canadian positions" by representing Canada at the United Nations, G8 (in particular through the Roma/Lyon Anti-Crime and Terrorism Experts Group), Asia-Pacific Economic Cooperation, Organization of American States, and Organization for Security and Co-operation in Europe, among other organizations.⁴⁴⁰ DFAIT supports its Minister in the fulfillment of the Minister's responsibilities for the terrorist listing mechanisms implemented under Canada's *United Nations Act*, through the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR) and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST).⁴⁴¹ Finally, DFAIT co-chairs the Interdepartmental Working Group on Terrorist Listings with Public Safety Canada in support of the Minister's legal responsibility to recommend entities to be listed under the RIUNRST. DFAIT also ensures that Canadian foreign policy and international programming complies with Canada's international obligations and domestic regulations to counter TF.⁴⁴²

3.7 Public Safety Canada

Public Safety Canada (PS) is responsible for providing support and policy advice to the Minister of Public Safety on all matters of public safety and national security, including money laundering and TF.⁴⁴³ The Public Safety website describes its areas of activity as emergency management, national security, law

⁴³⁷ Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6677.

⁴³⁸ Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6678; Department of Finance Memorandum of Evidence on Terrorist Financing, pp. 39-40.

⁴³⁹ Testimony of Keith Morrill, vol. 54, September 28, 2007, p. 6679.

⁴⁴⁰ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.

⁴⁴¹ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.

⁴⁴² Department of Finance Memorandum of Evidence on Terrorist Financing, pp. 39-40.

⁴⁴³ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 40.

enforcement, corrections and crime prevention,⁴⁴⁴ and its mandate as being to "...keep Canadians safe from a range of risks such as natural disasters, crime and terrorism."⁴⁴⁵

Public Safety works with the agencies within its portfolio, such as the RCMP and CSIS, other levels of government, first responders, community groups, the private sector and foreign countries.⁴⁴⁶ Departmental staff members advise the Minister of Public Safety on enforcement and intelligence matters, including those related to money laundering and TF. The Department coordinates policy advice received from its portfolio agencies, as well as the input of these agencies in government-wide exercises, such as the 2008 FATF Mutual Evaluation of Canada.⁴⁴⁷

Two important administrative processes involve the Minister of Public Safety directly in TF matters – the *Criminal Code* listing of terrorist groups and the process under the *Charities Registration (Security Information) Act* (CRSIA):

- The *Criminal Code* authorizes the Minister of Public Safety to recommend to the Governor in Council the listing of terrorist entities under the Code.⁴⁴⁸ Public Safety maintains a current *Criminal Code* listing on its website.⁴⁴⁹ Along with DFAIT, PS co-chairs the Interdepartmental Working Group on Terrorist Listings; and
- The Minister, with the Minister of National Revenue, is responsible under the CRSIA for preventing the use of charitable organizations for TF purposes.⁴⁵⁰ Both CSIS and the RCMP make recommendations to the Minister of Public Safety in this regard.⁴⁵¹ This process and the Minister's role are described in Chapter VI.

3.8 Office of the Superintendent of Financial Institutions

The Office of the Superintendent of Financial Institutions (OSFI) was established by the *Office of the Superintendent of Financial Institutions Act* (*OSFI Act*).⁴⁵² The Minister of Finance presides over and is responsible for OSFI.⁴⁵³ OSFI has a

⁴⁴⁴ Public Safety Canada, "What we do," online: Public Safety Canada <<http://www.ps-sp.gc.ca/abt/wwwd/index-eng.aspx>> (accessed April 22, 2009) [Public Safety Canada, "What we do"].

⁴⁴⁵ Public Safety Canada, "What we do."

⁴⁴⁶ Public Safety Canada, "What we do."

⁴⁴⁷ Exhibit P-383, Tab 11: Public Safety Canada's Submission to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, October 24, 2007, p. 1 [Public Safety Submission to the Commission].

⁴⁴⁸ *Criminal Code*, s. 83.05.

⁴⁴⁹ See Public Safety Canada, "Currently listed entities," online: Public Safety Canada <<http://www.publicsafety.gc.ca/prg/ns/le/cle-en.asp>> (accessed April 22, 2009).

⁴⁵⁰ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 40.

⁴⁵¹ Public Safety Submission to the Commission, p. 1; *A New Review Mechanism for the RCMP's National Security Activities*, p. 190.

⁴⁵² R.S.C. 1985, c. 18 (3rd Supp.), Part I.

⁴⁵³ *OSFI Act*, ss. 3, 4(1).

broad supervisory authority over financial institutions coming under federal jurisdiction and responsibility for providing guidance to these institutions. OSFI's powers are derived from several statutes besides the *OSFI Act*. These include the *Bank Act*,⁴⁵⁴ *Insurance Companies Act*,⁴⁵⁵ *Trust and Loan Companies Act*,⁴⁵⁶ *Pension Benefits Standards Act, 1985*⁴⁵⁷ and *Cooperative Credit Associations Act*.⁴⁵⁸ The financial institutions regulated by OSFI include the following:

- (i) banks;
- (ii) foreign bank branches in Canada;
- (iii) federally regulated trust and loan companies;
- (iv) federally regulated cooperative credit associations;
- (v) federally regulated property and casualty insurance companies; and
- (vi) fraternal benefit societies.⁴⁵⁹

OSFI's objects relating to financial institutions are as follows:

- (i) to supervise financial institutions in order to determine whether they are in sound financial condition and are complying with their governing statute and supervisory requirements;
- (ii) to promptly advise the management and board of directors of a financial institution if the institution is not in sound financial condition or is not complying with its governing statute or supervisory requirements and, in such a case, to take, or require the management or board to take, the necessary corrective measures or series of measures to deal with the situation in an expeditious manner;
- (iii) to promote the adoption by management and boards of directors of financial institutions of policies and procedures designed to control and manage risk; and
- (iv) to monitor and evaluate system-wide or sectoral events that may have a negative impact on the financial condition of financial institutions.⁴⁶⁰

454 S.C. 1991, c. 46.

455 S.C. 1991, c. 47.

456 S.C. 1991, c. 45.

457 R.S.C. 1985, c. 32 (2nd Supp.).

458 S.C. 1991, c.48.

459 See the definition of "financial institution" in s. 3 of the *OSFI Act*, and Office of the Superintendent of Financial Institutions Canada, "Who We Regulate," online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=568> (accessed August 1, 2008).

460 *OSFI Act*, s. 4(2).

OSFI states that it contributes to public confidence in the financial system.⁴⁶¹ It does not have any specific legislated role in TF matters but conducts its TF work as part of its obligation to regulate and monitor the financial sector.⁴⁶²

OSFI disseminates information about terrorist entities listed under the *Criminal Code* or under the two lists adopted by Canada through the RIUNRST and UNAQTR. OSFI has consolidated these three lists into two – one covering entities and the other covering individuals – and posts them on its website.⁴⁶³ It distributes updated information to the institutions under its jurisdiction.⁴⁶⁴ OSFI also communicates changes to the lists to provincial regulators and supervisors and several associations, such as the Canadian Bankers Association, the Canadian Life and Health Insurance Association and the Canadian Securities Administrators.⁴⁶⁵ OSFI provides monthly reminders to institutions under its jurisdiction that they must report any transaction related to an entity or individual named on the lists.

Financial institutions must report to OSFI whether they are in possession or control of property owned or controlled by or on behalf of a listed entity.⁴⁶⁶ “Reporting entities” must also report to FINTRAC,⁴⁶⁷ CSIS and the RCMP⁴⁶⁸ if property in their possession belongs to a listed entity or person. OSFI issues a monthly written reminder that financial institutions are required to file a report showing, in aggregate, the number of accounts and the dollar value of terrorist property frozen and reported to law enforcement.⁴⁶⁹

Unlike the case with other FINTRAC partners such as the RCMP, CSIS, CBSA and the CRA, there is no provision in the *PCMLTFA* permitting or requiring FINTRAC to disclose designated information to OSFI. Under a Memorandum of Understanding between OSFI and FINTRAC, OSFI sends FINTRAC copies of all OSFI’s dealings with the entities obliged to report to OSFI. Furthermore, OSFI

461 Office of the Superintendent of Financial Institutions (OSFI), Plans and Priorities 2008-2011, p. 1, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/reports/osfi/PP_2008_2011_e.pdf> (accessed August 1, 2008) [OSFI 2008-11 Plans and Priorities].

462 Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.

463 “Terrorism Financing,” online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=525> (accessed August 1, 2008) [OSFI, “Terrorism Financing”].

464 For list of OSFI notices, see OSFI, “Terrorism Financing.”

465 See, for example, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/issues/terrorism/updates/2008_08_01_e.pdf> (accessed August 1, 2008).

466 All entities listed in s. 83.11(1) of the *Criminal Code* are required to report the information “to the principal agency or body that supervises or regulates it under federal or provincial law.” In the case of federal institutions, it is OSFI: *Criminal Code*, s. 83.11(2); RIUNRST, s. 7(2); *United Nations Al-Qaida and Taliban Regulations*, S.O.R./99-444, s. 5.1(2) [UNAQTR].

467 S. 7.1(1) of the *PCMLTFA*. A person or entity who is required to make a disclosure under s. 83.1 of the *Criminal Code*, or s. 8 of the RIUNRST, must file a report with FINTRAC if that person or entity is also subject to the *PCMLTFA* (as described in s. 5 of the *PCMLTFA*).

468 *Criminal Code*, s. 83.1(1), RIUNRST, s. 8(1), UNAQTR, s. 5.2(1).

469 2008 FATF Mutual Evaluation of Canada, para. 332.

meets regularly with senior FINTRAC officials to discuss findings, trends and emerging issues.⁴⁷⁰

Besides issuing reminders and notices and providing current listings, OSFI conducts educational programs for financial institutions. For example, OSFI holds annual information sessions for compliance and risk management senior officers to discuss money laundering and TF.⁴⁷¹ As of May 2008, OSFI was scheduled to begin consultations with the private sector on a revised AML/ATF guideline that would take into account OSFI's accumulated experience with money laundering compliance efforts since 2004, the changes brought by Bill C-25 and the 2008 FATF Mutual Evaluation of Canada.⁴⁷² Another OSFI priority, identified in its 2008-2012 Plans and Priorities, was to respond to the recommendations of the FATF Mutual Evaluation.⁴⁷³

3.9 Integrated Threat Assessment Centre

The Integrated Threat Assessment Centre (ITAC) was created in 2004. Following the release of the National Security Policy later that year, it replaced the former CSIS Integrated National Security Assessment Centre.⁴⁷⁴

ITAC's role is to produce comprehensive and integrated assessments of threats to Canada's national security and to distribute them within the intelligence community and to first-line responders.⁴⁷⁵ ITAC focuses primarily on terrorist trends and on domestic and international events related to terrorism. ITAC threat assessments may be classified or unclassified.⁴⁷⁶

ITAC's director is appointed by the National Security Advisor (NSA) in consultation with the Director of CSIS. ITAC's Assessment Management Committee (composed of assistant deputy ministers from ITAC partners) advises the Management Board on the focus, effectiveness and efficiency of ITAC's activities.⁴⁷⁷ ITAC is staffed by representatives of several organizations, normally for two-year terms: CBSA, CSIS, Correctional Service of Canada, CSE, DND, DFAIT, FINTRAC, the Ontario

⁴⁷⁰ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.

⁴⁷¹ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 42.

⁴⁷² Remarks by Superintendent Julie Dickson, Office of the Superintendent of Financial Institutions Canada (OSFI), to the OSFI AML/ATF Conference, Toronto May 7, 2008, p. 3, online: Office of the Superintendent of Financial Institutions Canada <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/speeches/JDickson_OSFI_AML_ATF_e.pdf> (accessed August 1, 2008).

⁴⁷³ OSFI 2008-11 Plans and Priorities, p. 9.

⁴⁷⁴ Canadian Security Intelligence Service, "Backgrounder No. 13 - The Integrated Threat Assessment Centre (ITAC)," p. 1, online: Canadian Security Intelligence Service <<http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr13-eng.pdf>> (accessed August 6, 2008) [CSIS Backgrounder on ITAC]; *A New Review Mechanism for the RCMP's National Security Activities*, p. 141. For further information about the structure, mission and activities of ITAC, see the testimony of Daniel Giasson, Director, Integrated Threat Assessment Centre, Canadian Security Intelligence Service, Proceedings of the Standing Senate Committee on National Security and Defence, Issue 16 - Evidence, May 28, 2007, online: Parliament of Canada <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/Com-e/defe-e/16ev-e.htm?Language=E&Parl=39&Ses=1&comm_id=76> (accessed December 3, 2007).

⁴⁷⁵ CSIS Backgrounder on ITAC, p. 2.

⁴⁷⁶ *A New Review Mechanism for the RCMP's National Security Activities*, p. 141.

⁴⁷⁷ CSIS Backgrounder on ITAC, p. 2.

Provincial Police, PS, Privy Council Office, the RCMP, the *Sûreté du Québec* and Transport Canada.⁴⁷⁸ Individuals who are seconded to ITAC bring with them knowledge acquired at their home agencies.⁴⁷⁹

Besides providing threat assessments, ITAC has published studies either specifically about TF⁴⁸⁰ or about both terrorism and TF.⁴⁸¹ For example, in 2006 it published *Terrorist Financing - How It's Done and How It's Countered*.⁴⁸²

At the international level, ITAC carries out its functions mainly as part of the Five Eyes Terrorist Financing Working Group – a group with representatives from Canada, the UK, the US, Australia and New Zealand. Part of the work of the Five Eyes Working Group is to exchange threat assessments among members of the Group – the Joint Terrorism Analysis Centre in Britain, the National Counterterrorism Center in the United States, the National Threat Assessment Centre in Australia, the Combined Threat Assessment Group in New Zealand, and ITAC.⁴⁸³ Threat assessments produced by ITAC are shared with international partners unless designated “for Canadian eyes only.” ITAC also shares information with other foreign partners on a case-by-case basis.⁴⁸⁴

3.10 Other Departments and Agencies

Other federal departments and agencies have smaller roles in the fight against terrorism and TF, notably the Department of Justice, the Communications Security Establishment and the Privy Council Office.

3.10.1 Department of Justice

The Department of Justice is headed by a single Minister who serves as both Minister of Justice and Attorney General of Canada. The Minister is responsible for the development of law and procedure in regard to criminal law. The Minister is also responsible for the *Mutual Legal Assistance in Criminal Matters*

⁴⁷⁸ Testimony of John Schmidt, vol. 53, September 27, 2007, pp. 6642-6643; CSIS Backgrounder on ITAC, p. 2. ITAC can also draw information and expertise as needed from Agriculture Canada, Health Canada, Environment Canada and Natural Resources Canada. FINTRAC became a partner only in April 2006: see Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6644.

⁴⁷⁹ CSIS Backgrounder on ITAC, p. 2; Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6645.

⁴⁸⁰ Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, “Terrorism Financing and Financial System Vulnerabilities: Issues and Challenges” (ITAC Presents, Trends in Terrorism Series, Volume 2006-3), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-3-eng.pdf> (accessed December 3, 2007).

⁴⁸¹ Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, “A Framework for Understanding Terrorist Use of the Internet” (ITAC Presents, Trends in Terrorism Series, Volume 2006-2), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-2-eng.pdf>; Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, “Actual and Potential Links Between Terrorism and Criminality” (ITAC Trends in Terrorism Series, Volume 2006-5), online: Integrated Threat Assessment Centre <http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-5-eng.pdf> (accessed December 3, 2007).

⁴⁸² Other similar classified studies were examined by Commission counsel.

⁴⁸³ CSIS Backgrounder on ITAC, p. 3.

⁴⁸⁴ *A New Review Mechanism for the RCMP's National Security Activities*, p. 142.

Act.⁴⁸⁵ The 2008 FATF Mutual Evaluation of Canada criticized Canada's mutual legal assistance program, saying that "...[t]here are concerns about the ability of Canada to handle [mutual legal assistance] requests in a timely and effective manner and effectiveness of the current regime cannot be demonstrated due to the lack of adequate data."⁴⁸⁶

The *PCMLTFA* allows the Attorney General to apply for a production order for an investigation of a TF offence.⁴⁸⁷ The Attorney General, by way of the Director of Public Prosecutions and the Public Prosecution Service of Canada, has concurrent jurisdiction with provincial Attorneys General for TF prosecutions.⁴⁸⁸

3.10.2 Communications Security Establishment Canada

The Communications Security Establishment Canada (CSE) is Canada's cryptologic agency.⁴⁸⁹ Its mandate has three components:

- a. to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- b. to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
- c. to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.⁴⁹⁰

CSE can be involved in TF work in several ways:

- by providing technical and operational assistance to the RCMP or CSIS (mandate "c" above);⁴⁹¹
- by receiving information through its own activities (mandate "a") and forwarding it to the relevant agency, including FINTRAC; and
- by being the recipient of disclosures of designated information by FINTRAC. FINTRAC must disclose designated information to CSE if FINTRAC has reasonable grounds to suspect that the information

⁴⁸⁵ R.S.C. 1985, c. 30 (4th Supp.).

⁴⁸⁶ 2008 FATF Mutual Evaluation of Canada, p. 298.

⁴⁸⁷ *PCMLTFA*, s. 60(2).

⁴⁸⁸ Department of Finance Memorandum of Evidence on Terrorist Financing, p. 39.

⁴⁸⁹ Communications Security Establishment Canada, "Welcome to the Communications Security Establishment Canada," online: Communications Security Establishment Canada <<http://www.cse-cst.gc.ca/index-eng.html>> (accessed September 16, 2009).

⁴⁹⁰ *National Defence Act*, R.S.C. 1985, c. N-5, s. 273.64(1).

⁴⁹¹ Testimony of Jim Galt, vol. 55, October 1, 2007, pp. 6930-6931.

would be relevant to investigating or prosecuting a money laundering or TF offence and if FINTRAC also determines that the information is relevant to the mandate of CSE.⁴⁹²

3.10.3 Privy Council Office

The Privy Council Office (PCO) reports directly to the Prime Minister and is headed by the Clerk of the Privy Council and Secretary to the Cabinet. The PCO acts as the Cabinet secretariat and as the Prime Minister's main source of public service advice for the policy questions and operational issues of concern to the government of the day. The Clerk of the Privy Council is Canada's most senior public servant supporting the Prime Minister and has three main responsibilities: serving as the Prime Minister's Deputy Minister, Secretary to the Cabinet and Head of the Public Service.⁴⁹³

The National Security Advisor to the Prime Minister and Associate Secretary to the Cabinet assists the Clerk and provides information, advice and recommendations to the Prime Minister as follows:

- as Associate Secretary to the Cabinet, by acting on the Clerk's behalf on any of the policy and operational issues that come before the PCO; and
- as National Security Advisor to the Prime Minister, by ensuring the effective coordination of Canada's security and intelligence community and, together with the Deputy Minister of National Defence, by being responsible for CSE. The National Security Advisor also oversees the provision of intelligence assessments to the Prime Minister, other ministers and senior government officials.

3.11 Cooperation among Agencies

As this chapter has explained, several federal agencies are involved in implementing Canada's anti-TF program. Cooperation is not limited to formal interdepartmental committees. Some agencies work with each other one-on-one. RCMP Superintendent Reynolds testified, for example, that the RCMP works in this manner on a regular basis with CSIS, CRA and FINTRAC.⁴⁹⁴

⁴⁹² *PCMLTFA*, s. 55(3)(f).

⁴⁹³ Privy Council Office, "The Role and Structure of the Privy Council Office," November 2008, p. 1, online: Privy Council Office <<http://www.pco-bcp.gc.ca/docs/information/Publications/Role/docs/2008/role2008-eng.pdf>> (accessed September 16, 2009) [PCO, "The Role and Structure of the Privy Council Office"].

⁴⁹⁴ Testimony of Rick Reynolds, vol. 55, October 1, 2007, p. 6841.

Several formal cooperation mechanisms are discussed below.

3.11.1 Financial Crimes Interdepartmental Coordinating Committee (ICC)

The head of the Financial Crimes Section (Domestic/International) of Finance Canada chairs this working-level committee, which meets at least quarterly to "...address operational and administrative issues related to Canada's Anti-Money Laundering and Anti-Terrorist Financing regime and to coordinate policy in this area."⁴⁹⁵ Meetings may occur more often when Parliament is revising legislation and regulations. Diane Lafleur of Finance Canada testified that the committee can deal with both policy and operational issues related to the AML/ATF Initiative.⁴⁹⁶

The ICC's tasks include the following:

- to provide a forum for government working-level stakeholders to assess the operational efficiency and effectiveness of the AML/ATF Initiative, and identify problems/solutions;
- to coordinate and manage all parliamentary, Treasury Board-mandated and Auditor General reviews and audits related to the AML/ATF Initiative; and
- to provide input and advise on Government policy relating to Canada's AML/ATF Initiative.⁴⁹⁷

The ICC's participants are the Departments of Finance, Justice, Public Safety and DFAIT and the following agencies: CRA, FINTRAC, RCMP, CBSA, CSIS and OSFI.⁴⁹⁸

The Committee coordinated the 2008 FATF Mutual Evaluation of Canada and met several times for that purpose.

3.11.2 Financial Crimes Interdepartmental Steering Committee (ADM Steering Committee)

The Assistant Deputy Minister of the Financial Sector Policy Branch of Finance Canada chairs this committee, often referred to as the ADM Steering Committee. It meets twice a year, or as necessary, and provides strategies and general guidance for Canada's AML/ATF Initiative. The terms of reference of the committee describe its functions as follows:

⁴⁹⁵ Exhibit P-227, Tab 4: Financial Crimes Interdepartmental Committees (Coordinating & Steering) Terms of Reference, p. 1 [Financial Crimes Interdepartmental Committees Terms of Reference].

⁴⁹⁶ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6782.

⁴⁹⁷ Financial Crimes Interdepartmental Committees Terms of Reference, p. 2.

⁴⁹⁸ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6782; Financial Crimes Interdepartmental Committees Terms of Reference, p. 1. DFAIT participates only when international AML/ATF matters are involved.

- to provide a forum for ADM-level government stakeholders to assess the overall effectiveness of the AML/ATF Initiative;
- to provide guidance on the Government's AML/ATF communications strategy;
- to provide input and advice on Government policy relating to Canada's AML/ATF Initiative; and
- to oversee the work of a related working-level group, including providing feedback on issues of strategic importance that arise in the group.⁴⁹⁹

The participants are officials at the assistant deputy minister level from the same departments and agencies that belong to the ICC except that DFAIT does not participate in the ADM Steering Committee.

3.11.3 Interdepartmental Coordinating Committee on Terrorist Listings

The Interdepartmental Coordinating Committee on Terrorist Listings is co-chaired by officials from Public Safety and DFAIT. It coordinates the activities of all departments and agencies involved in the listing processes – not only the *Criminal Code* listing process but also the processes flowing from the RIUNRST and the UNAQTR. The committee consists of PS and DFAIT as co-chairs, RCMP and CSIS as intelligence providers, and the Privy Council Office, Department of Finance, CBSA, Department of Justice, CRA and OSFI.⁵⁰⁰ CSIS and the RCMP are the lead agencies responsible for preparing recommendations to list an entity and for collecting intelligence in support of the recommendation.

3.11.4 Integrated National Security Enforcement Teams (INSETs)

The RCMP describes the purpose of the INSETs as being to increase the capacity for the collection, sharing and analysis of intelligence among partners with respect to individuals and entities that are a threat to national security, create an enhanced investigative capacity to bring such individuals and entities to justice, and enhance partner agencies' collective ability to combat national security threats.⁵⁰¹ National Security Investigation Sections⁵⁰² (NSISs) and INSETs operate at the divisional level of the RCMP and have the primary responsibility for carrying out criminal investigations in national security matters.⁵⁰³

INSETs deal with TF issues as well as with terrorist investigations. They also provide a forum for the exchange of information among the agencies that may be involved alongside the RCMP – for example, CSIS, CBSA, Citizenship and

⁴⁹⁹ Financial Crimes Interdepartmental Committees Terms of Reference, pp. 3-4.

⁵⁰⁰ Public Safety Submission to the Commission, p. 2.

⁵⁰¹ Royal Canadian Mounted Police, "Integrated National Security Enforcement Teams," online: Royal Canadian Mounted Police <<http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm>> (accessed August 28, 2008) [RCMP, "Integrated National Security Enforcement Teams"].

⁵⁰² Since renamed "National Security Enforcement Sections."

⁵⁰³ *A New Review Mechanism for the RCMP's National Security Activities*, p. 102.

Immigration Canada, CRA, provincial and municipal police forces and other federal and provincial agencies.⁵⁰⁴ INSETs are located in Vancouver, Toronto, Ottawa and Montreal.⁵⁰⁵ Their activities are coordinated by RCMP National Headquarters. The RCMP is fully accountable for INSET operations and RCMP policies and rules apply to the work of INSET members.⁵⁰⁶

3.11.5 Integrated Border Enforcement Teams (IBETs)

In TF matters, Integrated Border Enforcement Teams (IBETs) coordinate the work of various agencies in monitoring the cross-border transportation of currency and other monetary instruments.⁵⁰⁷ The RCMP states that IBETs "...enhance border integrity and security along the shared Canada/US border, between designated ports of entry."⁵⁰⁸

IBETs consist of Canadian and American partners: the RCMP, the CBSA, the US Customs and Border Protection/Office of Border Patrol, the US Bureau of Immigration and Customs Enforcement, and the US Coast Guard.⁵⁰⁹ The RCMP and the CBSA share responsibility for collecting information to develop intelligence for investigations relating to national security or crimes such as organized crime and human smuggling.⁵¹⁰

3.11.6 Relationships among Agencies in the Same Ministerial Portfolio

David Quartermain, Director of the Borders Intelligence Division of CBSA's Intelligence Directorate, testified to having a close relationship with agencies within Public Safety Canada (for example, the RCMP and CSIS).⁵¹¹ Denis Vinette, Director of the CBSA Borders Enforcement Division, testified about the advantages of working with agencies from the same department:

[T]here is a benefit, I guess, to our reporting into the same organization, as well as to the same Minister, in terms of what the direction is in terms of our strategies and priorities of the day. And so it ensures that, as we work through the portfolio, Department of Public Safety, that those priorities are shared amongst all the agencies because we all have different roles

504 *A New Review Mechanism for the RCMP's National Security Activities*, p. 102. The report states that, for example, "in 2004, O-INSET (located in Toronto) had members from the Ontario Provincial Police, Toronto Police Service, York Regional Police, Durham Regional Police, Peel Regional Police, CSIS and the CBSA. As of August 2004, O-INSET comprised 53 RCMP regular members, two RCMP civilian members and 22 people on secondment from other agencies and RCMP units."

505 RCMP, "Integrated National Security Enforcement Teams."

506 *A New Review Mechanism for the RCMP's National Security Activities*, p. 102.

507 2008 FATF Mutual Evaluation of Canada, para. 572.

508 Royal Canadian Mounted Police, "Integrated Border Enforcement Teams (IBETs)," online: Royal Canadian Mounted Police <<http://www.rcmp-grc.gc.ca/ibet-eipf/index-eng.htm>> (accessed February 18, 2009) [RCMP, "Integrated Border Enforcement Teams"].

509 RCMP, "Integrated Border Enforcement Teams."

510 2008 FATF Mutual Evaluation of Canada, para. 574.

511 Testimony of David Quartermain, vol. 56, October 2, 2007, p. 7071.

to play, but in the same fight, if you will, when it comes to different types of priorities. And so it just ensures that all of our activities are aligned, be it intelligence information sharing, be it operationally on the ground.⁵¹²

3.11.7 International Cooperation

The number of interdepartmental activities⁵¹³ involving TF matters has increased, in part because Canadian agencies need to collaborate to fulfill international commitments and programs. The 2008 FATF Mutual Evaluation of Canada was one example. As well, FINTRAC has contributed to the typology exercises of a subgroup of FATF on topics such as the use of casinos and “proliferation financing.”⁵¹⁴

CSIS and the RCMP participate in the Five Eyes Terrorist Financing Working Group.⁵¹⁵ CSIS described its participation in the Working Group as follows:

The intent of the Five-Eyes working group is to bring together law enforcement and intelligence agencies to develop recommendations on countering terrorist financing through a coordinated international response. The [CSIS] Financial Analysis Unit has benefited from its continued participation in the Five-Eyes group. It serves to identify areas of mutual interest and emerging trends, and it assists in identifying issues that the Unit should consider in its provision of operational support on terrorist financing.⁵¹⁶

The meetings of the Working Group – involving representatives from Australia, Canada, New Zealand, the United Kingdom and the United States – are held under high security, which allows for the sharing of operational information about cases of mutual interest, including information about investigative and analytical techniques.⁵¹⁷

3.11.8 Secondments

As is the case in the federal government generally, secondments are common among the partners of the AML/ATF Initiative and are an effective means of promoting cooperation and better communication.⁵¹⁸ FINTRAC has a person

⁵¹² Testimony of Denis Vinette, vol. 56, October 2, 2007, pp. 7072-7073.

⁵¹³ Testimony of Mark Potter, vol. 56, October 2, 2007, p. 6997.

⁵¹⁴ Second FINTRAC Response to Supplementary Questions of the Commission, Question 2(d).

⁵¹⁵ Testimony of Jim Galt, vol. 55, October 1, 2007, p. 6928.

⁵¹⁶ CSIS Response to Supplementary Questions of the Commission, Question 3.

⁵¹⁷ CSIS Response to Supplementary Questions of the Commission, Question 3.

⁵¹⁸ Testimony of John Schmidt, vol. 53, September 27, 2007, p. 6642; Testimony of Jim Galt, vol. 55, October 1, pp. 6909-6910.

seconded to the RCMP Integrated Proceeds of Crime Unit.⁵¹⁹ CRA has employees seconded to the RCMP National Security Operations Branch and to CSIS. ITAC is staffed by representatives of several organizations.

Tom Quiggin, an expert in terrorism matters, testified about the value of personal contacts – the types of contacts that secondments help to develop:

During a time of crisis, during a time of stress, an organization like CSIS or an organization like the RCMP will almost never refuse to share information assuming there is a personal contact somewhere.⁵²⁰

3.11.9 Private/Public Sector Advisory Committee

The Department of Finance chairs a private/public sector advisory committee that was created in 2007 in response to recommendations from the November 2004 Auditor General's Report.⁵²¹ Its first meeting was held in November 2007. The membership of the committee includes representatives of many federal agencies and private sector organizations.⁵²²

A summary of the proceedings of the first meeting of the committee showed that it focused on guidance for the benefit of reporting entities and on opinions of the private sector about the anti-TF program. Several questions for future consideration by the private sector were raised on topics such as feedback from government authorities, the consultation process that led to Bill C-25 and communication between government authorities and the private sector.⁵²³ This committee offers government agencies direct contact with private sector representatives.

3.12 Conclusion

Those engaged in raising and moving funds for terrorist purposes have a host of means to do so. Many of those means are very difficult to detect among the massive number of legitimate movements of funds around the globe. Responding to TF involves many government agencies, international organizations and private sector entities.

This chapter has shown the range of government agencies and private sector entities involved in anti-TF efforts. It has also pointed to the complexity of the relationships among these agencies and entities, both in how they cooperate in practice and in the laws that frame their cooperation.

⁵¹⁹ Summary of Meeting with FINTRAC, p. 3.

⁵²⁰ Testimony of Thomas Quiggin, vol. 91, December 7, 2007, pp. 12053-12054.

⁵²¹ Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6784; 2004 Auditor General Report on Money Laundering, para. 2.29.

⁵²² Testimony of Diane Lafleur, vol. 54, September 28, 2007, p. 6784.

⁵²³ Department of Finance Response to Supplementary Questions of the Commission, Question 3(b).