An Examination of the Information Sharing Protocols and Legislated Requirements on the Principal Federal Departments and Agencies Involved in the Anti - Money Laundering / Counter - Threat Financing (AML/CTF) Regime in Canada

By

Andrew Ross

A Masters Research Paper Submitted to
Saint Mary's University, Halifax, Nova Scotia
in Partial Fulfillment of the Requirements for
the Degree of Masters of Business Administration.

August 2012, Halifax, Nova Scotia

Approved: Dr. Cathy Driscoll
Supervisor

Approved: Dr. Mark Raymond
Examiner

Date: August 29th, 2012

An Examination of the Information Sharing Protocols and Legislated Requirements on the Principal Federal Departments and Agencies Involved in the Anti - Money Laundering / Counter - Threat Financing (AML/CTF) Regime in Canada

by Andrew Ross

Abstract: Quantitative and qualitative assessments were conducted concerning the information sharing protocols and realities between the principal Canadian federal departments and agencies responsible for the prevention, detection, and deterrence of money laundering and threat (terrorist) financing activities. The principal agencies involved in the anti – money laundering / counter – threat financing (AML/CTF) regime are the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Royal Canadian Mounted Police (RCMP). Content analysis techniques, in particular Granovetter's (1973) "strength of weak ties", and network theory were utilized to develop the theoretical framework used to examine the links (relationships or ties) between the various departments and agencies involved in Canadian AML/CTF regime. Content analysis assessed various pieces of legislation, as well as for example various annual reports of agencies involved in the AML/CTF regime. This research is timely because three important reports relating to the AML/CTF regime in Canada have recently been released; the Final Report of the Air India disaster (which includes a large section on terrorist financing); the Treasury Board mandated 10 Year review of Canada's Anti-Money Laundering / Anti-Terrorist Financing Regime (fiscal year 2010/2011); and the Interim Report of the Special Senate Committee on Anti-terrorism – Security, Freedom And The Complex Terrorist Threat: Positive Steps Ahead. This research and analysis is exploratory in nature.

August 29th, 2012

Table of Contents

THE LEGALISE

Acknowledgments

My faculty advisor, Dr. Cathy Driscoll, without your willingness to tackle a unique project, your ongoing support and direction, this report would not have been completed.

My colleagues and management who provided countless terrific suggestions, good advice, and who without your training, support, and encouragement this project would not have been completed.

My family, without your ongoing support this project would not have been possible.

Thank you to you all.

INTRODUCTION

The Canadian anti - money laundering / counter - threat financing (AML/CTF) regime represents the federal Government of Canada's response to the illicit acts of money laundering and terrorist financing, and the associated crimes. Although the AML/CTF regime is principally coordinated by federal departments and agencies, many public and private organizations participate in the regime. Some organizations (e.g. financial institutions) are mandated by federal regulations to report certain financial transactions, or register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Without the various public and private organizations' due diligence, adherence to the laws governing their responsibilities as financial institutions, and countless professionals who ensure our financial system is protected from abuse – Canada's economy and reputation would suffer significantly. Several pieces of legislation criminalize money laundering, terrorist financing, and the associated crimes. This paper will outline these laws, describe the roles and responsibilities of the various departments, agencies, and international organizations – ultimately culminating in an examination and assessment of the communication and information sharing relationships of the AML/CTF partners.

Chapter 1 - THE PURPOSE AND IMPORTANCE

This chapter will explain why I am interested in doing this research, why this research is timely and important, and who might be interested in the results of this study.

The Purpose

The purpose of this research is to examine the extent and framework of the relationships between anti-money laundering / counter-threat financing (AML/CTF) regime partners in Canada. These relationships are controlled by the laws, systems, mandates, protocols, and agreements that are in place which govern the AML/CTF regime. Also guided are the activities, communication, information sharing, and disclosure between ministries, agencies, and departments of this regime. This review of the legislation, mandates, and connections between the Canadian Government departments and agencies involved in the AML/CTF regime will culminate in an assessment of the lines of communication and information sharing between the AML/CTF regime partners. These partners collectively monitor, analyze, and disseminate advice to government, and enforce the laws associated with the Canadian AML/CTF regime. This review will involve examining relevant legislation, for example the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*. Furthermore, it will involve examining reports such as the final report on *Air India Flight 182: A Canadian Tragedy,* and the *Audit report of The Privacy Commissioner of Canada on the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)*. This report will also examine and discuss the role that international bodies and agencies play in supporting member states (Canada if/when applicable), and how the Canadian AML/CTF regime compares to those of other countries around the world.

A general member of the public (a student/academic) would not necessarily have access to the individuals involved in money laundering (ML) or terrorist financing (TF) investigations, nor be able to effectively assess their relationships with counterparts in other agencies and departments. Furthermore, assessing the strength (or lack) of professional and personal relationships among individuals working for the various AML/CTF partner agencies would be enormously difficult, perhaps impossible, in the context of an academic research assignment of this nature – this research will examine the AML/CTF regime (the system) partners, their mandates, protocols and agreements. This research will culminate with an assessment of the overall framework and the links (communication and information sharing) between these partners.

More specifically, this report will conclude in numerous relationship (link) analyses, and assessments of the different Canadian AML/CTF regime partners communication and information sharing protocols. This report will utilize research and theories developed by numerous academics, professionals, and government and non-government agencies in the fields of network analysis, content analysis, and the analysis of the Canadian AML/CTF regime. Furthermore, this report will demonstrate whether the relationships (communication and information sharing) between the various Canadian AML/CTF partners are strong, weak, absent, or whether there was insufficient information to determine.

The Importance and Who May Benefit

The importance of this research and analysis should not be underestimated, and is quite relevant and timely for a number of reasons. First, three significantly important reports relating to the AML/CTF regime in Canada have recently been released; the Final Report

of the Air India disaster (which includes a large section on terrorist financing); the Treasury Board mandated 10 Year review of Canada's Anti-Money Laundering / Anti-Terrorist Financing Regime (fiscal year 2010/2011); and the Interim Report of the Special Senate Committee on Anti-terrorism – Security, Freedom And The Complex Terrorist Threat: Positive Steps Ahead. These reports explain the AML/CTF regime, identify current concerns, and suggest recommendations to improve among other things – communication and information sharing. Analyzing these reports, specifically the comments and recommendations related to communication and information sharing between partners will identify commonly identified areas that may require improvement. These reports will also help direct this research and analysis, by identifying key legislation, protocols, agreements, and regime participants' mandates. This research will hopefully be able to further analyze the already recognized important aspects of communication and information sharing, perhaps identifying previously undocumented areas for future examination.

Second, an increased awareness concerning the issues (the commonly identified areas that may require improvement related to the AML/CTF regime) will help facilitate a public debate, ultimately assisting in bringing these issues and concerns into the public sphere for discussion. This discussion will then hopefully encourage the implementation of improvements (if necessary) of the government's response to money laundering and terrorist resourcing, ultimately in line with the Canadian publics' expectations.

Third, Canada's obligations under the numerous international agreements and treaties, to which our government has signed, call for a strong AML/CTF regime of which information sharing and communication are integral components. An example of an

international non-governmental agency to which the Canadian government generally attempts to subscribe to the policy recommendations is the Financial Action Task Force (FATF) which will be discussed in detail at a later stage in this report. Previous FATF reports concerning the Canadian AML/CTF regime have identified areas for improvement. Canada's international reputation, and the Canadian publics' expectation that the Canadian government positively contributes to international security and stability require a robust AML/CTF regime. Meeting (and perhaps exceeding) the international standards set out in these agreements and treaties will assist Canada in earning a good reputation and encouraging the development of similar AML/CTF regimes around the world. It is hoped this research and analysis may play a role in assisting Canada to meet these goals by contributing to the public body of knowledge and debate concerning money laundering and terrorist financing issues. As such, this research, discussion, and analysis will help facilitate the public's increased awareness of the issues, concerns, and methodologies involved in countering money laundering and terrorist resourcing. Ideally, this will increase the public's understanding of the issues, hopefully leading to the most effective government policy.

Fourth, given the unprecedented civil unrest throughout much of the Middle East, as well as the introduction of the *Freezing Assets of Corrupt Foreign Officials Act*, I believe this type of examination is quite timely. This assessment is vital to ensure the AML/CTF regime partners are prepared to act in accordance with the new realities of the global financial system and are prepared to defend against the threats posed by corrupt regimes, terrorists and criminals, as well as to ensure all applicable Canadian law is upheld and enforced.

Fifth, recently, a number of news articles have discussed the issues of money laundering and terrorist financing, specifically how the perpetrators of these crimes "remain largely unknown and unpunished" (Sher, Globe and Mail, 2011). As described in another news article, the "AML/CTF regime in Canada involves 12 federal partners, with progress made over the past 10 years. However, communication and feedback between the regime's partners [should] be improved" (Staff report, Canadian Press, 2011). It is desired that this research and analysis may contribute to understanding and addressing this reported deficiency.

And finally, assuming this report is produced to an acceptable standard, it is hoped it will be a helpful resource to those individuals who work within the AML/CTF regime, and to academics and members of the general public who take an interest in this aspect of public policy, and public safety.

Guiding Theoretical and Methodological Frameworks

I used Granovetter's (1973) "strength of weak ties" and network theory as a theoretical framework to examine the links (relationships or ties) between the various departments and agencies involved in Canadian anti – money laundering / counter – threat financing (AML/CTF) regime. These ties between departments and agencies will be assessed quantitatively using the research and theoretical frameworks presented in several articles on content analysis. More specifically, these ties will be assessed and demonstrated as being either strong, weak or absent, against a set of criteria discussed in greater detail below. I have developed this set of criteria using related works of several academics as a foundation, as well as my own understanding of the AML/CTF regime in Canada. Furthermore, a qualitative assessment that identified key sections, policy, interpretation

and legislation was also undertaken. This work resulted in quantitative and qualitative assessments of the links between the department and agencies involved in the AML/CTF regime, and further demonstrated evidence to whether those links were strong, weak or absent. The quantitative assessment is discussed in detail in Chapter 5-B. The quantitative assessment involved identifying key sections of legislation, policy, information releases, and the interpretation of these documents, culminating in an assessment of the ties between departments and agencies as being either strong, weak, or absent.

MRP Limitations

Although this topic surely has a substantial amount of relevant information available within the classified domain of government, for several reasons this paper will draw only on publicly available information. First, as an employee of the Government of Canada, I have signed an oath to not disclose any sensitive or classified information that I have acquired through the performance of my duties and responsibilities. Second, this paper is an academic examination of the public record – not a journalistic investigative report. As such, an aim of this research is to enhance the public's understanding of the AML/CTF regime in Canada, and how this framework integrates with society to protect Canada's financial system, and Canadian interests. This can only be completed successfully through accurate and rigorous research and analysis of the public record. And finally, I personally believe in the protection of Canadian interests – and I believe part of protecting these interests is an educated public debate and understanding of the institutions that have been established to serve all Canadians and our collective best interests. Tied in with this is a fundamental principle (and expectation) that I and all

individuals privy to sensitive or classified information will not release any information that may jeopardize those interests.

Chapter 2 - THE THEORETICAL FRAMEWORK AND RELEVANT ASSUMPTIONS

Heavily influencing the development of this research is an area of study called *Network Theory* of which *Social Network Analysis* and *Link Analysis* are subsets. *Network Theory* is a multidiscipline area of research examining the links or relationships between actors. Actors could be any number of things, such as individuals, organizations, countries etc – depending on what is being examined. In this instance, this paper will assess the links between the departments and agencies involved in the AML/CTF regime in Canada. These departments and agencies are the actors, and the formal and informal associations, connections, legislated mandates and processes through which they interact are the links or relationships between those actors.

The work of Dr. Mark S. Granovetter, namely *The Strength of Weak Ties* and *The Strength of Weak Ties: A Network Theory Revisited,* which both discussed relationship analysis (link analysis) has been a strong influence on the development of this paper. Although much of Dr. Granovetter's research with respect to these academic articles involved studying the relationships between individuals and how these relationships affected their search for employment – the foundation of the theory is applied here to studying the relationships between the government departments and agencies involved with the AML/CTF regime because a clear set of criteria to assess these links has been established. Also strongly influencing the development of this research is the work of Snijdersy, van de Buntz, and Steglich (2010) from their article titled *Introduction to Stochastic Actor-Based Models for Network Dynamics.* Furthermore, utilizing research and theories developed by Dr. Stephen Schneider, particularly his article *Money*

Laundering in Canada: A Quantitative Analysis of Royal Canadian Mounted Police Cases in the *Journal of Financial Crime* has also enhanced the proposed framework for evaluating the relationships between the many partner agencies within the AML/CTF regime, as well it has provided valuable insights into AML/CTF background, theories and methodologies.

Much the way that Dr. Granovetter wanted to examine the "rather limited aspect of small-scale interaction—the strength of interpersonal ties" (Granovetter, 1973), this paper will examine the scope of information sharing among the departments and agencies involved in the AML/CTF regime in Canada. In [*T]he Strength of Weak Ties* Dr. Granovetter defined "the strength of a tie as a combination of the amount of time, the emotional intensity, the intimacy (mutual confiding), and the reciprocal services which characterize the tie" (Granovetter, 1973). Similarly this paper will utilize the notions of time (e.g. time spent working with or for colleagues from across the AML/CTF regime), intimacy (e.g. the extent of working relationships with colleagues from across the AML/CTF regime), and reciprocal services (e.g. mandates to assist domestic agencies involved with the AML/CTF regime), to examine the strength of the ties between those departments and agencies. But this paper will also discuss notions of legality (e.g. legal frameworks, legislated mandates), privacy, and how these notions interact with the communication and information sharing between partners.

The notions of time and intimacy in the context of interagency and interdepartmental cooperation and communication will be assessed. These examinations will be based on whether joint management meetings, interdepartmental expert groups (IEGs), strategic level exchanges of personnel (secondments), tactical level exchanges of personnel, or

Mutual Legal Assistance Treaties (MLATs) are in place. More specifically, relating to time, are these meetings scheduled regularly? Are these secondments ongoing? Although it may not be possible to answer all of these questions, expectantly an assessment (strong, weak, or absent) will be possible. Adding to the complexity of the notion of time are the concepts of intimacy and reciprocal services – which are anticipated to be more difficult to measure. The following questions will be used to help assess the intimacy and level of reciprocal services. For example, how well do the individuals meeting one another (joint management meetings, IEGs) know each other? Do they communicate only through formal channels, or is it possible for them to make informal disclosures and / or informal requests? Are there mutual training opportunities? At what level does communication occur (executive level, managerial level, analyst level)?

The goal of this paper is to examine the numerous relationships, at various levels, between the relevant departments and agencies, to identify and interpret the strength of the "ties" or relationships between them. To do so, a basic description of the various levels of assessment (strong, weak or absent ties) is required. These descriptions, broken into the various items being assessed are described below in the section "The Ties – Links or Relationships". However, prior to discussing these levels of assessment, several assumptions have been made to facilitate this research and analysis.

The Assumptions

Numerous assumptions have also been made to facilitate the assessment process. The following are the over-arching assumptions that have guided my research and analysis.

Snijdersy, van de Buntz, and Steglich (2010) made "a foundational assumption that [is] network ties examined in [this] work are not brief events, but rather can be regarded as states with a tendency to endure over time". Described in other words, the ties (links) discussed throughout this paper are assumed to be static relationships that have and will endure over time. These ties exist beyond the current government, beyond the state of the current political environment, and beyond those public servants who are currently employed within the framework of the AML/CTF regime. This will allow the assessment to examine the communication and information sharing as part of the AML/CFT regime holistically, and avoid an assessment, for example based solely on relationships between friends or colleagues who happen to currently get along well.

Secondly, also described by Snijdersy et al. (2010) is the assumption used herein which states "actors control their outgoing ties. This means not that actors can change their outgoing ties at will, but that changes in ties are made by the actors who send the tie, on the basis of their and others' attributes, their position in the network, and their perceptions about the rest of the network". Interpreted for this research, the various agencies and departments (the actors) involved with the AML/CTF regime control the communication and ultimately the information passed between them. Described in another way, this communication is based on their legislated mandates (attributes, and position), and the status of cases and/or investigations (perceptions).

A third important assumption for this analysis is that only official text–written and/or codified documents are examined. For example, only legislation, official statements or information sheets will be assessed. This is necessary because information sharing between the departments and agencies of the Government of Canada should only occur

under formal, legally established protocols, under certain circumstances. And those protocols must be written, often codified in the form of legislation. Most intelligence, compliance, and enforcement agencies make a distinction between tactical and strategic exchanges of information. Tactical information exchanges refers to information related to a particular individual, entity, or group associated to a particular investigation, or enforcement action. Strategic information exchanges often refers to information of a general nature, non-specific to a particular individual, entity or group, and information that will not necessarily result in a particular investigation, or enforcement action. This research and analysis will not be examining strategic exchanges of information, though this level of exchange is considered important. This research and analysis will examine only tactical information exchanges as these have the most immediate effect on individuals and groups. For example, a tactical level exchange of information may lead to an enforcement action, such as charges being laid against an individual, or immigration implications, such as the refusal of immigration visas etc.

This report will also only examine domestic exchanges of information. Although international information exchange is vital, and undoubtedly ongoing, this research will not extend beyond Canadian borders. This decision was made for several reasons, perhaps most importantly, access to information. Canada has a Federal government which is supposed to adhere to transparency and access to information protocols. This has facilitated access to the required information and documents. Also, the bounds of this research must be drawn at an appropriate limit – and examining domestic information sharing is a logical limit as domestic information sharing directly affects all Canadians.

In fact, current public debate on the issue of information sharing with foreign countries, and those countries' security services is a hot topic. The protocols, requirements, nature and extent of information sharing with foreign counties are likely to be adjusted in the near term.

And finally, a last interesting notion worth mentioning is "that the loss when terminating a reciprocal tie is greater than the gain in creating [a new] one" (Snijdersy et al., 2009, p.24). This is also assumed to be the case in considering the relationships between AML/CTF regime partners. The connections between AML/CTF regime partners are often established by legislation when those departments and agencies are created. It is also assumed those relationships are further enhanced through MOU's, secondments and agreements.

Chapter 3 – METHODS

This paper is the result of the research, analysis, and findings of the extent of information sharing between the key departments and agencies within the AML/CTF regime in Canada. This work is exploratory in scope. The methodologies utilized herein, to assess the information sharing between regime partners, are from the discipline of *content analysis*. As described by Neuendorf (2002, p.1), content analysis "may be briefly defined as the systematic, objective, quantitative analysis of message characteristics". The research design and methods are explained in more detail in this chapter.

The Research Design

This research has relied on human coding rather than computer coding, and I, the writer, was the only "active coder". However, this human coding has been aided by technology through exploiting digitized documents and the imbedded search / find features of the computer programs. This ensured the coder found all instances of the terms searched, and as such eliminated the possibly of human error.

The type of analysis used is typically referred to as *text analysis* or *text content analysis* (Neuendorf, 1969). As described by Neuendorf (2002, p.88), a "purposive or judgment sampling" technique was utilized to determine what units were deemed appropriate to be included in this study. This technique relies on the experience and judgement of the researcher to properly identify the most relevant items to be assessed. Helping to identify the proper sample size, of both the departments and agencies to be assessed, what pieces of legislation, annual reports, pamphlets etcetera would be analysed were statements made by key departments. For example, FINTRAC in its first annual report (2001), describes the primary departments and agencies that comprise the AML/CTF regime to be

the Department of Finance, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and the Canada Customs and Revenue Agency (now the Canada Revenue Agency), and the Department of Foreign Affairs and International Trade.

There have been numerous improvements to the AML/CTF regime in Canada during the last two decades. Perhaps the most important development was Bill C-22, the *Proceeds of Crime (Money Laundering) Act* which received Royal Assent in June of 2000, and as a result FINTRAC was officially created on July 5th, 2000. Furthermore, with legislative amendments occurring as a result of the September 11, 2001 terrorist attacks on the World Trade Centre in New York City, NY, including Parliament enacting the *Anti-terrorism Act*, which added combating terrorist financing to FINTRAC's mandate–this research and analysis will focus on these two important pieces of legislation. The addition of combating terrorist financing resulted in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act.* Due to the importance of FINTRAC as Canada's financial intelligence unit, this research has examined FINTRAC's latest annual report, and two pamphlets produced by FINTRAC concerning that agency's information sharing with the AML/CTF regime partners in Canada. The RCMP does not release an annual public report; however much of their activity is legislated by the *Criminal Code of Canada*. The CSIS does issue an annual public report; as such the latest version of this report was considered for this research. Furthermore, the *CSIS Act* which describes what is a threat to the security of Canada was also examined.

Numerous Parliamentary / Senate review have clearly identified the critical departments and agencies involved in the AML/CTF regime. As such, this has facilitated in the idenfication of appropriate documents. And finally, although there is certainly other

annual reports, public reports, speeches, press releases etcetera that could be examined, this research is exploratory in nature.

The "Ties" (links or relationships)

The following explanations, broken into the various items that will be assessed, describes strong, weak, and absent ties/links/relationships within the context of this paper. This is commonly referred to as the "code book" which explains the coding process used during the research and analysis of the various departments and agencies of the Canadian AML/CTF regime. The two other complementary components to the coding process are the "coding form" and the "coding legend" (Neuendorf, 2002). These documents can be found in Appendices 3 and 4 at the end of this report.

Strong Ties

This section describes what constitutes strong ties/links/relationships under each section to be examined. Furthermore, the key terms and references that were utilized to identify a strong tie have been itemized on the "coding form" which can found in Appendix 2.

Legislation

Is the department or agency allowed (by legislation) to share information? If yes, this would qualify as a strong link, or perhaps more appropriately, a possible strong link. However, for the purposes of this research and analysis, if legislation does exist which allows a department or agency to share information with partner Canadian agencies (and international agencies); this will be considered a strong tie. The legislative framework will be based upon examining the provisions within the various relevant Canadian laws

and Parliamentary Acts. Among the most important is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PC(ML)TFA)*.

Mandate

Is the department or agency mandated (by legislation) to share information related to money laundering and/or terrorist financing? This element goes further than the legislation component because this describes a situation where the department or agency must share information, rather than simply being allowed to do so. An example of this would be if a non-law enforcement department or agency must report any instance of an illegal act to the appropriate law enforcement agency. As such, if a department or agency must share information, this would be considered a strong tie.

Priorities

Has the department or agency publically acknowledged that sharing information related to money laundering and / or terrorist financing is a current and on-going top priority? This type of public acknowledgement may arise in annual public reports, media releases, or public statements by the head of the particular department or agency and/or by the department's public relations office. If the answer is yes, then this would qualify as a strong tie.

Inter-Governmental Working Groups

Inter-Governmental Expert Groups (IEGs)

Joint Management Groups

Joint Intelligence Groups (JIGs)

Are there established inter-governmental working / expert groups, or Joint Management / Intelligence Groups which meet regularly and consistently? If yes, this is a strategic / high level of communication between departments and agencies, and would qualify as a strong tie.

Working level collaboration

Are there established inter-governmental groups / meetings / exchanges (e.g. communication) between "working" level analysts, employees, officers etc at the various departments and agencies involved in the AML/CTF regime which are encouraged to communicate and share ideas, best practices, information and expertise regularly and consistently? If yes, this is a tactical / working level of communication between departments and agencies, and would qualify as a strong tie.

Process

Is there an established strategic process that the department or agency follows in the course of completing their duties and mandate – of which communication with partner agencies is an integral component? If the answer is yes, then this would qualify as a strong tie.

Threshold

Is there an element of threshold – or in other words, a test that must be met in order to share information? For example, must a suspicion or belief exist that the information or intelligence held by one department or agency, may assist another department or agency in meeting their duties to investigate money laundering or terrorist financing? If yes, then this circumstance would be categorized as a strong tie.

Secondment(s)

Secondments between departments and agencies are an excellent conduit for communication, aligning goals and objectives and most importantly excellent for information sharing. If there are either two-way or one-way secondments currently staffed at one or both concerned agencies, this will be considered a strong tie.

Liaison(s)

Liaison exchanges between departments and agencies are an excellent conduit for communication, information sharing, and collaboration on topics, cases, and investigations of mutual concern or interest. If there are either two-way or one-way official liaison officers exchanges, currently staffed at one or both concerned agencies, this will be assessed as a strong tie.

Educational Exchanges

Are there formal established exchanges of expertise? For example, training courses open to individuals from various departments or agencies. These type of exchanges allow for individuals to meet their counterparts for other AML/CTF regime partner agencies, develop and maintain a network of contacts, and share information, best practices, and

techniques for countering/combating money laundering and terrorist financing. If these formal exchanges exist and are routinely used, this would be characterized as a strong tie.

Memorandum Of Understanding (MOUs)

Memorandums of Understanding formalize the relationship between signatory departments or agencies. Under this category, to be considered a strong tie it is not only necessary that a MOU be signed, but that it lays out the condition(s) under which information sharing and exchanging must occur. The key under the strong tie classification is that communication must occur between the departments or agencies – they do not have an option.

Weak "Ties"

This section describes what constitutes weak ties/links/relationships under each section to be examined. Furthermore, the key terms and references that were utilized to identify weak ties have been itemized on the "coding form" which can found in Appendix 2.

Legislation

Is the department or agency allowed to share information? The situation becomes more complicated when conditions are imposed upon a department or agency – for example that FINTRAC must be at arm's-length from law enforcement and intelligence agencies. This condition would be considered a weak link (or weak tie). Yes, a department or agencies legislation allows, even directs that department or agency to share information; however that information sharing can only be done under strict conditions and circumstances.

Mandate

Is the department or agency mandated (by legislation) to share information related to money laundering and/or terrorist financing? This element goes further than the legislation component because this describes a situation where the department or agency can share information, rather than simply being allowed to do so. Whereas for this category to be considered a strong tie, the characteristic is must share information, under a weak tie situation the department or agency can share. An example of this would be if a non-law enforcement department or agency can report any instance of an illegal act to the appropriate law enforcement agency, although there are circumstances (e.g. national security concerns) where they can choose not to share information.

Priorities

Has the department or agency publically acknowledged that sharing information related to money laundering and / or terrorist financing is a secondary or tertiary priority, perhaps not directly linked to the department or agencies primary mandate? This type of public acknowledgement may arise in annual public reports, media releases, or public statements by the head of the particular department or agency and/or by the department's public relations office. If the answer is yes, then this would qualify as a weak tie.

Inter-Governmental Working Groups

Inter-Governmental Expert Groups (IEGs)

Joint Management Groups

Joint Intelligence Groups (JIGs)

Are there established inter-governmental working / expert groups, or Joint Management / Intelligence Groups which meet irregularly, inconsistently, or perhaps on a case by case

basis? If yes, this is a strategic / high level of communication between departments and agencies, and would qualify as a weak tie.

Working level collaboration

Are established inter-governmental groups / meetings / exchanges (e.g. communication) between "working" level analysts, employees, officers etc at the various departments and agencies involved in the AML/CTF regime allowed –however not necessarily encouraged – to communicate and share ideas, best practices, information and expertise? If yes, then this is an irregular, inconsistent, or case by case tactical / working level of communication between departments and agencies, and would qualify as a weak tie.

Process

Is there an established strategic process that the department or agency follows in the course of completing their duties and mandate – of which communication with partner agencies is a possible component or outcome (depending on the circumstances)? If the answer is yes, then this would qualify as a weak tie.

Threshold

Is there an element of threshold – or in other words, a test that must be met in order to share information? If the test is more severe, such as a department or agency is only allowed to acquire information or intelligence from another by executing warranted powers, then this circumstance would be categorized as a weak tie.

Secondment(s)

Secondments between departments and agencies are an excellent conduit for communication, aligning goals and objectives and most importantly excellent for

information sharing. However, if there are provisions for either two-way or one-way secondments, but if one or both of these secondments are not currently staffed, this will be considered a weak tie.

Liaison(s)

Liaison exchanges between departments and agencies are an excellent conduit for communication, information sharing, and collaboration on topics, cases, and investigations of mutual concern or interest. If there is a provision for either a two-way or one-way liaison officer exchange program, however, these positions are not currently staffed; this will be assessed as a weak tie.

Educational Exchanges

Are there informal exchanges of expertise between departments or agencies? For example, irregular, inconsistent, or on a case by case basis, are limited training course seats offered limited numbers of individuals from various departments or agencies? These types of exchanges allow for individuals to meet their counterparts for other AML/CTF regime partner agencies, develop and maintain a network of contacts, and share information, best practices, and techniques for countering/combating money laundering and terrorist financing. However, if these informal exchanges exist only as the exception, this would be characterized as a weak tie.

Memorandum Of Understanding (MOUs)

Memorandums of Understanding formalize the relationship between signatory departments or agencies. Under this category, to be considered a weak tie it is not only necessary that a MOU be signed, but that it lays out the condition(s) under which

information sharing and exchanging can occur. The key under the weak tie classification is that communication can occur, rather than must occur between the departments or agencies.

Absent "Ties"

This section describes what constitutes absent ties/links/relationships under each section to be examined. Essentially, if information sharing is not addressed to any extent in the documents examined, this could qualify as an absent tie.

Legislation

Is the department or agency allowed, by law or by an Act, to share information? If no, this would qualify as an absent link.

Mandate

Is the department or agency mandated (by legislation) to not share information related to money laundering and/or terrorist financing? Or does the department or agency require judicial authorization (a warrant) to be executed on them, in order to share information related to money laundering and/or terrorist financing? In these instances, this could be considered an absent tie.

Priorities

If the department or agency has publically acknowledged that sharing information related to money laundering and / or terrorist financing is not a priority, then this would qualify as an absent tie.

Inter-Governmental Working Groups

Inter-Governmental Expert Groups (IEGs)

Joint Management Groups

Joint Intelligence Groups (JIGs)

If these inter-governmental working / expert groups, or Joint Management / Intelligence Groups don't occur or if they are not allowed to occur – this indicates there is no strategic / high level of communication between departments and agencies, and would qualify as an absent tie.

Working level collaboration

If these inter-governmental groups / meetings / exchanges (e.g. communication) between "working" level analysts, employees, officers etc at the various departments and agencies involved the AML/CTF regime don't occur or if they are not allowed to occur - then this is a lack of tactical / working level of communication between departments and agencies, and would qualify as an absent tie.

Process

If there is no established strategic process that the department or agency follows in the course of completing their duties and mandate – or if an established strategic process does not include communication with partner agencies is an integral component – then this would qualify as an absent tie.

Threshold

Is there an element of threshold – or in other words, a test that must be met in order to share information? If there is no test to meet – simply put, the department or agency is

not allowed to pass information, then this circumstance would be categorized as an absent tie.

Secondment(s)

Secondments between departments and agencies are an excellent conduit for communication, aligning goals and objectives and most importantly excellent for information sharing. If there are no (two-way or one-way) secondments, this will be considered an absent tie.

Liaison(s)

Liaison exchanges between departments and agencies are an excellent conduit for communication, information sharing, and collaboration on topics, cases, and investigations of mutual concern or interest. If there are no (two-way or one-way) official liaison officers' exchanges, this will be assessed as an absent tie.

Educational Exchanges

Are there formal established exchanges of expertise? For example, training courses open to individuals from various departments or agencies. These type of exchanges allow for individuals to meet their counterparts for other AML/CTF regime partner agencies, develop and maintain a network of contacts, and share information, best practices, and techniques for countering/combating money laundering and terrorist financing. If these formal exchanges do not exist, this would be characterized as an absent tie.

Memorandum of Understanding (MOUs)

Memorandums of Understanding formalize the relationship between signatory departments or agencies. Under this category, to be considered an absent tie there can be no MOU signed between departments or agencies.

Unknown "Ties"

Unfortunately, on occasion when completing research involving government departments and agencies concerning a topic which can be sensitive, certain information is unavailable including information on the extent, or not, of information sharing. If the necessary information to assess a relationship between a department or agency is unavailable, for any reason, than this tie will be assessed as unknown. These unknown ties are an example of a potential area of further research that could be addressed in later work.

The Document Scan

One of the most difficult tasks associated with this project was attempting to ensure a reasonable sample of the relevant documents (legislation, annual reports, press releases, reviews, speeches by senior bureaucrats etc) were identified, located, retrieved and incorporated into this research. For several reasons, there is no way to ensure absolutely every relevant document is considered; this is an inherent weakness in this type of research work. However, by reviewing reports that have previously examined the AML/CTF regime, by keeping appraised of current affairs, and through my own work and experience, this weakness can be mitigated. For example, *Volume 5 of the Air India Report* provided excellent information concerning the AML/CTF regime in Canada, the various partners, their roles, and the overarching legislation that controls information sharing.

Once all the relevant documents were located, they were saved in digital format (PDF format). This helped facilitate the "coding" process (which is described in section "The Coding", shortly after this section), because the digital searching of terms within the documents removed the human error factor. For example, instead of manually scanning the documents for key words and expressions, a computer would complete the searching, and a human (the writer) could interpret the results. Practically speaking, this often involved using the "CTRL F" (find) feature of Adobe Reader ©, which will scan and identify all searched terms within a document.

Identified / Located / Retrieved Documents

The documents listed below were; identified as being relevant to this research; they were located, primarily on the internet; retrieved and incorporated into this research and

analysis. They were analyzed from the perspective of whether strong, weak or absent ties could be identified within the areas of research described in the "The Ties (links or relationships)" section of this report.

- FINTRAC Annual Report 2010
- CSIS Annual Report 2009-2010
- *Canadian Security Intelligence Service Act (C-23)*
- *Criminal Code (C-46)*
- *Proceeds of Crime (Money Laundering) Terrorist Financing Act*
- FINTRAC Pamphlets
    - Sharing Intelligence – Making The Links
    - Connecting the Money to the Crime

The "coding"

Coding is the process of examining documents identified during the document scan for specific terms, words, expressions, themes etc. Both, the terms, words, expressions, and themes which allowed information sharing, but also prohibited information sharing were categorized. Once these terms were identified and recorded, they were *assessed* against the description of each section (strong, weak, absent, and unknown) described above under "[T]he "Ties" (links or relationships)". The results of this assessment were *documented* on the "coding forms", and *tabulated* on the "coding tables".

To further facilitate the assessment and identification of terms allowing and prohibiting information sharing, Appendix 2 describes words, terms and expressions that positively, quasi-positively, and negatively reflected information sharing.

More specifically with respect to coding annual report type documents, the Coding Tables contain references such as P4Pg6L3 which corresponds to: page number 4, paragraph number 6, and line number 3. Furthermore, a paragraph which begins on one page and continues onto another page will not count as the first paragraph from the new page, as to avoid being counted twice. To denote a term which is found in one of these paragraphs which continued onto another page, paragraph number 0 will be used to denote the continuation of the paragraph from the previous page. Words, terms and expressions that occur within legends, titles, section headings, and official names (e.g. *The Privacy Act*) will not be counted within this coding, as it has been deemed redundant.

Chapter 4 - THE BACKGROUND

The Canadian Financial Sector

As one of the world's most wealthy counties, a population of over 34 million people and one of the most advanced financial services industries in the world – Canada is an attractive locale for business and investment, by individuals, entities and groups who may want to take advantage of this prosperous nation – through both legal and illegal methods. Financial institutions in general are designed to move large quantities of funds between individuals and entities, often in and through various foreign jurisdictions. Canadian financial institutions are no different – and the complex web of banks, money service businesses, correspondent banks, alternative remittance companies etcetera, complicates the AML/CTF regime.

Specifically relating to banks, the *Bank Act* designates banks in one of two categories; Schedule I banks and Schedule II banks. There is a third category, Schedule III, also defined in the *Bank Act*. Schedule I banks are domestic deposit taking institutions that are not a foreign owned bank. An example is the Bank of Nova Scotia. Schedule II banks are deposit taking institutions that are subsidiaries of foreign owned banks. An example is Barclays Bank PLC. Schedule III institutions are foreign banks that are allowed to operate in Canada under restricted conditions as set out in the *Bank Act*.

It is vital to understand that banks are not the only type of financial institution that operates in Canada. There are various money service businesses (e.g. Western Union), credit card companies (e.g. Visa), credit unions (e.g. Desjardins Group), and debit card companies (e.g. Interac) to name a few financial services companies. Each type of

financial institution quite often provides different, yet often complimentary, financial services. And each has legislated responsibilities under the AML/CTF regime in Canada, which often involve reporting certain transactions to the proper authorities, and "know your client" (KYC) requirements.

Money Laundering / Terrorist Financing / Threat Financing

Though often used interchangeably, the terms money laundering (ML), terrorist financing (TF), and threat financing actually describe fundamentally different situations. Moreover, some suggest the term threat resourcing ought to be used, as it describes an array of support that extends beyond simply financing (e.g. funding with money), and should include the provision of services, food and supplies, housing, to help facilitate an act of terrorism. However, first, as terrorist financing is more widely used and accepted, and second, as this paper focuses on the issue of *communication* between government agencies and departments countering illicit funding, TF will be used within this paper to describe the notion of threat resourcing, terrorist financing and money laundering (unless otherwise stated).

Terrorist financing describes a situation where funds, either derived from lawful sources (e.g. earned wages, charitable donations, government transfers etc), or from unlawful sources (e.g. criminal activity), are ultimately used to facilitate or engage in a terrorist act.

Conversely, money laundering begins with a criminal act (the predicate offence) which produces illicit funds. The criminal will want to "cleanse" those funds so the proceeds of the criminal act can be entered into the formal financial sector and enjoyed by the criminals. To "cleanse" those funds, the criminal will typically perform a variety of

activities designed to obscure the true source (the criminal act) and end use of the funds. These activities are the various stages described as money laundering. There are a number of generally accepted frameworks which describe the money laundering process. One that covers generally the various stages is the 3 C's of money laundering – the concealment of the proceeds, the conversion of the proceeds, and the conduits in which the proceeds travel.

And finally, threat financing (or threat resourcing) describes a similar situation to terrorist financing, however encompasses all "threats" to the national security of Canada as defined in section 2 of the *CSIS Act*. For example, terrorist financing relates specifically to section 2(c) of the CSIS Act, which describes violence to achieve a political, religious, or ideological objective. As such, any funds used to facilitate or engage in this behaviour would be considered terrorist financing. However, threat financing would be broader, and would include any financing of "threats" to the security of Canada as defined in sections 2(a) to 2(d) of the *CSIS Act*. Those 'threats" to the security of Canada include: sabotage and espionage; foreign influenced activity; violence to achieve a political, religious, or ideological objective; and subversion.

THE AML/CTF REGIME PARTICIPANTS

The Canadian anti – money laundering / counter – threat financing (AML/CTF) regime is composed of several departments and agencies at the federal, provincial, and municipal levels, as well as numerous organizations (e.g. public and private companies, such as reporting entities and national as well as provincial regulators). The federal government's – Department of Finance is the lead agency charged with the mandate of protecting the Canadian financial system. Several key agencies report to the Minister of Finance or

report to Parliament through the Department of Finance including the Financial Transactions and Reports Analysis Centre (FINTRAC), and the Office of the Superintendent of Financial Institutions of Canada (OSFI). Moreover, the Department of Public Safety houses several government agencies who contribute and fulfil roles related the AML/CTF regime - namely, the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and the Canada Border Services Agency (CBSA). And finally, the Canada Revenue Agency (CRA) contributes to the AML/CFT regime through a variety of facets associated to its administration of the *Income Tax Act*. Below a more in-depth discussion of each partner is conducted, focussing on the mandate and priorities of each department and agency.

The Office of the Superintendent of Financial Institutions of Canada (OSFI)

The Office of the Superintendent of Financial Institutions of Canada (OSFI) is a federal government agency that falls under the umbrella of the Department of Finance. Established in 1987, OSFI has a mandate to "contribute to the safety and soundness of the Canadian financial system by supervis[ing] and regulat[ing] federally registered banks and insurers, trust and loan companies, as well as private pension plans by ensur[ing] they are complying with their governing legislation" (*OSFI and the Canadian Financial System* brochure, 2009). Although OSFI operates at arm's length from the Department of Finance, it reports to Parliament through the Minister of Finance.

As of February 28th, 2012, the Office of the Superintendent of Financial Institutions Canada (OSFI) regulated a total of one-hundred and fifty-two (152) deposit taking institutions, and two-hundred and seventy-two (272) insurance companies. Of the financial institutions, seventy-seven (77) were banks, forty-nine (49) were trust

companies, nineteen (19) were loan companies, six (6) were cooperative credit associations, and one (1) was a cooperative retail association. Specifically relating to the category of banks; twenty-three (23) were domestic banks, twenty-six (26) were foreign banks, twenty-three (23) were foreign bank branches (full service), and five (5) were foreign bank branches (lending).

Along with OSFI, the Canada Deposit Insurance Corporation (CDIC), the Federal Consumer Agency of Canada, the Bank of Canada, and the Department of Finance comprise the Financial Institutions Supervisory Committee (FISC). This committee meets on a quarterly basis, and helps OSFI meet its mandate.

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

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is best described as Canada's financial intelligence unit (FIU) whose mission as stated in the *Annual Report 2010 - FINTRAC* is "[T]o contribute to the public safety of Canadians and to help protect the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist financing". FINTRAC was established by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PC(ML)TFA)* in 2000, and is governed by the regulations set out in this Act. Ultimately, FINTRAC was established to "collect, analyze and disclose financial information and intelligence on suspected money laundering and terrorist financing activities" to the appropriate police force and/or intelligence agency. However, FINTRAC is legislated to be at "arms length" from law enforcement and intelligence agencies. And finally, FINTRAC reports to Parliament, through the Department of Finance.

The Office of the Superintendent of Bankruptcy

The Office of the Superintendent of Bankruptcy (OSFI) is a federal government agency reporting through the Department of Finance to Parliament. Established in 1987, OSFI's mandate is to "contribute to the safety and soundness of the Canadian financial system. OSFI supervises and regulates federally registered banks and insurers, trust and loan companies, as well as private pension plans subject to federal oversight, and ensures they are complying with their governing legislation" (OSFI and the Canadian Financial System, brochure). Although OSFI's role extends beyond the national security and law enforcement objectives associated with the AML/CTF regime – OSFI does play an important role in contributing to the success of the AML/CTF regime.

The Canadian Security Intelligence Service (CSIS)

The Canadian Security Intelligence Service (CSIS) is Canada's civilian security intelligence agency responsible for investigating threats to national security. The McDonald Commission of Inquiry and the Mackenzie Commission laid the groundwork for the separation of security intelligence work and law enforcement, both previously the responsibility of the Royal Canadian Mounted Police (RCMP). The Canadian Security Intelligence Service Act (Bill C-23) provides the legislated mandate and expectations for CSIS, and established this agency in 1984.

The CSIS' primary mandate as stated by Section 12 of the *CSIS Act* is to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada". Section 2 of the CSIS Act describes

threats to the national security of Canada, and they include; sabotage and espionage (2a), foreign influenced activity (2b), the threat or use of serious violence to achieve a political religious or ideological objective (2c), and subversion (2d).

The Communications Security Establishment Canada

The Communications Security Establishment Canada (CSEC) is Canada's cryptologic agency responsible for acquiring information to assist the Government of Canada, and protecting Government of Canada information. More specifically, CSEC is mandated to "acquire and provide foreign signals intelligence, and to provide advice, guidance and services to help ensure the protection of Government of Canada electronic information and information infrastructures. [They] also provide technical and operational assistance to federal law enforcement and security agencies" (CSEC Information Kit, http://www.cse-cst.gc.ca/home-accueil/media/information-eng.html). CSEC's mandate has been codified by Canada's National Defence Act, recently amended by the 2001 Anti-Terrorism Act. CSEC is accountable to Cabinet and Parliament through the Minister of National Defence. "The Chief of CSEC reports to the Minister through two Deputy Ministers, the National Security Advisor responsible for CSEC's policies and operations, and the Deputy Minister of National Defence overseeing financial and administrative matters. The CSE Commissioner also prepares an annual report to the Minister of National Defence on the results of all review activities" (Parliamentary Accountability, http://www.cse-cst.gc.ca/home-accueil/privacy-privee/parliament-parlement-eng.html).

The Royal Canadian Mounted Police (RCMP)

The Royal Canadian Mounted Police (RCMP) is an enormous institution with an extremely broad mandate, with a history dating back well over a century. Established in

1919 by merging the Royal North West Mounted Police and the Dominion Police – "the RCMP has a mandate to enforce laws, prevent crime, and maintain peace, order and security" (RCMP Corporate Facts brochure). Serving from coast to coast, the RCMP had 29,292 persons serving as of September 30th, 2010. The RCMP is Canada's national police force comprising numerous divisions, branches, and units – responsible for a wide variety of programs and services. Relating to the AML/CTF regime, the RCMP has a number of program areas that play a role, including; the Commercial Crime Section, the Customs and Excise Program, the Integrated Counterfeit Enforcement Teams (ICETs), the Integrated Market Enforcement Teams (IMETs), Interpol Ottawa Section, the National Anti-Counterfeiting Bureau (NACB), the Organized Crime Section, the Proceeds of Crime Section, and the National Security Criminal Operations Branch.

The Canada Revenue Agency (CRA)

The Canada Revenue Agency (CRA), previously the Canada Customs and Revenue Agency (CCRA) is "responsible for the administration of tax programs, as well as the delivery of economic and social benefits" (Structure and Operational Framework, http://www.cra-arc.gc.ca/gncy/brd/bm-bkgrd-eng.html). CRA "promotes compliance with Canada's tax legislation and regulations and plays an important role in the economic and social well-being of Canadians" (ibid). And finally, the CRA is "committed to working closely with stakeholders, providing excellent service to clients, and ensuring responsible enforcement of legislation" (ibid).

The Canada Border Services Agency (CBSA)

The Canada Border Services Agency (CBSA) is a large agency comprised of "approximately 13,000 employees, including over 7,200 uniformed CBSA officers who

provide services at approximately 1,200 points across Canada and at 39 international locations" (About Us, What We Do, http://www.cbsa-asfc.gc.ca/agency-agence/what-quoi-eng.html). The services and responsibilities of the CBSA are extensive and varied, and as described by the CBSA website "About Us, What We Do" located at http://www.cbsa-asfc.gc.ca/agency-agence/what-quoi-eng.html including:

- administering legislation that governs the admissibility of people and goods, plants and animals into and out of Canada;
- detaining those people who may pose a threat to Canada;
- removing people who are inadmissible to Canada, including those involved in terrorism, organized crime, war crimes or crimes against humanity;
- interdicting illegal goods entering or leaving the country;
- protecting food safety, plant and animal health, and Canada's resource base;
- promoting Canadian business and economic benefits by administering trade legislation and trade agreements to meet Canada's international obligations;
- enforcing trade remedies that help protect Canadian industry from the injurious effects of dumped and subsidized imported goods;
- administering a fair and impartial redress mechanism;
- promoting Canadian interests in various international forums and with international organizations; and
- collecting applicable duties and taxes on imported goods.

The Department of Finance

The Department of Finance is the "lead department in the federal government's overall initiative to combat money laundering (ML) and TF. 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-Terrorist Act (ATA) in 2001" (Volume Five: Terrorist Financing, Air India Report, pg 76). Finance is the umbrella department responsible for a number of key agencies involved in the AML/CTF regime. The Office of the Superintendent of Financial Institutions Canada (OSFI) and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) are at the forefront of the Canadian government's AML/CTF regime designed to prevent, detect and deter money laundering and terrorist financing.

Inter-Governmental / Non-Governmental Organizations

The following international non-governmental organizations contribute to, or affect the AML/CTF regime in Canada:

- The Financial Action Task Force (FATF)

- The Wolfsberg Group

- The Egmont Group

- The United Nations (UN)

- The International Monetary Fund

- The World Bank

The Financial Action Task Force (FATF)

The above listed inter-governmental and non-governmental organizations contribute to the health and stability of the global financial system through a variety of mandates. The most pertinent organization involved with this work is the Financial Action Task Force (FATF), which has set out an AML/CTF framework or guideline for member countries. "The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard" (Financial Action Task Force, *Handbook for Countries and Assessors*).

Chapter 5 A - THE RESULTS

The following "coding" totals were tallied from the individual coding forms (available in Appendix 4). To interpret the information contained in the table below, the first number is: terms present / total number. For example, concerning the *Criminal Code of Canada* under *positive*, out of the twenty-two (22) terms identified as positive examples of information sharing, nine (9) were located within the *Criminal Code of Canada*. The second number is: the total number of instances those nine (9) positive terms were located within the *Criminal Code of Canada*.

Coding Forms Totals

Criminal Code of Canada	9 / 22 ; 66	1 / 9 ; 6	3 / 10 ; 12
CSIS Act	10 / 22 ; 61	0 / 9 ; 0	3 / 10 ; 3
CSIS Public Report 2009/2010	16 / 22 ; 84	3 / 9 ; 6	2 / 10 ; 7
FINTRAC Annual Report 2011	16 / 22 ; 141	4 / 9 ; 5	3 / 10 ; 12
FINTRAC - Connecting Money to the Crime pamphlet	5 / 22 ; 23	2 / 9 ; 2	4 / 10 ; 5
FINTRAC - Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links pamphlet	12 / 22 ; 52	0 / 9 ; 0	1 / 10 ; 1
PC(ML)TFA	14 / 22 ; 191	0 / 9 ; 0	2 / 10 ; 13
	Positive	**Quasi-Positive**	**Negative**

Chapter 5 B - THE ASSESSMENT

For several reasons, this research and analysis should be considered exploratory in scope. First, due to the extremely large body of material that could be coded, second, the methodology used to code this material (e.g. manual human coding), and the time constraints on this work, this research cannot be considered complete. Moreover, this research and analysis has been conducted under several assumptions that have limited the scope. Furthermore, no federal Canadian departments or agencies were engaged from an *Access to Information Act (ATIP)* perspective. Under the *ATIP* regime, additional information may be available concerning memoranda of understanding, secondments etcetera that may facilitate information sharing between departments and agencies. Expanding this research, choosing different assumptions, and sending key departments and agencies *ATIP* requests may shed light on, or reveal enhanced and/or limited relationships.

Quantitative Analysis / Results

The quantitative results of the coding process show significantly higher frequencies of positive information sharing terms compared to quasi-positive and negative terms. The results also show significantly higher instances of these positive terms when compared to the total number of quasi-positive and negative terms within the documents examined.

There is a potentially strong bias that may have influenced these results unfairly. That is that the total number of positive information terms searched for (22) is higher than quasi-positive terms (9) and negative terms (10). Although, if you combined the results of quasi-positive and negative terms, the total number of positive terms found within these documents still significantly outnumbers that of the former.

This would appear to indicate that of the documents examined, which were chosen due to their relevance to the topic of information sharing between domestic departments and agencies involved in the AML/CTF regime in Canada, they exhibit a strong propensity or they instil a strong requirement to share information. However, the presence of quasi-positive and negative terms would seem to indicate that there are likely limits on the extent of allowable information sharing. Or that information sharing can only occur under certain situations or when certain requirements are satisfied. To confirm this assessment a qualitative review, analysis, and assessment is required. The qualitative analysis will help to identify those limits, situations and requirements. A detailed breakdown of the assessment follows.

Qualitative Analysis/Results

The Canadian Security Intelligence Service Act

There are numerous sections of the *CSIS Act* which pertain to the sharing of information related to the contribution of the CSIS to the AML/CTF regime in Canada, namely Sections 12 to 14, Section 17 and Section 19. More specifically, Section 12 sets out the general information sharing protocols of the CSIS mandate as stated by "[T]he Service shall...report to and advise the Government of Canada." Section 13 is more specific as to what can be reported (security assessments in this instance) to the provinces and foreign states, and under what circumstances. As the scope of this research is limited to domestic information sharing, Section 13(2) discusses arrangements with Canadian provinces. The *CSIS Act* requires that the CSIS can only enter into an arrangement with a province with the approval of the Federal Minister responsible for the CSIS and if the CSIS is providing security assessments to any police force in a province, the approval of

the provincial Minister responsible for police forces is required. Section 14 states that the CSIS may advise any Minister on matters related to the security of Canada which would include money laundering and terrorist financing. Furthermore, Section 14 also states that the CSIS may provide any Minister with information relating to security matters or criminal activities. The limit established by Section 14 is that this information sharing can only occur "related to the exercise of any power or the performance of any duty or function under the *Citizenship Act* or the *Immigration and Refugee Protection Act"*. Much like Section 13, Section 17 states that the CSIS may cooperate with any province of Canada, however the approval of the Minister is required. And again the same as Section 13, if the CSIS wants to cooperate with any police force within a province, the approval of the provincial Minister responsible for police forces is also required. And finally, Section 19 discusses the authorized disclosure of information. Interestingly, Section 19 states that "information obtained by the Service shall not be disclosed except in accordance with this section". This is an interesting approach, as it dictates strict guidance describing the circumstances under which disclosure is allowed. This section does not direct or proscribe the CSIS to disclose; rather it gives the CSIS the authority to disclose should it choose to do so.

The CSIS Annual Public Report 2009/2010

The CSIS Annual Public Report 2009/2010 contains numerous references which indicate strong and/or weak ties between CSIS and other departments, not all of which necessarily pertain to the AML/CTF regime in Canada. For example, this public report states that the "Service provides advice to Citizenship and Immigration Canada (CIC) through this (immigration screening) program in order to help it with its decisions, as well as to the

Canada Border Services Agency (CBSA)". The advice the CSIS provides to CIC would likely not be in support of the AML/CTF regime in Canada; however, the advice the CSIS provides to the CBSA may indeed be in support of the AML/CTF regime. For example, the CBSA may utilize CSIS information to help identify high risk flights to jurisdiction of concern, that could help any currency interdiction programs, which may be connected to money laundering or terrorist financing activities. In other words, CBSA may use CSIS information to help them attempt to stop individuals from engaging in money laundering and/or terrorist financing activities, such as bulk cash smuggling. However, it is also interesting this CSIS annual report does state that under the Government Screening program, CSIS may provide all government departments and institutions security assessments. Perhaps, most importantly in this CSIS annual report is the section which discusses terrorist financing and financial investigation. Specifically, this CSIS public report states "[B]y partnering with other agencies and institutions, CSIS remains vigilant in investigating all forms of terrorist financing or support".

The Anti-Terrorism Act

The *Anti-Terrorism Act* is a piece of legislation introduced after the September 11th attacks of 2001 essentially as a means to bring Canadian laws up to date with the current realities of international terrorism and extremism. This Act acknowledges that individuals "are entitled to live their lives in peace, freedom and security". Furthermore, this Act acknowledges that "acts of terrorism constitute a substantial threat to both domestic and international peace and security ... that acts of terrorism threaten Canada's political institutions, the stability of the economy and the general welfare of the nation". Moreover, this Act states that "the challenge of eradicating terrorism, with its

sophisticated and trans-border nature, requires enhanced international cooperation and a strengthening of Canada's capacity to suppress, investigate and incapacitate terrorist activity" and that "the Parliament of Canada, recognizing that terrorism is a matter of national concern that affects the security of the nation, is committed to taking comprehensive measures to protect Canadians against terrorist activity while continuing to respect and promote the values reflected in, and the rights and freedoms guaranteed by, the *Canadian Charter of Rights and Freedoms*". This Act amends numerous other pieces of legislation including:

- the *Criminal Code*,
- the *Official Secrets Act*,
- the *Canada Evidence Act*,
- the *Proceeds of Crime (Money Laundering) Act*,
- the *Income Tax Act*, Sections 114 to 144,
- and finally the *Charities Registration (Security Information) Act* was enacted.

The pertinent question to ask with respect to this research is: has the *Anti-Terrorism Act* enhanced domestic information sharing between departments and agencies involved in Canada's AML/CTF efforts?

The Criminal Code

Many other pieces of legislation which pertain to the AML/CTF regime in Canada derive definitions, meanings, and authority to respond to money laundering and terrorist financing due to various sections within the *Criminal Code of Canada*. For example, Section 83 of the *Criminal Code*, specifically relates to terrorism. Furthermore, Section 448 concerns offences related to currency, and Sections 462.3 to 462.5 relate to proceeds

of crime. More specifically, this *Act* describes a "money laundering offence" to mean an offence under subsection 462.31(1). Moreover, "terrorist activity" is defined in subsection 83.01(1), and "terrorist activity financing offence" is defined under sections 83.02, 83.03 or 83.04 of the *Criminal Code*, or to mean an offence under section 83.12 of the *Criminal Code* arising out of a contravention of section 83.08.

The coding process for this particular piece of legislation was limited. There are two primary reasons for this limiting of the coding process to these sections (83, 448, and 462.3) described directly above. First, the size of this Act is huge, well over 1,000 pages of detailed legislation. And second, the Criminal Code of Canada covers all criminal acts, the vast majority of which have no relation whatsoever to anti - money laundering or countering terrorist financing. As such, the above sections were identified as the relevant sections related to the AML/CTF regime in Canada. And the following analysis will focus only on the above stated sections.

Section 83.06 deals with the admission of foreign information, which a judge of the Federal Court of Canada will make the decision whether that information will be admissible. However, for the purposes of this research, foreign information sharing is outside of the scope of this report.

Section 83.1(1) discusses disclosure of information to the RCMP and the CSIS, specifically it states: "[E]very person in Canada and every Canadian outside Canada shall disclose forthwith to the Commissioner of the Royal Canadian Mounted Police and to the Director of the Canadian Security Intelligence Service: (a) the existence of property in their possession or control that they know is owned or controlled by or on behalf of a

terrorist group; and (b) information about a transaction or proposed transaction in respect of property referred to in paragraph (a)." This would seem to give the authority to anybody, from anywhere, the legal ability to disclose information to the RCMP or the CSIS about property owned or controlled by a terrorist group, or a transaction related to property owned or controlled by a terrorist group. The Government of Canada maintains a listing mechanism within the *Criminal Code* that identifies which groups it considers to be a terrorist entity, and this listing is publically available information.

Section 83.28(8) states that a person ordered to answer questions or produce something for a judge can refuse if "answering a question or producing a thing would disclose information that is protected by any law relating to non-disclosure of information or to privilege".

Under section 448 relating to currency there are no specific portions which concern information sharing.

Section 462.48(1.1) states that the Attorney General of Canada the authority to file "for an order for disclosure of information under subsection (3), for the purposes of an investigation". Furthermore, section 462.48(2) states "[A]n application under subsection (1.1) shall be made ex parte in writing to a judge and be accompanied by an affidavit sworn on the information and belief of the Attorney General or a person specially designated by the Attorney General". Moreover, section 462.48(3) gives the judge, assuming the judge is "satisfied that the disclosure of information is in the public interest and that this disclosure will likely accrue benefit to the investigation of a crime", the authority to "order the Commissioner of Revenue to allow a police officer named in the

order access to all such information and documents and to examine them, or where the judge considers it necessary to produce all such information and documents and allow the police officer to remove the information and documents". There are a number of interesting points to consider here, specifically, the fact that the applications will be made ex parte. And that the disclosure of information must be in the public interest and will also accrue a benefit to the investigation of a crime. And finally, the judge can impose "any conditions that they consider advisable in the public interest".

Section 462.48(6) gives the "Minister of National Revenue or any person specially designated in writing by that Minister for the purposes of this section may object to the disclosure of any information or document in respect of which an order under subsection (3)" under certain circumstances. Those circumstances are itemized in sub-sections (a) to (d) of Section 462.48(6), and include:

> (a) the Minister of National Revenue is prohibited from disclosing the information or document by any bilateral or international treaty, convention or other agreement respecting taxation to which the Government of Canada is a signatory;
>
> (b) a privilege is attached by law to the information or document;
>
> (c) the information or document has been placed in a sealed package pursuant to law or an order of a court of competent jurisdiction; or
>
> (d) disclosure of the information or document would not, for any other reason, be in the public interest.

Section 462.48(15) is also relevant as it limits the further dissemination of information or documents that have been "disclosed or provided pursuant to this subsection or pursuant to an order made under subsection (3) ... except for the purposes of the investigation in relation to which the order was made".

The Proceeds of Crime (Money Laundering) Terrorist Financing Act

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PC(ML)TFA)* was given royal assent on the 29th of June, 2000. This act is designed with three objectives as described by Section 3 of the Act. First, to combat the laundering of proceeds of crime (anti money laundering) and combat the financing of terrorist activities (counter threat financing), partly by establishing FINTRAC, but also by creating the system to "detect and deter money laundering and the financing of terrorist activities and to facilitate the investigation and prosecution of money laundering offences and terrorist activity financing offences". Second, to attempt to counter the "threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities" – however, at the same time protecting the personal information of individuals. And finally, the PC(ML)TFA is designed "to assist in fulfilling Canada's international commitments to participate in the fight against transnational crime, particularly money laundering, and the fight against terrorist activity".

A noteworthy component of this legislation is that any transaction(s) that occurs or any transaction(s) that is attempted, and is suspected to be related to the commission or the attempted commission of a money laundering or terrorist financing offence is to be reported to FINTRAC, and depending on the circumstances to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service (Section 7). Moreover, financial institutions et al as described by Section 5 must fully identify an individual in order to open an account on their behalf (Section 9.2). This type of due diligence is commonly referred to "know your customer" (KYC). Another aspect of this due

diligence is discussed in Section 9.6 which describes the expected compliance programs for financial institutions et al, for example risk assessments and record keeping.

It is interesting that the section of the PC(ML)TFA that deals with disclosure and use of information, which begins at section 36, begins with a prohibition of disclosure and use of information, specifically Section 36(1)(a) to Section 36(1)(c). It is also interesting to note that this prohibition is also related to the Privacy Act. It seems the government of Canada is attempting to strike a balance between the constitutionally and legislatively protected privacy afforded to individuals against the mandated duties of law enforcement and intelligence services to protect Canadians, Canadian interests, and Canadian society writ large. Moreover, section 53 further limits information sharing, or perhaps more appropriately enhances the privacy afford to Canadians by specifically stating that "[T]he Director (of FINTRAC) may not disclose any information under section 52 that would directly or indirectly identify an individual who provided a report or information to the Centre, or a person or an entity about whom a report or information was provided under this Act". Furthermore, section 54(e) directs FINTRAC to destroy any report referred to in section 54(a) "15 years after the day on which a report referred to in paragraph [54](a) is received".

Section 36(1.1) authorises an "officer [of FINTRAC] who has reasonable grounds to suspect that the information referred to in subsection (1) is relevant to determining whether a person is a person described in sections 32 to 42 of the Immigration and Refugee Protection Act or is relevant to an offence under any of the sections 117 to 119, 126 or 127 of that Act". This essentially gives authority to FINTRAC to share pertinent information with Citizenship and Immigration Canada (CIC) and the Canada Border

Services Agency (CBSA) to assist them in the fulfilment of their mandated duties. It is also worth noting that the threshold is reasonable grounds to suspect, not the higher threshold of reasonable grounds to believe.

Section 36(1.2) authorises an "officer [of the FINTRAC] 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". This essentially gives authority to FINTRAC to share information under its control with the RCMP when it (FINTRAC) has reasonable grounds to suspect that information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence. Again it is also worth noting that the threshold is reasonable grounds to suspect, not the higher threshold of reasonable grounds to believe.

Section 36(3) states an "officer [believed to be of the RCMP] may disclose to the Centre [FINTRAC] information referred to in subsection (1) if the officer has reasonable grounds to suspect that it would be of assistance to the Centre in the detection, prevention or deterrence of money laundering or of the financing of terrorist activities".

Section 37 limits the extent to which information obtained under this Act can be used and shared. Specifically, section 37 states "[N]o official shall use information referred to in subsection 36(1) for any purpose other than exercising powers or performing duties and functions under this Part".

Section 38, 39, 56, and 65.1 specifically relate to the exchange of information with foreign states, as such is outside the scope of this research and analysis.

Section 54 describes the type of information, and under what conditions FINTRAC is allowed to accept. More specifically, section 54(a) states that FINTRAC "shall receive ... information provided to the Centre by law enforcement agencies or government institutions or agencies, and other information voluntarily provided to the Centre about suspicions of money laundering or of the financing of terrorist activities".

Section 55(1) states what information FINTRAC is prohibited from disclosing, whereas section 55(3) states what information (referred to as "designated information") FINTRAC is authorised to disclose if FINTRAC "on the basis of its analysis and assessment under paragraph 54(c), 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". Section 55(3), also identifies what Canadian government departments and agencies FINTRAC shall disclose information to, and under what circumstances, if the previously discussed threshold is met. These departments and agencies, and the circumstances are listed as follows:

> (a) the appropriate police force;
>
> (b) the Canada Revenue Agency, if the Centre also has reasonable grounds to suspect 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;
>
> (b.1) the Canada Border Services Agency, if the Centre also has reasonable grounds to suspect 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;
>
> (c) the Canada Revenue Agency, if the Centre also has reasonable grounds to suspect that the information is relevant to determining

(i) whether a registered charity, as defined in subsection 248(1) of the Income Tax Act, has ceased to comply with the requirements of that Act for its registration as such, or

(ii) 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 Income Tax Act, is eligible to be registered as such;

(d) the Canada Border Services Agency, if the Centre also determines that 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 that Act;

(e) the Canada Border Services Agency, if the Centre 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 Customs Act or under any other Act of Parliament; and

(f) the Communications Security Establishment, if the Centre 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 National Defence Act.

It is interesting to note the slight difference between sections 55(1) and 55.1(1). As noted above, section 55(1) states "FINTRAC must have reasonable grounds to suspect the designated information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence" in order for it to disclose to law enforcement, CRA, CBSA, and CSEC. In contrast, section 55.1(1) states that, if FINTRAC "on the basis of its analysis and assessment ... has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada, the Centre shall disclose that information to the Canadian Security Intelligence Service". It seems section 55.1(1) utilises the definition of threats to the security of Canada as defined in section 2 of the CSIS Act. The *CSIS Act* states those threats as: sabotage and espionage; foreign influenced activity; violence to achieve a political, religious, or ideological objective; and subversion. It is also worth mentioning that the definitions of

"designated information" in sections 55(7) and 55.1(1)(3) have been compared, and are indeed the same.

Section 60 sets out the framework which "[T]he Attorney General may, for the purposes of an investigation in respect of a money laundering offence or a terrorist activity financing offence, make an application" to a judge. Section 60(3) goes on to state that the "application shall be made ex parte in writing to a judge and be accompanied by an affidavit sworn on the information and belief of the Attorney General". Section 60(4) states that the judge can "impose whatever conditions he considers advisable in the public interest ... to allow a police officer ... have access to and examine all information and documents to which the application relates". Section 60(8) allows the Director of FINTRAC to object to disclosure of any information or document in respect of which an order under section 60(4). This order would commonly be known as a warrant.

Section 60.1 sets out a similar framework which allows "[T]he Director of the Canadian Security Intelligence Service ... for the purposes of an investigation in respect of a threat to the security of Canada, after having obtained the approval of the Minister of Public Safety and Emergency Preparedness, make an application ... to a judge for an order for disclosure of information".

Section 60.3(1) sets out a similar framework which allows "the Commissioner of Revenue ... may, for the purposes of an investigation in respect of an offence that is the subject of the disclosure, after having obtained the approval of the Minister of National Revenue, make an application for an order for disclosure of information".

It is interesting to note the difference in the definition of judge in sections 60, 60.1, and 60.3. Section 60 and 60.3 state "judge means a provincial court judge as defined in section 2 of the Criminal Code or a judge as defined in subsection 462.3(1) of that Act. Whereas section 60.1 states "[I]n this section, “judge” means a judge of the Federal Court designated by the Chief Justice of the Federal Court for the purposes of the Canadian Security Intelligence Service Act".

Sections 62-65 concern compliance, insofar as FINTRAC is legislatively mandated to ensure those entities proscribed as reporting entities conform to their legally mandated function to report certain transactions to FINTRAC. Section 65 states that FINTRAC “may disclose to the appropriate law enforcement agencies any information of which it becomes aware under section 62, 63 or 63.1 and that it suspects on reasonable grounds is evidence of a contravention of Part 1”.

Section 70(2) puts further restrictions on the Auditor General Canada and anyone working on behalf of the Auditor General of Canada.

FINTRAC Annual Report 2011

The FINTRAC Annual Report 2011 states the agency has an extensive number of domestic relationships, including with the primary AML/CTF regime partners, namely the CSIS, the RCMP, the CBSA, and the CRA. The annual report gets more specific, and says “[T]he agencies key domestic partners are the Royal Canadian Mounted Police, all municipal and provincial police services, the Canadian Security Intelligence Service, the Canada Revenue Agency, and the Canada Border Services Agency” (pg 2). It goes onto to say “[V]oluntary information may be provided to FINTRAC by members of the public,

but it is usually provided by its law and security partners as part of their own investigations ... [T]hat information, when combined with the results of FINTRAC's own data mining, may lead to a disclosure by FINTRAC to law enforcement" (pg 13). Moreover, the annual report states "[D]isclosures can be made to a partner only when FINTRAC has reasonable grounds to suspect that the information to be disclosed would be relevant to an investigation or prosecution of a money laundering or terrorist activity financing offence, or relevant to threats to the security of Canada. When it does show such grounds, then FINTRAC must make a disclosure." The annual report also states simply that "FINTRAC is an independent agency" (pg 13). It goes onto say "FINTRAC also maintains strong partnerships with national, provincial and international financial and other regulators, and has entered into 19 memoranda of understanding (MOUs) with these regulators. The MOU with the Office of the Superintendent of Financial Institutions (OSFI), for example, enables OSFI to share information with FINTRAC related to the compliance of federally regulated financial institutions (FRFIs) with their anti-money laundering/anti-terrorist financing obligations"(pg 28).

It is noteworthy that according to the FINTRAC website on February 6, 2012, an Access to Information Act request (request number A-2011-00013) was filed with FINTRAC relating to "[A]ll memoranda of understanding (MOU) pertaining to the relationship between FINTRAC and CSIS, from September 11, 2001 to present (November 10, 2011)". No material was released as it was considered "all exempted" from release under the Access to Information Act. It is believed this is due to the sensitive and classified nature of this information.

FINTRAC, Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links – pamphlet

The very title of this pamphlet leads one to believe that FINTRAC, law enforcement, and intelligence partners work together through sharing intelligence in order to make the links between individuals, entities, and groups engaged in money laundering, terrorist financing, and threat related activities. Through analysis of transaction reports contained in FINTRAC's dataset, it "is disclosed as tactical financial intelligence (typically referred to as a "disclosure") to the appropriate investigative and intelligence organizations at the federal, provincial and municipal levels. Such organizations include any police service in Canada, Canadian Security Intelligence Service (CSIS), Canada Border Services Agency (CBSA) and Canada Revenue Agency (CRA), among others" (pg.4). This pamphlet goes on to state what information is disclosed, referred to as *designated information*. Moreover, this pamphlet states what information FINTRAC uses in its analysis, who must report transaction data to FINTRAC, what type of transactions are reported, and what triggers a FINTRAC case. This pamphlet closes by stating "Where appropriate, financial intelligence pertaining to suspected cases of money laundering, terrorist activity financing, or threats to the security of Canada is disclosed." (pg.11) Those disclosures are provided to "intelligence/enforcement agencies, foreign FIUs, Canada Revenue Agency, and Canada Border Services Agency" (pg 11).

FINTRAC Connecting the Money to the Crime – pamphlet

Disclosure is certainly at the heart of what FINTRAC is mandated / legislated to do. Simply put, FINTRAC is "a government agency created to collect, analyse, and disclose financial intelligence on suspected money laundering and terrorist financing activities".

However, "FINTRAC is an independent agency, operating at arm's length from the police and other departments and agencies of government to whom it can provide financial intelligence". This pamphlet echoes sentiments found in FINTRAC Annual Reports, legislation, and other publically available sources. The messaging is consistent across these various forums. For example, the pamphlet goes on to state:

> FINTRAC collects reports on financial transactions from numerous entities and subjects them to rigorous analysis. These reports contain information on suspicious or large cash financial transactions, international electronic funds transfers, as well as on the cross-border movements of currency and monetary instruments. When FINTRAC determines, on the basis of its analysis, that there are reasonable grounds to suspect its information would be relevant to investigating or prosecuting a money laundering or terrorist financing offence, it will disclose key identifying information to law enforcement. In addition, when it also suspects the information would be relevant to a tax or duty evasion offence, FINTRAC will disclose it to the Canada Revenue Agency or the Canada Border Services Agency, as applicable. Similarly, when it suspects the information would also be relevant to the Communications Security Establishment's (CSE) mandate, FINTRAC will disclose it to CSE. Likewise, when it suspects that any information, whether related to money laundering or terrorist financing, would be relevant to threats to the security of Canada, it will disclose the information to CSIS.

Qualitative Assessments

The following qualitative assessments were completed by the author based upon his exposure to the subject matter by going through the legislation manually. Each quality was assessed against the previously established parameters discussed in Appendix 3. Moreover, Appendix 3 describes each code. Essentially, the numbering refers to the item, and the letter refers to the strength of the tie. For example, 1 – B translates to under the legislation section, the departments or agencies in question have formally stated information sharing is a secondary or tertiary priority, perhaps not directly linked to their primary mandate. Also the qualitative assessment was partly built upon the results of the quantitative assessment, as well as the work done manually examining the documents

mentioned in the references section, and particularly the documents examined (as stated in Appendix 1).

Legislation

From

CSIS		1 - B	1 - B	1 - B	1 - B
RCMP	1 - C		1 - B	1 - C	1 - C
FINTRAC	1 - B	1 - B		1 - B	1 - B
CBSA	1 - B	1 - B	1 - B		1 - C
CRA	1 - B	1 - B	1 - B	1 - B	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Mandate

From

CSIS		2 - A	2 - A	2 - A	2 - A
RCMP	2 - B		2 - B	2 -D	2 - D
FINTRAC	2 - A	2 -A		2 - A	2 - A
CBSA	2 - B	2 - B	2 - A		2 - D
CRA	2 - B	2 - B	2 - B	2 - D	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Priorities

From

CSIS		3 - B	3 - B	3 - B	3 - B
RCMP	3 - D		3 - B	3 - D	3 - D
FINTRAC	3 - A	3 - A		3 - A	3 - A
CBSA	3 - D	3 - D	3 - B		3 - D
CRA	3 - B	3 - B	3 - B	3 - D	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Inter-Governmental Working Groups
Inter-Governmental Expert Groups (IEGs)
Joint Management Groups
Joint Intelligence Groups (JIGs)

From

CSIS		4 - D	4 - D	4 - D	4 - D
RCMP	4 - D		4 - D	4 - D	4 - D
FINTRAC	4 - D	4 - D		4 - D	4 - D
CBSA	4 - D	4 - D	4 - D		4 - D
CRA	4 - D	4 - D	4 - D	4 - D	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Working level collaboration

From

CSIS		5 - D	5 - D	5 - D	5 - D	
RCMP	5 - D		5 - D	5 - D	5 - D	
FINTRAC	5 - D	5 - D		5 - D	5 - D	
CBSA	5 - D	5 - D	5 - D		5 - D	
CRA	5 - D	5 - D	5 - D	5 - D		
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**	**To**

Process

From

CSIS		6 - A	6 - A	6 - A	6 - A	
RCMP	6 - B		6 - A	6 - D	6 - D	
FINTRAC	6 - A	6 - A		6 - A	6 - A	
CBSA	6 - B	6 - B	6 - A		6 - D	
CRA	6 - A	6 - A	6 - A	6 - D		
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**	**To**

Threshold

From

CSIS		7 - A	7 - A	7 - A	7 - A
RCMP	7 - A		7 - A	7 - A	7 - A
FINTRAC	7 - A	7 - A		7 - A	7 - A
CBSA	7 - D	7 - D	7 - A		7 - D
CRA	7 - A	7 - A	7 - A	7 - D	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Secondment(s)

From

CSIS		8 - D	8 - D	8 - D	8 - D
RCMP	8 - D		8 - D	8 - D	8 - D
FINTRAC	8 - D	8 - D		8 - D	8 - D
CBSA	8 - D	8 - D	8 - D		8 - D
CRA	8 - D	8 - D	8 - D	8 - D	
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**

To

Liaison(s)

From

CSIS		9 - D	9 - D	9 - D	9 - D	
RCMP	9 - D		9 - D	9 - D	9 - D	
FINTRAC	9 - D	9 - D		9 - D	9 - D	
CBSA	9 - D	9 - D	9 - D		9 - D	
CRA	9 - D	9 - D	9 - D	9 - D		
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**	**To**

Educational Exchanges

From

CSIS		10 - D	10 - D	10 - D	10 - D	
RCMP	10 - D		10 - D	10 - D	10 - D	
FINTRAC	10 - D	10 - D		10 - D	10 - D	
CBSA	10 - D	10 - D	10 - D		10 - D	
CRA	10 - D	10 - D	10 - D	10 - D		
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**	**To**

Memorandum of Understanding (MOUs)

From

CSIS		11 - D	11 - D	11 - D	11 - D	
RCMP	11 - D		11 - D	11 - D	11 - D	
FINTRAC	11 - D	11 - D		11 - D	11 - D	
CBSA	11 - D	11 - D	11 - D		11 - D	
CRA	11 - D	11 - D	11 - D	11 - D		
	CSIS	**RCMP**	**FINTRAC**	**CBSA**	**CRA**	**To**

Chapter 6 – DISCUSSION AND IMPLICATIONS

An effective anti money laundering (ML) / counter threat financing (TF) (AML/CTF) regime is one that the various departments and agencies of government mandated to prevent, detect, and deter money laundering and terrorist (or "threat") financing also work with the private sector and educate the public writ large. Numerous entities, for example banks and financial institutions have a legal responsibility under Canadian law to help in the prevention, detection, and deterrence of ML and TF. A transparent dialogue between all stakeholders can only help to improve the AML/CTF regime in Canada. Overall, Canada is mostly compliant with the recommendations offered by the Financial Action Task Force (Financial Action Task Force, 2008). The writer also assesses that the Canadian AML/CTF regime has the legislation in place to effectively share information. However, without detailed information concerning the implementation and use of that legislation, it is impossible to absolutely confirm the AML/CTF regimes' information sharing effectiveness. More research and analysis would be beneficial in that regard.

An issue with the Financial Action Task Force (FATF), and more specifically concerning the 49 recommendations to combat money laundering and terrorist financing is that no member of the FATF is fully compliant with all the recommendations; this includes the founding members of FATF (of which Canada is one). Many of these recommendations concern the sharing of information. Is this simply hypocritical? Or is FATF setting the ideal example for countries to strive for? It seems this is a complicated, and often political, issue that goes beyond simple hypocrisy. Consider that the legislative and legal environments vary considerably from country to country. For example, Canada has taken a strong stance protecting individual rights and freedoms, as enshrined in the *Constitution*

and the *Charter of Rights and Freedoms*. Not all countries share these type of documents nor collective values.

Other concerns involving specifically the FINTRAC and the definition of "designated information". It may prove useful and helpful for the definition to "designated information" to be broadened. This would require a legislative amendment to the PC(ML)TFA, which is currently being considered as part of the legislated review of the PC(ML)TFA.

Currently, the term "terrorist financing" is used to describe the funds utilized, or potentially used, for terrorist related activity. The writer offers that perhaps an alternative term to "financing" be used, as to broaden the interpretation / understanding of "threat financing" or "threat resourcing" to encompass not only what is typically considered terrorist activity (e.g. bombs going off), but also threat procurement of dual use goods, or goods procured by or on behalf of sanctioned governments, groups and individuals.

The Canadian Security Intelligence Service (CSIS)

The Canadian Security Intelligence Service (CSIS) has the authority to disclose or share information with a variety of government departments and agencies at both the federal and provincial levels. The CSIS is not obliged to share information. There are several review bodies (the Security Intelligence Review Committee, the Inspector General, possibly other internal mechanisms yet to be identified) that are charged with ensuring the CSIS acts in accordance with all applicable laws and directs its activities to fulfill government and Ministerial direction. The CSIS is an integral component of the AML/CTF regime in Canada, and although outside of the scope of this research plays a

role in Canada's international commitments in tackling the world wide concerns of money laundering and terrorist financing.

The Royal Canadian Mounted Police (RCMP)

It is worth noting that along with the CSIS, the RCMP is often the recipient of information concerning suspected money laundering, terrorist financing, and threat resourcing. It appears the RCMP is quite often the recipient of information, and often the sharing of information with the RCMP is legally required in certain circumstances.

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

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has an important role in the detection of money laundering, terrorist financing, and threat resourcing. However, the Centre is bound by legislation and privacy constraints, to only disclose information when it is suspected that it might assist a designated law enforcement or intelligence service in them fulfilling their mandates. And only certain information (designated information) will be disclosed.

Outstanding Issues and Future Research

It is hoped this report will be useful as an introduction to the AML/CTF regime in Canada. It is believed that an educated public debate on security issues, and the stability of our financial system are important to all Canadians, but particularly important to many business people in many sectors. As highlighted by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as the many public documents released by FINTRAC, there are many sections that have reporting requirements, notably the

financial services industry, the real estate industry, and gambling industry to name just a few.

As this research and analysis is exploratory in scope, numerous outstanding questions remain that may be answered with further study. For example:

- What is potentially contained in a security assessment? Could money laundering and terrorist financing be components of these security assessments?
- Expanded examination of secondary and tertiary departments and agencies involved in the AML/CTF regime in Canada.

Moreover, numerous additional areas may benefit from further study, for example:

- Information sharing from a strategic perspective between Canadian domestic departments and agencies involved in the AML/CTF regime.
- Information sharing with foreign governments and non-governmental organizations, at either the tactical or the strategic level.

GLOSSARY

AML – Anti money laundering

Casino Disbursement Report (CDR) – "A report that a casino covered by the PCMLTFA must file with FINTRAC when it makes a disbursement of $10,000 or more in the course of a single transaction, or when it makes two or more disbursements totalling $10,000 or more that it knows were made within 24 consecutive hours on behalf of the same individual or entity." (FINTRAC Annual Report, 2010)

Cooperative Credit Associations – "Are set up under the *Cooperative Credit Associations Act*, and is an association that is organized and operated on cooperative principles, with one of its principal purposes being to provide financial services to its members." (OSFI website)

Cross-Border Currency Report (CBCR) – "A report that must be filed with the CBSA by a person entering or leaving Canada advising that the person is carrying large sums of currency or monetary instruments ($10,000 or more), or by a person mailing or sending such large sums into or out of Canada." (FINTRAC Annual Report, 2010)

Cross-Border Seizure Report (CBSR) – "A report filed with FINTRAC by a CBSA officer who seizes cash or monetary instruments for which reporting obligations were not met." (FINTRAC Annual Report, 2010)

CTF – Counter terrorist financing

Domestic Banks – "Institutions regulated by the *Bank Act*." (OSFI website)

Electronic Funds Transfer Report (EFTR) – "A report that a reporting entity must file with FINTRAC in respect of a transmission of instructions for the transfer of $10,000 or more out of or into Canada in a single transaction or in two or more transactions totalling

$10,000 or more that it knows were made within 24 consecutive hours of each other by or on behalf of the same individual or entity, through any electronic, magnetic or optical device, telephone instrument or computer." (FINTRAC Annual Report, 2010)

Foreign Banks – "Foreign banks are subsidiaries regulated under the *Bank Act*. Foreign bank subsidiaries are controlled by eligible foreign institutions." (OSFI website)

Foreign Bank Branches (Full Service) – "Are foreign banks that have been authorized under the *Bank Act* to establish branches in Canada to carry on banking business in Canada. Generally, these foreign banks may not in Canada accept deposits of less than $150,000." (OSFI website)

Foreign Bank Branches (Lending) – "Are foreign banks that have been authorized under the *Bank Act* to establish branches in Canada to carry on banking business in Canada. Generally, these foreign banks may not in Canada accept deposits of less than $150,000." (OSFI website)

Large Cash Transaction Report (LCTR) – "A report that a reporting entity must file with FINTRAC when it receives $10,000 or more in cash in the course of a single transaction, or when it receives two or more cash amounts totalling $10,000 or more that it knows were made within 24 consecutive hours of each other by or on behalf of the same individual or entity." (FINTRAC Annual Report, 2010)

Loan Companies – "Are financial institutions that operate under either provincial or federal legislation and conducts activities similar to those of a bank." (OSFI website)

Suspicious Transaction Report (STR) – "A report that a reporting entity must file with FINTRAC in respect of a financial transaction that occurs or that is attempted in the course of its activities and for which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering

or terrorist activity financing offence." (FINTRAC Annual Report, 2010)

Trust Companies – "Are financial institutions that operate under either provincial or federal legislation and conducts activities similar to those of a bank. However, because of its fiduciary role, a trust company can administer estates, trusts, pension plans and agency contracts, which banks are not permitted to administer." (OSFI website)

Voluntary Information Record (VIR) – "A record of information voluntarily submitted to FINTRAC about suspicions of money laundering or of the financing of terrorist activities." (FINTRAC Annual Report, 2010)

APPENDIX 1 – AGENCIES & DOCUMENTS EXAMINED

It is important to consider that this study is exploratory in nature. As such, not all domestic departments and agencies that may be involved in the AML/CTF regime in Canada may have been examined in this research and analysis. Moreover, not all relevant documents have been coded and examined.

List of agencies examined

- Canadian Security Intelligence Service (CSIS)
- Royal Canadian Mounted Police (RCMP)
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
- Canada Border Services Agency (CBSA)
- Canada Revenue Agency (CRA)

List of documents examined

- FINTRAC Annual Report 2011
- CSIS Public Report 2009-2010
- *Canadian Security Intelligence Service Act (C-23)*
- *Criminal Code (C-46)*
- *Proceeds of Crime (Money Laundering) Terrorist Financing Act*
- FINTRAC Pamphlets
    - Sharing Intelligence – Making The Links
    - Connecting the Money to the Crime

APPENDIX 2 – CODING: TERMS, WORDS, EXPRESSIONS

The following terms, words, and expressions were identified and associated to strong (positive), weak (quasi-positive) or a negative indication of information sharing between the various domestic AML/CTF regime partners in Canada.

These terms, words, and expressions formed the basis of the coding section of this research and analysis. For each of the documents that were coded, each of these terms were searched, located, documented, and counted. The interpretation of the results can be found in the quantitative results section under the assessments chapter.

The coding forms were separated into positive terms (terms which suggest a strong information sharing relationship), quasi-positive terms (terms which suggest a weak information sharing relationship), and negative terms (terms which suggest a negative information sharing relationship).

Strong indication of information sharing:

- Disclosure
- Disclose
- Advice
- Advise
- Recommendation
- Suggestion
- Direction
- Cooperation
- Formal

- Partnership
- Relationship
- Memorandum of Understanding
- Mandate
- Lawful
- Query
- Involuntary (disclosure...)
- Report
- Provide
- Agreement
- Share
- Guidance
- Sharing

Weak indication of information sharing:

- Mutual (training, management)
- Informal
- Collaborate
- Voluntary disclosure
- Choice
- Option
- Ability
- Joint (training, management)
- Meeting

Negative indication of information sharing:

- Prohibited
- Not allowed
- Discouraged
- Illegal
- Unconstitutional
- Unlawful
- Discourage
- Arms length
- Privacy
- Non-disclosure

APPENDIX 3 – CODING LEGEND

Coding Legend

1 = Legislation

2 = Mandate

3 = Priorities

4 = Inter-Governmental Working Groups (IGWGs), Inter-Governmental Expert Groups (IGEGs), Joint Management Groups (JMG), and Joint Intelligence Groups (JIGs)

5 = Working level collaboration

6 = Process

7 = Threshold

8 = Secondment(s)

9 = Liaison(s)

10 = Educational exchanges

11 = Memorandum of Understanding

A = Strong Tie

B = Weak Tie

C = Absent Tie

D = Unknown Tie

Strong Ties

1-A = Yes, the departments or agencies are formally allowed to share information (by legislation).

2-A = Yes, the departments or agencies are formally mandated (must) to share information (by legislation).

3-A = Yes, the departments or agencies have formally stated information sharing is a top priority.

4-A = Yes, the departments or agencies have formal IGWGs, IGEGs, JMGs, and JIGs.

5-A = Yes, the departments or agencies allow formal working level collaboration.

6-A = Yes, the departments or agencies have strategically established information sharing as a process.

7-A = Yes, the departments or agencies have a formal test (threshold) that must be met to share information.

8-A = Yes, the departments or agencies have a formal secondment currently staffed.

9-A = Yes, the departments or agencies have a formal liaison relationship currently staffed.

10-A = Yes, the departments or agencies engage in formal exchanges of expertise (e.g. training courses offered to partner agencies and departments).

11-A = Yes, the departments or agencies have a formal MOU in place which formalizes the relationship (information sharing must be a component) between signatory departments or agencies.

Weak Ties

1-B = The departments or agencies legislation allows, even directs that department or agency to share information, however that information sharing can only be done under strict conditions and circumstances (by legislation).

2-B = The departments or agencies are formally allowed (can) to share information (by legislation).

3-B = The departments or agencies have formally stated information sharing is a secondary or tertiary priority, perhaps not directly linked to their primary mandate.

4-B = The departments or agencies have formal IGWGs, IGEGs, JMGs, and JIGs - however they meet irregularly, inconsistently, or perhaps on a case by case basis.

5-B = The departments or agencies allow formal working level collaboration, however these relationships are not necessarily encouraged.

6-B = The departments or agencies have strategically established information sharing as a process, however this is a possible component or outcome to their overall mandate.

7-B = The departments or agencies require a judicial order (warrant) that must be provided to share information.

8-B = The departments or agencies have a formal secondment, but this position is not currently staffed.

9-B = The departments or agencies have a formal liaison relationship, but this position is not currently staffed.

10-B = The departments or agencies engage in formal exchanges of expertise (e.g. training courses offered to partner agencies and departments), however these exchanges exist only as an exception.

11-B = The departments or agencies have a formal MOU in place which formalizes the relationship (information sharing can be a component) between signatory departments or agencies.

Absent Ties

1-C = The departments or agencies are have no legislated provision allowing them to share information (by legislation).

2-C = The departments or agencies are formally prohibited to share information (by legislation).

3-C = The departments or agencies have formally stated information sharing is not a top priority.

4-C = The departments or agencies are prohibited from, or do not engage in, IGWGs, IGEGs, JMGs, and JIGs.

5-C = The departments or agencies prohibit formal working level collaboration, or it does not occur.

6-C = The departments or agencies do not have strategically established information sharing protocols as a process.

7-C = The departments or agencies do not have a formal test (threshold) because they are prohibited from sharing information.

8-C = The departments or agencies do not have a formal secondment provision.

9-C = The departments or agencies do not have a formal liaison provision.

10-C = The departments or agencies do not engage in formal exchanges of expertise (e.g. training courses offered to partner agencies and departments).

11-C = The departments or agencies do not have a formal MOU in place.

Unknown Ties

1-D = There is not sufficient information to determine whether the departments or agencies are formally allowed to share information (by legislation).

2-D = There is not sufficient information to determine whether the departments or agencies are formally mandated to share information (by legislation).

3-D = There is not sufficient information to determine whether the departments or agencies have formally stated information sharing is a top priority.

4-D = There is not sufficient information to determine whether the departments or agencies have formal IGWGs, IGEGs, JMGs, and JIGs.

5-D = There is not sufficient information to determine whether the departments or agencies allow formal working level collaboration.

6-D = There is not sufficient information to determine whether the departments or agencies have strategically established information sharing in process.

7-D = There is not sufficient information to determine whether the departments or agencies have a formal test (threshold) that must be met to share information.

8-D = There is not sufficient information to determine whether the departments or agencies have a formal secondment currently staffed.

9-D = There is not sufficient information to determine whether the departments or agencies have a formal liaison relationship currently staffed.

10-D = There is not sufficient information to determine whether the departments or agencies engage in formal exchanges of expertise (e.g. training courses offered to partner agencies and departments).

11-D = There is not sufficient information to determine whether the departments or agencies have a formal MOU in place which formalizes the relationship (information sharing must be a component) between signatory departments or agencies.

APPENDIX 4 – CODING FORMS

Criminal Code of Canada

Positive

Document: *Criminal Code of Canada*
Date: January 4, 2012
Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		83.05(6)(a); 83.05(6)(b); 83.06(1)(b); 83.06(3); 83.1(2); 83.12(2); 83.31(4); 462.48(1.1); 462.48(6); 462.48(6)(d); 462.48(7); 462.48(8); 462.48(12)(b).
Disclose		Y		83.06(1)(b); 83.06(3); 83.1(1); 83.28(8); 462.48(6); 462.48(15).
Advice		N		N/A
Advise		N		N/A
Recommendation		Y		83.05(1); 83.05(1.1); 83.05(9).
Suggestion		N		N/A
Direction		Y		83.05(1)(b); 83.08(1)(c); 83.13(2)(a); 83.18(3)(b); 83.13(3)(d); 83.2; 83.21(1); 83.21(2)(d); 462.31(3); 462.331(1)(a).
Cooperation		N		N/A
Formal		N		N/A
Partnership		Y		83.01(1).
Relationship		N		N/A
Memorandum of Understanding		N		N/A
Mandate		N		N/A
Lawful		Y		83.02; 83.231(1); 450; 451; 452; 454; 458; 459; 462.32(4.1); 462.32(4.1)(a); 462.34(4)(c); 462.34(6)(b); 462.41(3); 462.43(c)(i); 462.43(c)(ii); 462.43(c)(iii).

Query		N		N/A
Involuntary (disclosure...)		N		N/A
Report		Y		83.05(6)(a); 83.11(2); 83.11(2)(b); 83.11(3); 83.11(4)(a); 83.31(1); 83.31(2); 83.31(3); 83.31(4); 462.32(4)(b); 462.32(4)(c); 462.32(4.1)(c); 462.36.
Provide		Y		83.02; 83.03; 83.05(6)(a); 83.05(6)(c); 83.06(1)(b); 83.06(2)(b); 83.08(1)(c); 83.11(1)(g); 83.13(1.1); 83.13(7); 83.14(2); 83.14(4); 83.18(3)(b); 462.32(4)(c); 462.45(a); 462.48(14); 462.48(15).
Agreement		Y		462.48(6)(a).
Share		N		N/A
Guidance		N		N/A
Sharing		N		N/A

Quasi-Positive

Document: *Criminal Code of Canada*

Date: January 4, 2012

Coder: Andrew Ross

Quasi positive terms (allowing information sharing under certain circumstances)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Mutual (training, management)		N		N/A
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A
Option		N		N/A
Ability		Y		83.18(1); 83.18(2)(b); 83.21(1); 83.21(2)(f).
Joint (training, management)		N		N/A
Meeting		N		462.34(4)(c)(i); 462.34(4)(c)(ii).

Negative

Document: *Criminal Code of Canada*
Date: January 4, 2012
Coder: Andrew Ross

Negative terms (prohibiting information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Prohibited		Y		83.09(1); 83.3(10); 462.1; 462.48(6)(a).
Not allowed		N		N/A
Discourage		N		N/A
Illegal		N		N/A
Unconstitutional		N		N/A
Unlawful		Y		83.01(1)(a)(i); 83.01(1)(a)(ii); 83.01(1)(a)(vi); 83.01(1)(a)(vii); 83.01(1)(a)(viii); 462.43(1)(c)(ii); 462.43(1)(c)(iii).
Discourage		N		N/A
Arms length		N		N/A
Privacy		N		N/A
Non-disclosure		Y		83.28(8).

CSIS Act

Positive

Document: *Canadian Security Intelligence Service Act*
Date: Dec 05, 2011
Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		Sections 19, 19(2)(d), 19(3), 25(a), 25(b)
Disclose		Y		Sections 18(1), 18(2), 19(1), 19(2), OATH OF SECRECY
Advice		Y		Sections 7(3), 14, 15
Advise		Y		Sections 7(3), 12, 14(a)
Recommendation		Y		Sections 52(1)(a), 52(2)

Suggestion		N		N/A
Direction		Y		Sections 6(1), 6(2), 6(3), 7(1)(a), 7(3), 33(2)(a), 38(a)(ii), 40
Cooperation		Y		Section 17
Formal		N		N/A
Partnership		N		N/A
Relationship		N		N/A
Memorandum of Understanding		N		N/A
Mandate		N		N/A
Lawful		Y		Section 2(d)(note)
Query		N		N/A
Involuntary (disclosure...)		N		N/A
Report		Y		Sections 12, 19(3), 20(2), 20(3), 31, 33(1), 33(2), 33(3), 38(a)(i), 38(a)(iv), 38(c)(ii), 39(2)(a), 40(a), 52(1)(a), 52(1)(b), 52(2), 53, 54, 55(b), 56(2),
Provide		Y		Sections 5(2), 8(1)(a), 13(1), 13(2)(b), 13(3), 14(b), 16(2), 40(a), 42(2), 42(3)(b), 52(1)(a), 52(1)(b), 52(2),
Agreement		N		N/A
Share		N		N/A
Guidance		N		N/A
Sharing		N		N/A

Quasi-Positive

Document: *Canadian Security Intelligence Service Act*
Date: 2011 12 05
Coder: Andrew Ross

Quasi positive terms (allowing information sharing under certain circumstances)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Mutual (training, management)		N		N/A
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A

Option		N		N/A
Ability		N		N/A
Joint (training, management)		N		N/A
Meeting		N		N/A

Negative

Document: *Canadian Security Intelligence Service Act*
Date: Dec 05, 2011
Coder: Andrew Ross

Negative terms (prohibiting information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Prohibited		N		N/A
Not allowed		Y		Section 42(4)
Discourage		N		N/A
Illegal		N		N/A
Unconstitutional		N		N/A
Unlawful		Y		Sections 2("threats")(d), 20(2)
Discourage		N		N/A
Arms length		N		N/A
Privacy		Y		Section 19(2)(d)
Non-disclosure		N		N/A

CSIS Public Report 2009/2010

Positive

Legend: P=page number, Pg = Paragraph number, L=Line number

Document: *CSIS Public Report 2009/2010*
Date: Dec 26, 2011
Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		P45Pg6L3.
Disclose		N		N/A

Advice		Y		P4Pg1L4; P24Pg1L6; P29Pg3L3; P44Pg2L4; P46Pg1L4.
Advise		Y		P4Pg3L2.
Recommendation		Y		P31Pg3L3; P43Pg4L7; P43Pg4L10; P43Pg4L11; P47Pg2L2; P47aPg2L3; P47Pg5L3.
Suggestion		N		N/A
Direction		Y		P12Pg1L7; P29Pg2L3; P30Pg1L5; P35Pg3L5; P43Pg3L2.
Cooperation		Y		P27Pg1L1; P27Pg1L3; P27Pg4L4; P30Pg5L4.
Formal		Y		P14Pg2L1.
Partnership		Y		P37Pg2L4; P52Pg4L8.
Relationship		Y		P5Pg1L5; P30Pg3L2; P31Pg2L5; P31Pg5L4; P32Pg0L2; P44Pg3L8; P52Pg1L4.
Memorandum of Understanding		N		N/A
Mandate		Y		P18Pg0L4; Pg27Pg1L2; P28Pg3L3; P30Pg1L2; P31Pg5L6; P44Pg4L1; P50Pg2L4; P51Pg1L7;
Lawful		N		N/A
Query		N		N/A
Involuntary (disclosure...)		N		N/A
Report		Y		P6Pg1L3; P6Pg1L4; P17Pg4L1; P18Pg3L1; P27Pg4L6; P28Pg1L7; P28Pg2L1; P28Pg2L2; P28Pg3L3; P28Pg3L5; P28Pg4L2; P28Pg4L3; P32Pg1L2; P34Pg1L4; P43Pg1L4; P43Pg4L2; P44Pg1L1; P46Pg1L2; P46Pg3L3; P47Pg2L2; P50Pg1L2; P50Pg2L1; P50Pg2L11.

Provide		Y		P1Pg1L6; P5Pg1L3; P14Pg1L4; P23Pg3L3; P23Pg4L2; P23Pg5L1; P23Pg5L6; P24Pg1L6; P25Pg1L5; P27Pg3L5; P28Pg1L5; P28Pg3L1; P30Pg1L5; P31Pg2L6; P31Pg2L7; P31Pg4L3; P32Pg1L1; P35Pg1L5; P40Pg1L7; P43Pg4L7; P44Pg1L2; P44Pg4L6; P45Pg3L4; P46Pg1L3; P47Pg1L5; P50Pg2L8; P50Pg2L12; P51Pg2L3; P52Pg1L5; P52Pg1L7.
Agreement		Y		P14Pg4L5; P23Pg5L1; P23Pg5L6; P30Pg5L5.
Share		Y		P27Pg4L1; P31Pg2L1; P31Pg3L4; P47Pg2L1; P52Pg1L6; P53Pg2L6.
Guidance		Y		P29Pg3L3; P46Pg1L4.
Sharing		Y		P12Pg4L2; P30Pg1L4.

Quasi-Positive

Document: *CSIS Public Report 2009/2010*
Date: Dec 26, 2011
Coder: Andrew Ross

Legend: P=page number, Pg = Paragraph number, L=Line number

Quasi positive terms (allowing information sharing under certain circumstances)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Mutual (training, management)		Y		P13Pg4L7; P27Pg2L8; P52Pg4L12.
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		Y		P34Pg3L6.
Option		N		N/A
Ability		Y		P13Pg4L4; P32Pg0L1.
Joint (training, management)		N		N/A
Meeting		N		N/A

Negative

Document: *CSIS Public Report 2009/2010*
Date: Dec 26, 2011
Coder: Andrew Ross

Legend: P=page number, Pg = Paragraph number, L=Line number

Negative terms (prohibiting information sharing)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Prohibited		N		N/A
Not allowed		N		N/A
Discourage		N		N/A
Illegal		Y		P15Pg2L9; P15Pg4L9.
Unconstitutional		N		N/A
Unlawful		N		N/A
Discourage		N		N/A
Arms length		N		N/A
Privacy		Y		P31Pg2L2; P43Pg1L8; P45Pg1L2; P45Pg2L1; P45Pg6L1.
Non-disclosure		N		N/A

FINTRAC Annual Report 2011

Positive

Document: *FINTRAC Annual Report 2011*
Date: February 5, 2012
Coder: Andrew Ross

Legend: P=page number, Pg = Paragraph number, L=Line number

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		P9Pg1L4; P9Pg2L4; P10Pg1L1; P10Pg2L2; P10Pg4L2; P12Pg6L3; P13Pg1L5; P13Pg2L1; P13Pg2L4; P13Pg4L3; P14Pg1L1; P14Pg1L3; P14Pg3L1; P14Pg5L2; P14Pg6L1; P14Pg6L2; P14Pg6L4; P15Pg1L1; P15Pg1L3; P15Pg1L9; P15Pg2L1; P15Pg3L1; P15Pg3L5; P15Pg3L7; P16Pg1L1; P16Pg1L2; P17Pg2L1; P17Pg2L3; P18Pg1L1; P19Pg1L3; P20Pg1L1; P20Pg1L3; P20Pg18L2; P20Pg20L2; P20Pg21L1; P20Pg21L5; P23Pg4L3; P25Pg1L5; P29Pg1L5; P34Pg1L2; P34Pg2L5; P37Pg5L8.
Disclose		Y		P6Pg3L5; P9Pg1L5; P13Pg2L2; P13Pg7L4; P14Pg3L4; P28Pg5L2; P37Pg5L1.
Advice		N		N/A
Advise		N		N/A
Recommendation		Y		P2Pg5L2; P32Pg6L3.
Suggestion		N		N/A
Direction		N		N/A
Cooperation		Y		P13Pg8L5; P14Pg9L7.

Formal		Y		P33Pg6L1.
Partnership		Y		P28Pg6L1.
Relationship		Y		P2Pg3L1; P18Pg2L1; P20Pg15L1; P32Pg1L4.
Memorandum of Understanding		Y		P19Pg1L4; P28Pg6L2; P28Pg6L3.
Mandate		Y		P4Pg1L1; P4Pg1L4; P5Pg1L1; P12Pg1L5; P33Pg2L3; P36Pg3L1; P37Pg5L5.
Lawful		Y		P37Pg8L9.
Query		Y		P21Pg1L1.
Involuntary (disclosure...)		N		N/A
Report		Y		P2Pg3L1; P3Pg1L1; P3Pg1L3; P9Pg1L5; P10Pg3L2; P10Pg3L3; P10Pg5L1; P12Pg4L3; P12Pg4L4; P12Pg5L1; P12Pg5L2; P12Pg5L3; P12Pg5L4; P12Pg6L1; P13Pg3L2; P13Pg6L1; P14Pg2L4; P20Pg18L3; P20Pg19L1; P20Pg20L2; P21Pg2L6; P22Pg2L1; P22Pg3L1; P22Pg3L2; P23Pg4L3; P23Pg6L2; P23Pg6L4; P23Pg6L5; P23Pg7L1; P24Pg1L4; P24Pg1L5; P24Pg3L1; P24Pg3L4; P24Pg4L2; P25Pg1L1; P25Pg1L3; P25Pg1L5; P25Pg2L2; P25Pg2L3; P25Pg3L3; P25Pg4L2; P25Pg5L1; P25Pg5L2; P28Pg1L5; P28Pg2L1; P28Pg2L3; P28Pg4L2; P28Pg4L3; P28Pg5L3; P28Pg5L8; P28Pg6L7; P29Pg1L2; P29Pg2L1; P29Pg2L2; P29Pg2L3; P29Pg3L2; P29Pg4L2; P29Pg5L4; P30Pg1L5; P30Pg1L9; P30Pg2L3; P30Pg3L1; P30Pg3L2; P30Pg3L6; P30Pg3L8; P30Pg3L10;

				P30Pg3L11; P31Pg1L1; P31Pg1L6; P34Pg2L1; P34Pg4L4; P34Pg4L5; P34Pg5L3; P35Pg2L3; P36Pg3L1; P36Pg4L1; P36Pg5L1; P36Pg6L1; P36Pg6L2; P36Pg8L1; P37Pg3L2; P37Pg4L1; P37Pg7L1.
Provide		Y		P3Pg1L3; P7Pg2L3; P12Pg2L3; P13Pg1L1; P13Pg1L2; P13Pg1L3; P14Pg2L3; P14Pg4L1; P14Pg5L6; P14Pg7L1; P14Pg8L1; P14Pg8L5; P14Pg9L1; P15Pg1L3; P17Pg2L3; P24Pg3L4; P24Pg4L5; P24P5L4; P28Pg4L4; P29Pg5L2; P32Pg5L3; P33Pg4L6; P34Pg4L6; P35Pg3L2; P37Pg1L2; P37Pg2L2.
Agreement		Y		P13Pg7L4; P13Pg7L5; P13Pg7L6.
Share		Y		P17Pg1L2; P28Pg6L4; P36Pg7L2.

Guidance		N		N/A
Sharing		Y		P6Pg5L4; P13Pg8L6; P34Pg7L2.

Quasi-Positive

Document: *FINTRAC Annual Report 2011*
Date: February 5, 2012
Coder: Andrew Ross

Legend: P=page number, Pg = Paragraph number, L=Line number

Quasi positive terms (allowing information sharing under certain circumstances)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Mutual (training, management)		Y		P32Pg6L1; P38Pg4L4.
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A
Option		N		N/A
Ability		Y		P7Pg1L1.
Joint (training, management)		Y		P24Pg2L11.
Meeting		Y		P24Pg2L11.

Negative

Document: *FINTRAC Annual Report 2011*
Date: February 5, 2012
Coder: Andrew Ross

Legend: P=page number, Pg = Paragraph number, L=Line number

Negative terms (prohibiting information sharing)		**Is the searched term present? Y or N**		**Reference: Section, page number, paragraph etc...**
Prohibited		N		N/A
Not allowed		N		N/A
Discourage		N		N/A
Illegal		Y		P12Pg3L2; P17Pg2L2; P19Pg1L1.
Unconstitutional		N		N/A
Unlawful		Y		P37Pg8L9.

Discourage		N		N/A
Arms length		N		N/A
Privacy		Y		P7Pg5L3; P9Pg2L3; P9Pg3L1; P9Pg3L2; P9Pg3L3; P9Pg3L4; P9Pg3L5; P13Pg5L2.
Non-disclosure		N		N/A

FINTRAC – Connection the Money to the Crime pamphlet

Positive

Document: FINTRAC Connecting the Money to the Crime pamphlet
Date: February 8, 2012
Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		Pg5L1; Pg7L2.
Disclose		Y		Pg1L3; Pg3L9; Pg3L11; Pg3L15; Pg3L17; Pg4L5; Pg8L5.
Advice		N		N/A
Advise		N		N/A
Recommendation		N		N/A
Suggestion		N		N/A
Direction		N		N/A
Cooperation		N		N/A
Formal		Y		Pg12L12.
Partnership		N		N/A
Relationship		N		N/A
Memorandum of Understanding		N		N/A
Mandate		N		Pg3L14.
Lawful		N		N/A
Query		N		N/A
Involuntary (disclosure...)		N		N/A
Report		Y		Pg1L1; Pg3L1; Pg3L2; Pg8L2; Pg9L1; Pg11L3.
Provide		Y		Pg2L3; Pg4L2; Pg5L2; Pg8L3;

				Pg11L4; Pg16L2.
Agreement		N		N/A
Share		N		N/A
Guidance		N		N/A
Sharing		N		N/A

Quasi-Positive

Document: FINTRAC Connecting the Money to the Crime pamphlet
Date: February 8, 2012
Coder: Andrew Ross

Quasi positive terms (allowing information sharing under certain circumstances)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Mutual (training, management)		N		N/A
Informal		Y		Pg14L11.
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A
Option		N		N/A
Ability		Y		Pg6L5.
Joint (training, management)		N		N/A
Meeting		N		N/A

Negative

Document: FINTRAC Connecting the Money to the Crime pamphlet
Date: February 8, 2012
Coder: Andrew Ross

Negative terms (prohibiting information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Prohibited		N		N/A
Not allowed		N		N/A
Discourage		N		N/A
Illegal		Y		Pg10L3; Pg11L5.
Unconstitutional		N		N/A
Unlawful		Y		Pg8L5.
Discourage		N		N/A

Arms length		Y		Pg2L1; Pg4L1.
Privacy		Y		Pg8L6.
Non-disclosure		N		N/A

FINTRAC – Law Enforcement and Intelligence Partners: Sharing Intelligence and Making Connections

Positive

Document: FINTRAC, Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links

Date: February 2, 2012

Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		P4Pg6L2; P5Pg2L3; P5Pg3L1; P5Pg3L6; P6P1L1; P6Pg1L3; P7Pg2L1; P8Pg1L1; P8Pg3L1.
Disclose		Y		P4Pg6L1; P5Pg1L1; P11Pg2L5.
Advice		Y		P4Pg3L4.
Advise		N		N/A
Recommendation		N		N/A
Suggestion		N		N/A
Direction		N		N/A
Cooperation		N		N/A
Formal		N		N/A
Partnership		N		N/A
Relationship		Y		P6Pg1L11; P6Pg2L10.
Memorandum of Understanding		N		N/A
Mandate		Y		P4Pg3L1.
Lawful		N		N/A
Query		Y		P11Pg2L5.
Involuntary (disclosure...)		N		N/A

Report		Y		P4Pg1L1; P4Pg4L2; P5Pg1L1; P5Pg1L2; P7Pg8L1; P7Pg8L2; P7Pg13L2; P8Pg1L3; P8Pg1L5; P8Pg2L2; P8Pg2L3; P9Pg15L1; P9Pg19L1; P9Pg21L1; P10Pg1L2; P10Pg3L1; P10Pg4L3; P10Pg5L2; P10Pg5L4; P10Pg5L6; P10Pg5L8; P10Pg5L9; P10Pg6L2; P10Pg6L4; P11Pg1L1.
Provide		Y		P3Pg1L4; P4Pg3L2; P5Pg1L2; P5Pg2L5; P8Pg1L2; P8Pg4L1; P9Pg17L1; P9Pg18L1; P9Pg21L1; P10Pg4L3; P11Pg2L1; P12Pg1L4.
Agreement		Y		P8Pg6L1; P8Pg7L1; P8Pg7L6;
Share		Y		P5Pg4L7.
Guidance		Y		P12Pg3L1.
Sharing		Y		P8Pg7L1; P8Pg7L5.

Quasi-Positive

Document: FINTRAC, Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links

Date: February 2, 2012

Coder: Andrew Ross

Quasi positive terms (allowing information sharing under certain circumstances)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Mutual (training, management)		N		N/A
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A
Option		N		N/A
Ability		N		N/A
Joint (training, management)		N		N/A
Meeting		N		N/A

Negative

Document: FINTRAC, Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links

Date: February 2, 2012

Coder: Andrew Ross

Negative terms (prohibiting information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Prohibited		N		N/A
Not allowed		N		N/A
Discourage		N		N/A
Illegal		Y		P12Pg1L3.
Unconstitutional		N		N/A
Unlawful		N		N/A
Discourage		N		N/A
Arms length		N		N/A
Privacy		N		N/A
Non-disclosure		N		N/A

Proceeds of Crime (Money Laundering) Terrorist Financing Act (PC(ML)TFA)

Positive

Document: *PC(ML)TFA*

Date: January 11, 2012

Coder: Andrew Ross

Positive terms (allowing information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Disclosure		Y		7.1(1); 11.4(3); 40(c); 55(6); 55(7)(L); 55.1(3)(L); 56.1(5)(L); 60(L); 60(2); 60(3)(C); 60(5); 60(8).

Disclose		Y		8; 11; 36(1); 36(2); 36(3); 36(3.1); 36(4); 40(a); 40(b); 52(3); 52(4); 53; 54(e); 55(1); 55(3); 55(5.1); 55(6); 55.1(1); 55.1(2); 56(3)(b); 56.1(1); 56(2); 56.1(2.1); 56.1(3); 56.1(4); 58(2); 60(8); 60.1(7); 60.3(7); 65(1); 65(2); 65(3); 65.1(1)(c); 70(2).
Advice		N		N/A
Advise		Y		14(3)(b); 42(4); 64(10).
Recommendation		Y		67
Suggestion		N		N/A
Direction		Y		42(2); 43(3); 45(1); 45(2); 52(2); 69; 70(2).
Cooperation		N		N/A
Formal		N		N/A
Partnership		N		N/A
Relationship		Y		9.4(1); 9.4(2); 9.4(3); 55(7)(h); 55.1(3)(h); 56.1(5)(h); 73(1)(o).
Memorandum of Understanding		Y		55(2)(b).
Mandate		Y		49(3)(c); 55(f).
Lawful		Y		18(2); 25.
Query		N		N/A
Involuntary (disclosure...)		N		N/A
Report		Y		2; 3(a)(ii); 3(a)(iii); 7; 7.1(1); 8; 9(1); 9(3); 9.1; 10; 12(1); 12(2); 12(3); 12(4); 12(4)(a); 12(5); 13; 14(1); 14(3)(a); 13(4)(b); 13(5); 15(c); 16(1); 16(2); 20; 33(c); 36(1)(a); 38(1); 38(1)(a); 38(1)(b); 38(2); 38(3); 38.1; 41(1); 42(4); 52(1); 53; 54(a); 54(c); 54(d); 54(e); 55(1)(a); 55(1)(a.1); 55(1)(b); 55(1)(b.1); 55(1)(c); 55(1)(k); 55(1)(l); 55(1)(m); 55.1(1)(3)(k); 55.1(1)(3)(l); 55.1(1)(3)(m); 56.1(1)(5)(k); 56.1(1)(5)(l); 56.1(1)(5)(m); 58(1)(a); 58(2); 60(3)(c); 60.1(2)(b); 60.3(2)(c);

				65.1(1); 71(1); 71(2); 72(2); 73(1)(e.1).
Provide		Y		3(a)(i); 5(g); 9.4(3); 11.1; 11.13; 11.14(1); 11.14(2); 11.17(1); 11.17(2); 11.3(1); 24; 38(1)(a); 38(1)(b); 38.1; 49(3)(d); 51; 53; 54(a); 55(a)(b.2); 55(1)(d); 56.2; 58(1)(a); 58(2); 60(16); 60.1(15); 60.3(15); 63.1(2); 65.1(2); 65.1(3).
Agreement		Y		9.4(3); 38(1); 38(2); 38(3); 38.1; 51; 54(b); 55(2)(b); 56(1); 56(2); 56(3); 56.1(1)(b); 56.1(2)(b); 56.1(3); 56.2; 60(8)(a); 60.1(7)(a); 60.3(7)(a); 65.1(1); 65.1(2); 65.1(3); 66(1); 66(2); 66(3).
Share		Y		11.11(1)(e).
Guidance		N		N/A
Sharing		Y		60(8)(a); 60.1(7)(a); 60.3(7)(a).

Quasi-Positive

Document: *PC(ML)TFA*
Date: January 11, 2012
Coder: Andrew Ross

Quasi positive terms (allowing information sharing under certain circumstances)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Mutual (training, management)		N		N/A
Informal		N		N/A
Collaborate		N		N/A
Voluntary disclosure		N		N/A
Choice		N		N/A
Option		N		N/A
Ability		N		N/A
Joint (training, management)		N		N/A
Meeting		N		N/A

Negative

Document: *PC(ML)TFA*
Date: January 11, 2012
Coder: Andrew Ross

Negative terms (prohibiting information sharing)		Is the searched term present? Y or N		Reference: Section, page number, paragraph etc...
Prohibited		Y		55(e); 60(8)(a); 60.1(7)(a); 60.3(7)(a).
Not allowed		N		N/A
Discourage		N		N/A
Illegal		N		N/A
Unconstitutional		N		N/A
Unlawful		N		N/A
Discourage		N		N/A
Arms length		N		N/A
Privacy		Y		3(b); 36(1); 36(5); 54(d); 54.1(6); 55(1); 59(1); 60(1); 72(2).
Non-disclosure		N		N/A

REFERENCES

- Granovetter, Mark S. (1973). The Strength of Weak Ties. *American Journal of Sociology, Volume 78, Issue 6*, 1360-1380.
- Granovetter, Mark S. (1983). The Strength of Weak Ties: A network theory revisited. *Sociological Theory 1,* 201–233.
- Neuendorf, Kimberly A. (2002). *The content analysis guidebook.* California: Sage Publications Inc.
- Holsti, Ole R. (1969). *Content Analysis for the Social Sciences and Humanities.* Don Mills, Ontario: Addison Wesley Publishing Company.
- Ruef, Martin. (2002). Strong ties, weak ties and islands: structural and cultural predictors of organisational innovation. *Industrial and Corporate Change, Volume 2, Number 3*, 427-449.
- Speaking Notes (2011). *2011 CASIS International Conference, 10 November 2011, Fairmont Chateau Laurier Hotel, Ottawa, Canada*. Retrieved July 17, 2011, from http://www.csis.gc.ca/nwsrm/spchs/spch10112011-eng.asp
- Canada. Parliament of Canada. (2000). *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (c.17)*. Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/P-24.501/index.html.
- Canada. Parliament of Canada. (2002). *Cross-border Currency and Monetary Instruments Reporting Regulations (SOR/2002-412).* Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/SOR-2002-412/index.html.
- Canada. Parliament of Canada. (2007). *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations*

(SOR/2007-292). Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/SOR-2007-292/index.html.

- Canada. Parliament of Canada. (2007). *Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations (SOR/2007-121).* Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/SOR-2007-121/index.html.
- Canada. Parliament of Canada. (2002). *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184).* Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/SOR-2002-184/index.html.
- Canada. Parliament of Canada. (2001). *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (SOR/2001-317).* Retrieved November 30, 2010, from http://laws.justice.gc.ca/eng/SOR-2001-317/index.html.
- United Nations. (1999). *International Convention for the Suppression of the Financing of Terrorism.* Retrieved on February 22, 2010, from http://treaties.un.org/doc/db/Terrorism/english-18-11.pdf.
- Canada. The Office of the Superintendent of Financial Institutions (OSFI). (2012). *Who We Regulate – listing.* Retrieved February 28, 2012, from http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?DetailID=568.
- Canada. The Communications Security Establishment Canada (CSEC). (2011). *Parliamentary Accountability.* Retrieved August 3, 2011, from http://www.cse-cst.gc.ca/home-accueil/privacy-privee/parliament-parlement-eng.html.
- Canada. The Communications Security Establishment Canada (CSEC). (2011). *Information Kit*. Retrieved July 29, 2011, from, http://www.cse-cst.gc.ca/home-accueil/media/information-eng.html.

- Canada. The Communications Security Establishment Canada (CSEC). (2011). *The Anti-Terrorism Act and CSEC's Evolution*. Retrieved July 29, 2011, from http://www.cse-cst.gc.ca/home-accueil/media/ata-lat-eng.html.
- Canada. The Communications Security Establishment Canada (CSEC). (2011). *CSEC: Frequently ask questions*. Retrieved July 29, 2011, from http://www.cse-cst.gc.ca/faq-eng.html.
- Canada. The Canada Revenue Agency (CRA). (2011). *Structure and Operational Framework.* Retrieved August 7, 2011, from http://www.cra-arc.gc.ca/gncy/brd/bm-bkgrd-eng.html.
- Sher, J. (2011, June 28). Money laundering going largely unpunished in Canada. *Globe and Mail*, general section.
- Staff report (2011, March 7). Canada still has more work to do on money laundering. *Canadian Press*, general section.
- Financial Action Task Force (FATF). (April 2009). *AML/CFT Evaluations and Assessments. Handbook for Countries and Assessors*. Retrieved August 15, 2011, from http://www.fatf-gafi.org/dataoecd/7/42/38896285.pdf
- Financial Action Task Force (FATF). (February 2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations*. Retrieved February 17, 2012, from http://www.fatf-gafi.org/document/50/0,3746,en_32250379_32236920_49653426_1_1_1_1,00.html.
- Financial Action Task Force (FATF). (October 2011). *FATF Standards – FATF IX Special Recommendations*. Retrieved August 15, 2011, from http://www.fatf-

gafi.org/findDocument/0,3770,en_32250379_32236920_1_34956090_1_1_1,00.html.

- Financial Action Task Force (FATF). (February 2008). Financial Action Task Force (FATF) – Third Mutual Evaluation On Anti-Money Laundering and Combating the Financing of Terrorism. Retrieved April 9, 2012, from http://www.fatf-gafi.org/document/58/0,3343,en_32250379_32236963_40199098_1_1_1_1,00.html.
- Canada. The Office of the Superintendent of Financial Institutions (OSFI). (2011). Role of AML/ATF in the Financial System. Retrieved September 28, 2011, from http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/speeches/TP20100427_e.pdf.
- Canada. The Office of the Superintendent of Financial Institutions (OSFI). (2011). *Fighting Financial Crime: The role of the Canadian financial sector.* Retrieved September 29, 2011, from http://www.osfibsif.gc.ca/app/DocRepository/1/eng/speeches/ABC07_e.pdf
- Canada. Parliament of Canada. (1985). *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23). Retrieved September 19, 2011, from http://laws-lois.justice.gc.ca/eng/acts/C-23/.
- Canada. Parliament of Canada. (2001). *Anti-terrorism Act (S.C. 2001, c. 41)*. Retrieved September 19, 2011, from http://laws-lois.justice.gc.ca/eng/acts/A-11.7/index.html.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2011). *FINTRAC Annual Report 2011.* Retrieved September 19, 2011, from http://www.fintrac.gc.ca/publications/ar/2011/1-eng.asp.

- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2011). *FINTRAC Annual Report 2010.* Retrieved September 19, 2011, from http://www.fintrac.gc.ca/publications/ar/2010/1-eng.asp.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2011). *FINTRAC Annual Report 2009.* Retrieved September 19, 2011, from http://www.fintrac.gc.ca/publications/ar/2009/1-eng.asp.
- Canada. Canadian Security Intelligence Service (CSIS). (2011). *CSIS Public Report 2009-2010.* Retrieved September 19, 2011, from https://www.csis.gc.ca/pblctns/nnlrprt/2009-2010/rprt2009-2010-eng.asp.
- Canada. Canadian Security Intelligence Service (CSIS). (2001). *Economic Security*. Retrieved October 5, 2004, from http://www.csis-scrs.gc.ca/eng/operate/es2_e.html.
- Canada. Canadian Security Intelligence Service (CSIS). (2004). *The CSIS Mandate*. Retrieved October 5, 2004, from http://www.csis-scrs.gc.ca/eng/backgrnd/back1_e.html.
- Canada. Canadian Security Intelligence Service (CSIS). (2004). *The CSIS Mission Statement*. Retrieved October 5, 2004, from http://www.csis-scrs.gc.ca/eng/backgrnd/mission_e.html.
- Canada. Canadian Security Intelligence Service (CSIS). (2004). *CSIS and the Security Intelligence Cycle*. Retrieved October 5, 2004, from http://www.csis-scrs.gc.ca/eng/backgrnd/back3_e.html.
- Canada. Canadian Security Intelligence Service (CSIS). (2004). *Frequently Asked Questions*. Retrieved October 5, 2004, from http://www.csis-scrs.gc.ca/eng/menu/faq_e.html.

- Canada. Canadian Security Intelligence Service (CSIS). (2004). *Human Resources*. Retrieved July 9, 2005, from http://www.csis-scrs.gc.ca/eng/backgrnd/back4_e.html.
- Canada. Senate. (2011). *Security, Freedom and the Complex Terrorist Threat: Positive Steps Ahead – Interim Report of the Special Senate Committee on Anti-terrorism*. Retrieved October 10, 2011, from http://www.parl.gc.ca/content/sen/committee/403/anti/rep/rep03mar11-e.pdf.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2011*). FINTRAC, Law Enforcement and Intelligence Partners: Sharing Intelligence, Making the Links*. Retrieved October 3, 2011, from http://www.fintrac.gc.ca/publications/brochure/2011-02/1-eng.asp.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2011*). Connecting the money to the crime.* Retrieved October 3, 2011, from http://www.fintrac.gc.ca/publications/brochure/05-2003/1-eng.asp.
- Freeze, Colin. (2011, December 22). *New powers urged for financial intelligence agents*. Globe and Mail, General section.
- Staff report. (2011, March 7). *Canada still has more work to do on money laundering*. Canadian Press, general section.
- Sher, Julian. (2011, June 28). *Money laundering going largely unpunished in Canada*. Globe and Mail, General section.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2010*). FINTRAC Annual Report Highlights Ten Years of Connecting the Money to the Crime.* Retrieved November 27, 2010, from http://www.fintrac-canafe.gc.ca/publications/nr/2010-11-18-eng.asp.

- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2009*). AUSTRAC and FINTRAC sign agreement to share compliance information.* Retrieved September 24, 2010, from http://www.fintrac-canafe.gc.ca/publications/nr/2009-03-05-eng.asp.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2006*). Results for 2005-2006 – Ensuring Compliance with the Legislation.* Retrieved September 24, 2010, from http://www.fintrac-canafe.gc.ca/publications/nr/2006/32-eng.asp.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2004*). OSFI and FINTRAC to Join Forces Against Money Laundering and Terrorist Financing.* Retrieved September 24, 2010, from http://www.fintrac-canafe.gc.ca/publications/nr/2004-07-08-eng.asp.
- Schneider, Stephen. (2004). *Money Laundering in Canada: A Quantitative Analysis of Royal Canadian Mounted Police Cases*. Journal of Financial Crime; Feb 2004; 282-291.
- Canada. The Office of the Superintendent of Financial Institutions (OSFI). (2009). *The 2008 – 2009 Annual Report*. Retrieved January 21, 2011, from http://www.osfi-bsif.gc.ca/app/DocRepository/1/RA/0809/eng/5.3a_e.html.
- Canada. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (2004*). Canada's Anti-Money Laundering and Anti-Terrorist Financing Initiative.* Retrieved August 19, 2010, from http://www.fintrac-canafe.gc.ca/fintrac-canafe/antimltf-eng.asp.

- Canada. Canada Border Services Agency. (2008). *About Us – What We Do*. Retrieved August 18, 2011, from http://www.cbsa-asfc.gc.ca/agency-agence/what-quoi-eng.html.
- Canada. Canada Border Services Agency. (2008). *About Us – Who We Are*. Retrieved August 18, 2011, from http://www.cbsa-asfc.gc.ca/agency-agence/who-qui-eng.html.
- Canada. Canada Border Services Agency. (2008). *Crossing the border with $10,000 or more?*. Retrieved August 18, 2011, from http://www.cbsa-asfc.gc.ca/publications/pub/bsf5052-eng.html.