Office of the
Privacy Commissioner
of Canada

AUDIT REPORT OF THE PRIVACY COMMISSIONER OF CANADA

Financial Transactions and Reports Analysis Centre of Canada

Section 37 of the *Privacy Act*

Section 72 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

FINAL REPORT

2009

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP54-29/2009E-PDF
ISBN 978-1-100-14051-3

This publication is also available on our Web site at **www.priv.gc.ca**.

Table of Contents

Main Points

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC or the Centre) is an independent agency operating at arms length from law enforcement. Created in 2001, the Centre's mandate is to collect and analyze financial transactions, and disseminate intelligence in order to assist in the detection, prevention and deterrence of money laundering and terrorist financing. The Centre's mandate also includes protecting personal information under its control.

Government institutions must have statutory authority to collect personal information for the purpose of carrying out their programs and activities. Privacy audits rely upon an organization's enabling legislation to assess its compliance with the *Privacy Act*. A legislative mandate is the benchmark against which personal information management practices are measured; what information is collected, how it is used, to whom and under what circumstances it is disclosed, and when it is destroyed. FINTRAC's legislative mandate is derived from the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). It is against this that we assessed compliance.

What we examined

The Office of the Privacy Commissioner (OPC) examined relevant policies, practices and procedures, guidelines, analytical tools, security assessments, training materials and information sharing agreements. We also reviewed an exploratory sampling of all types of reports FINTRAC receives, as well as information it discloses to law enforcement agencies, and other federal departments and agencies.

While security within the public and reception areas of the Centre's offices were included as part of our lines of enquiry, we focused on the acquisition (receipt and collection), processing and storage of personal information within the operational and restricted areas of FINTRAC.

In addition, we assessed the Centre's overall privacy management framework, meaning the way in which FINTRAC assigns privacy responsibilities, manages privacy risks and ensures compliance with its obligations under the *Privacy Act*.

Why it is important

Security and intelligence agencies require personal information to carry out their mandates. However, there must be a balance between national security and law enforcement activities and the fundamental human right to privacy. This may include the right to control the collection, use, and disclosure of one's personal information.

Entities which are subject to the PCMLTFA (see Appendix A) must scrutinize and report on the financial transactions of clients. These entities, potentially up to 300,000 in number, transmit reports containing sensitive personal information to FINTRAC (see Appendix B). The reports are submitted without the consent of the individuals concerned and may not be accessible to them under the *Privacy Act*.

Sanctions for non-compliance with reporting requirements are substantial. With fines up to $2,000,000 and prison terms ranging from six months to five years, there is a danger that entities may over report.

Canadians must be assured that their personal information is being appropriately managed within well established controls. The requirement to safeguard information assets, while common to all government departments, is heightened for organizations such as FINTRAC.

What we found

FINTRAC has a robust and comprehensive approach to security. It has incorporated elements of many relevant federal government policies into its own policy and security management framework. We found no evidence that personal information could be compromised because of inadequate security controls once it has been received by FINTRAC.

Ensuring that access to information is restricted to those with a legitimate requirement represents a key safeguard in privacy protection. FINTRAC has controls to ensure that access is restricted to those with a need to know.

We found that the Centre's use and disclosure practices comply with the PCMLTFA and the *Privacy Act.* However, FINTRAC could benefit from the development of criteria to govern disclosures to the Canada Border Services Agency and the Communications Security Establishment of Canada. FINTRAC should also seek ways of ensuring that information it shares with foreign financial intelligence agencies is adequately protected.

In fulfilling its mandate, the Centre acquires information in two ways: it receives and collects it. While we found no evidence to suggest FINTRAC is collecting information beyond what is authorized, we noted that it has received and retains information beyond the Centre's legislative authority. Current controls, including front-end screening and ongoing monitoring of reports, need to be enhanced to ensure that FINTRAC's information holdings are both relevant and not excessive.

FINTRAC is responsible for ensuring that reporting entities comply with their obligations under the PCMLTFA, and has enlisted a number of regulatory partners to assist in this regard. The Centre was unable to provide assurance that the guidance these partners provide to reporting entities is consistent with PCMLTFA requirements.

While the Centre has put in place elements of a privacy management framework, there are gaps which need to be addressed. Specifically, governance and accountability for privacy are not clearly defined, FINTRAC's privacy risk management process is not formalized and there is a lack of privacy-specific training for staff. Strengthening the framework will assist in ensuring that FINTRAC meets its obligations under the *Privacy Act*.

FINTRAC has responded. The Centre's responses follow each recommendation throughout the report.

Introduction

Background

1. Money laundering is the process used to disguise the origin of money or assets derived from criminal activity. In 1989, Canada implemented legislation establishing an Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) regime. This legislation, which was amended in 2000 and again in 2006, established the Financial Transactions and Reports Analysis Centre (FINTRAC or the Centre) as Canada's financial intelligence unit.
2. The objectives of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) are to:
    - implement measures to detect and deter money laundering and the financing of terrorist activities and to facilitate their investigation and prosecution;
    - provide law enforcement officials with the information required to deprive individuals of the proceeds of their criminal activities, while ensuring that appropriate safeguards are in place to protect privacy; and,
    - fulfill Canada's international commitments to participate in the fight against transnational crime, particularly money laundering and the fight against terrorist activity.
3. The *Act* requires a broad range of entities – including banks, foreign exchange dealers, life insurance companies and several other types of businesses and professionals (see Appendix A) – to collect and maintain specific information about their clients and their transactions (see Appendix B). Entities are also required to report certain types of transactions to the Centre.
4. The *Act* also establishes a requirement to report the cross border movement or seizure of currency or monetary instruments with a value equal to or greater than $10,000, or its equivalent in foreign currency.
5. Amendments to the PCMLTFA in 2006 increased both the number of organizations subject to the *Act* and the types of transactions which are subject to scrutiny and reporting. They also enable FINTRAC

to disclose more information to law enforcement and security organizations, as well as the Canada Border Services Agency (CBSA) and the Canada Revenue Agency (CRA).

Entity profile

6. FINTRAC is an independent agency, operating at arms-length from law enforcement and other entities to which it is authorized to disclose information. The Centre, which became operational in October 2001, collects, analyzes and disseminates information concerning suspected money laundering and terrorist financing, and other threats to the security of Canada.

7. In addition to its analysis and disclosure functions, FINTRAC carries out a compliance program to verify whether reporting entities are complying with the obligations prescribed under the PCMLTFA and corresponding regulations. The Centre is also responsible for enhancing public awareness of matters relating to money laundering.

8. FINTRAC reports to the Minister of Finance through its Director. As of March 31, 2008, the Centre had 319 staff and an annualized budget of $52.8 million. Further information about FINTRAC is available on its website at http://www.fintrac-canafe.gc.ca.

Focus of the audit

9. The audit focused on FINTRAC's management of personal information, both in its capacity as a financial intelligence unit and while discharging its compliance activities as required by the PCMLTFA.

10. Our objective was to assess whether FINTRAC has appropriate controls in place to protect personal information, and whether its processes and practices for managing such information comply with sections 4 through 8 of the *Privacy Act*.

11. The audit was not undertaken to evaluate the effectiveness or intrusiveness of Canada's AML/ATF regime.

12. We examined FINTRAC's management of personal information acquired, used and disclosed under the PCMLTFA. We did not review the Centre's handling of personal information about its employees. Furthermore, we did not assess the control frameworks implemented by reporting entities to manage their personal information holdings.

13. Information on the objective, criteria, scope and approach is found in the **About the Audit** section of this report.

Observations and Recommendations

Protection of information holdings

14. Maintaining the security of personal information is a key component in meeting protection requirements established under the *Privacy Act*. Appropriate measures and controls must be present to ensure that personal data is not subject to unauthorized use, disclosure, alteration or destruction.

15. The Government Security Policy (GSP), which prescribes safeguards to protect and preserve the confidentiality and integrity of government assets including personal information, establishes baseline (mandatory) security requirements. Federal departments and agencies are required to conduct their own assessments to determine whether safeguards above baseline levels are necessary. The GSP also calls for ongoing monitoring of the threat environment to ensure appropriate security measures are maintained.

16. We found that FINTRAC has instituted a layered security infrastructure to protect its personal information holdings. Administrative and organizational security, personnel security, physical security, and information technology security are all components of the Centre's integrated security program.

Physical security infrastructure is sound

17. FINTRAC's facilities and information assets are controlled by various measures, including guards, security cameras and intrusion detection alarm systems. Electronic access control cards, security containers and storage vaults are among the measures used to restrict access to the Centre's operational, security and high security zones. The records office, financial intelligence analysis area and FINTRAC's IT server and network rooms are located within high security zones.

18. FINTRAC commissioned third parties to conduct physical security and threat and risk assessments (TRA), which identified opportunities for improvement. We are satisfied that the issues raised by these

assessments have been addressed. However, records capturing the actions taken to address the deficiencies were not appended to the applicable assessment reports, and the reports lacked confirmation that the findings and recommendations were reviewed and accepted by senior management.

Recommendation: FINTRAC should ensure that all actions taken to address observations noted in TRAs or security assessments are appended to the documents of record. In addition, management should, through sign off, formally acknowledge and accept the risks identified in these assessments.

The Centre's response. FINTRAC welcomes this recommendation. Steps have been taken to ensure that actions taken to address observations are appended to TRAs and security assessments and that formal sign offs are conducted.

19. Physical security measures are complemented by the Centre's clean desk policy and routine security inspections. All employees are responsible for ensuring that information is appropriately stored during quiet hours. Any violations are reported to the Departmental Security Officer, and details are included on the employee's security file.

20. Government departments and agencies are required to manage the risk of unauthorized disclosure of information through the establishment of a classification/protection regime. We examined areas where information is retained in hard copy format; without exception, we found that documents were stored in accordance with GSP requirements.

Personnel security screening is operating in accordance with the Government Security Policy

21. The GSP requires that all employees and contract personnel undergo a screening process commensurate with the level of information or assets to which they will have access. All FINTRAC employees are cleared to the Secret level prior to commencing employment. A Top Secret clearance process is initiated once the individual begins working; this clearance must be maintained as a condition of employment. Short-term contractors, temporary employees and students are cleared to a minimum of Secret.

22. FINTRAC has established entrance and exit procedures for managing and controlling assets assigned to staff, including system access. As part of our testing we examined a sample of personnel security files of current and former employees. On the basis of our review, we conclude that the personnel screening and termination processes are functioning in accordance with prescribed policy.

Comprehensive IT security management is in place

23. Information Technology (IT) security is the process of preventing and detecting unauthorized use of computer systems. Evolving technology presents corresponding threats that may affect the confidentiality and integrity of personal information.

24. To prevent unauthorized access to any part of a computer system, organizations must protect their data through the use of appropriate safeguards including firewalls, intrusion detection systems, encrypted connections and segregated networks. IT systems should also be subject to ongoing monitoring and routine vulnerability assessments and testing.

25. We found FINTRAC to be, in many ways, an example to others in terms of having implemented a comprehensive security management framework which adheres to industry best practices. An overview of some key features is provided below.

26. **Certification and Accreditation (C&A).** The Management of Information Technology Security standard issued by the Treasury Board Secretariat requires departments to certify and accredit their IT systems prior to approving them for operation. Certification verifies that baseline security requirements for a particular IT system are applied and augmented as necessary to ensure the integrity and confidentiality of information, and that controls and safeguards are functioning as intended. Accreditation signifies that management has authorized operation of the system and has accepted any residual risk.

27. Although implemented fairly recently, we found that the Centre's C&A framework is clearly defined and supported by a strong implementation strategy. At the time we concluded our examination, the C&A process had been completed for one system and the process for a second was under way.

28. **Securing IT applications and systems.** The security architecture of an IT system refers to the mainframe computer, its servers, communication links, firewalls and defined security zones intended to protect the system and its contents from external attacks.

29. We found that the security architecture of FINTRAC's applications and systems provides several types of protection at every critical IT level and a central control over access between controlled zones. In addition, the Centre's network architecture is such that the corporate and analytical networks are completely separate; no cross-over connectivity between the two is possible.

30. FINTRAC exercises security best practices at all levels within its networks. For security reasons, specific details cannot be disclosed in this report; we are satisfied that adequate security controls are in place,

including (but not restricted to) the use of encryption and firewalls, segregation of networks and isolation from external connectivity.

31. It is important to test network security routinely for possible vulnerabilities or configuration weaknesses. TRAs and vulnerability assessments identify weaknesses which could compromise security. Penetration testing determines whether the established controls can be circumvented to exploit vulnerabilities.

32. A number of vulnerability assessments and penetration tests of outward facing network zones have been performed by third parties, including the Communications Security Establishment of Canada (CSEC). These tests confirmed that FINTRAC's networks are secure. We are satisfied that the Centre has the appropriate testing tools and performs ongoing vulnerability assessments and penetration testing.

33. **Introducing changes to IT.** Change management within the IT environment relies on developing procedures, controls, technology and software to modify IT hardware and software programs. We found that FINTRAC has a well defined and controlled change management framework which follows approved industry best practices for incorporating IT changes.

34. **Controlling access to data.** Controlled access to an IT system and its data elements represents a key safeguard because it restricts the use and disclosure of personal information to those who have a need to know.

35. An effective method of mitigating the risk of data being compromised – improperly used, disclosed, modified or deleted – is to limit access rights to the system. This is commonly referred to as "role based access." We found that FINTRAC ensures that only those with a legitimate operational need receive access to information, controlled by a user authentication process, and only at the level required by their defined role.

36. Logging user activities is crucial to determining whether access rights have been appropriately exercised according to the need to know principle. We examined the logging practices across all systems. While we found that the procedures vary amongst the different components, full user activity logging is captured. Furthermore, the integrity of the log files is maintained through proper security measures and controls.

Compliance with the Code of Fair Information Practices

37. The *Privacy Act* takes a life-cycle approach to the management of personal information. Sections 4 through 8, referred to as the "Code of Fair Information Practices", restrict the collection of personal information and limits how that information, once collected, can be used and disclosed. It balances the legitimate collection and use requirements essential to many federal government programs with the right to a reasonable expectation of privacy.

38. Within the federal context, section 4 of the *Privacy Act* establishes the criteria for the collection of personal information by government institutions. Specifically, it must relate directly to an operating program or activity of the institution.

39. The PCMLTFA authorizes FINTRAC to receive information from individuals, reporting entities and other sources. It also permits the Centre to collect information it considers relevant to money laundering or terrorist financing activities, as well as information required to fulfill its compliance mandate.

Acquisition of information extends beyond legislative authority

40. Part 1 of the PCMLTFA requires individuals and reporting entities (see Appendix A) to submit to FINTRAC:

    - Large cash transaction reports (LCTRs) of $10,000 or more;
    - Electronic funds transfer reports (EFTRs) of $10,000 or more;
    - Reports concerning suspicious transactions (STRs) or suspicious attempted transactions related to money laundering or terrorist financing, regardless of the amount of the transaction or attempted transaction; and,
    - Terrorist property reports (TPRs) where the entity reports the existence of terrorist property in its possession or control, or information about any transaction or proposed transaction relating to the property, regardless of the value.

41. Under Part 2 of the *Act*, individuals and entities must declare to the Canada Border Services Agency (CBSA) the cross border movement of currency or monetary instruments worth $10,000 or more. These are reported to FINTRAC by way of Cross Border Currency Reports. CBSA is also required to file Cross Border Seizure Reports where the value of the currency or monetary instruments seized is $10,000 or more.

42. The Centre also receives voluntary information concerning suspicions of money laundering and terrorist financing. These reports, referred to as Voluntary Information Records (VIRs), are received from various sources, including the general public, the RCMP, the Canadian Security Intelligence Service (CSIS), provincial and municipal law enforcement agencies and foreign financial intelligence units.

43. In addition to the information it receives, FINTRAC may collect information from federal and provincial law enforcement and national security databases where an agreement governing such access exists. The Centre currently has memoranda of understanding with the RCMP, the Canadian Police Information Centre, and the Organized Crime Agency of British Columbia.

44. **Reporting under prescribed threshold**. LCTRs and EFTRs account for the majority of FINTRAC's information holdings. The factual elements captured in these reports are prescribed by regulation and include extensive personal information.

45. The PCMLTFA sets the prescribed reporting threshold for these reports at $10,000 or more in a single transaction, or two or more transactions that are less than $10,000 but collectively total $10,000 or more within a 24-hour period by or on behalf of the same individual or entity.

46. We extracted a random exploratory sample of reports as part of our testing and found that 17% of this sample was under the threshold. We asked the Centre to produce evidence to support the inclusion of these reports in the database; in some instances, it was unable to do so.

47. We also found instances where a casino reported transactions involving the disbursement of $10,000 or more as LCTRs. While casinos had an obligation to retain a record of such disbursements, the requirement to report the transactions to FINTRAC did not take effect until September 28, 2009. In addition, we found a number of Cross Border Currency Reports which fell below the $10,000 threshold.

48. In summary, we found that FINTRAC has received financial information that did not meet the prescribed threshold and therefore should not have been reported. Mindful of the size of our audit sample, the extent to which the Centre's information holdings are populated with such reports is unknown.

49. **Absence of "reasonable grounds to suspect".** Entities subject to the PCMLTFA are required to submit a Suspicious Transaction Report (STR) when there are reasonable grounds to suspect that a transaction is related to money laundering or terrorist financing. As of June 23, 2008, this applies whether the transaction was completed or simply attempted. In addition to information about the individuals involved, STRs capture the circumstances that led the entity to file the report.

50. The legal threshold of "reasonable grounds to suspect" is not defined in the PCMLTFA. FINTRAC policy describes it as a level of suspicion above "mere suspicion" and below "reasonable belief". We found that although STRs are reviewed and prioritized upon receipt, they are not assessed for reasonable suspicion of money laundering or terrorist financing.

51. Of the files sampled, we identified a number that did not demonstrate "reasonable grounds to suspect" money laundering or terrorist financing. This would suggest that reporting entities may either be unclear on their reporting obligations, or default to reporting in cases where a level of doubt exists, rendering privacy a secondary consideration. Examples of such files are provided below in Exhibit A.

Exhibit A

- A reporting entity filed a number of reports indicating that they "are taking a conservative approach in reporting this as [a Suspicious Transaction Report] because there are no grounds for suspecting that this transaction is related to the commission of a money laundering offence but there is a lack of evidence to prove that the transaction is legitimate."
- An individual deposited cash under the $10,000 reporting threshold in a financial institution. When questioned about the source of funds, he declared that he bought merchandise in Canada and sold it abroad. The report indicated that although the account activity appeared normal, the report was filed to ensure the individual complied with all tax requirements. There was no indication that the transaction related to suspected money laundering or terrorist financing.
- An individual deposited a government cheque for an amount of less than $300 and then withdrew the entire amount. The financial institution filed a Suspicious Transaction Report concerning this transaction, but did not indicate why it was deemed suspicious.

52. We also examined a sample of Voluntary Information Records (VIRs). Upon receipt, FINTRAC assesses these records to determine whether they fall within its mandate. Records unrelated to the Centre's mandate are retained but not made available for analysis purposes. Despite this screening, we found a number of VIRs in FINTRAC's database where no suspicion of money laundering or terrorist financing was evident; Exhibit B provides examples.

Exhibit B

- FINTRAC received VIRs from a retailer which has implemented its own anti-money laundering program, whereby all cash and debit transactions in excess of $10,000 are reported. None of these reports contain any indication that money laundering is suspected.
- An individual converted some foreign currency at a money service business. When asked to provide information to meet PCMLTFA record-keeping requirements, the individual asked if this information would be shared with other federal government agencies. The clerk explained that the information would only be retained by the business, and that it was needed to comply with federal regulations. The client left the establishment without completing the transaction. The VIR includes the comment: "I don't believe [the individual] was laundering money but was concerned about immigration or taxation for some reason."
- A VIR was submitted by an anonymous individual who was tired of an acquaintance bragging about how his company was paying his expenses even though he hadn't travelled for years, which he wasn't claiming as a taxable benefit. The VIR states, "this man should pay taxes just like everybody else." There was no reference to a suspicion of money laundering or terrorist financing.
- An individual deposited a cheque from a law firm in a financial institution. At the time of the transaction, the financial institution was satisfied that the individual provided legitimate reasons for the source of funds. Nevertheless, the entity decided to notify FINTRAC because of the individual's ethnic origin and the fact that the individual had recently taken a pleasure trip to a particular country.

53. **Receipt of extraneous information.** FINTRAC has published and disseminated extensive documentation to direct entities regarding what must be submitted. Despite this guidance, we found that extraneous information has been submitted to and, more importantly from a privacy perspective, retained by the Centre.

54. To meet their client identification obligations under the PCMLTFA, entities are directed to consult the individual's birth certificate, driver's licence, passport, record of landing, permanent resident card or other similar document.

55. FINTRAC's guidelines state that an individual's provincial health card may be used as identification, but only if it is not prohibited by provincial or territorial legislation. In addition, although the Social Insurance Number (SIN) can be used to verify the identity of a client, the number is not to be provided to the Centre on any type of report.

56. Notwithstanding, both SINs and certain health cards were included in some reports we examined. We also found VIRs and STRs that, although relevant to FINTRAC's mandate, contained information that was extraneous in nature, as reported below in Exhibit C.

Exhibit C

- A source provided medical information about the subject of the report as well as allegations unrelated to money laundering or terrorist financing.
- A report was submitted regarding allegations of fraud relating to an individual failing to declare income. It included personal information about the subject's daughter which did not have any relevance to the case under investigation.
- A financial institution submitted a suspicious transaction report which included a comment which was highly subjective in nature.

Reports are not adequately screened

57. Treasury Board Secretariat Policy on the Collection of Personal Information requires government institutions to manage their personal information holdings in keeping with the limiting collection principle. Given both the volume and the sensitivity of the information it receives and collects, we would expect that FINTRAC ensure that it is both relevant and not excessive.

58. The Centre's web-based reporting system provides entities with field-by-field instructions for filing reports electronically, identifying errors and issuing warnings if mandatory data are not captured. Mandatory fields include date, time and amount of transaction, who conducted it, and where and how it was conducted. Where required, reports are returned to the originator for correction. Voluntary Information Records (VIRs) are subjected to a manual analysis upon receipt.

59. With the exception of VIRs, FINTRAC's screening processes are designed primarily to address issues of data quality – that is, that all required fields in reports are completed. They do not address whether the information is relevant to the Centre's mandate or is excessive in nature.

60. The absence of such a process is a gap which warrants attention. Ongoing audit and monitoring of incoming reports would provide FINTRAC with an effective tool to assist in meeting its privacy obligations, while providing valuable data for its outreach and compliance activities.

Recommendation: FINTRAC should work with reporting entities to ensure that the Centre does not obtain personal information (1) which it has no legislative authority to receive and (2) that it does not need or use. To that end, FINTRAC should continue to enhance the processes for front-end screening of reports, and develop a complementary program of ongoing monitoring and review.

The Centre's response. FINTRAC agrees to this recommendation. The Centre has already taken steps to limit the information it receives from reporting entities:

- Since February 2006, FINTRAC has, through the introduction of a new reporting system, introduced improved ways to validate the reports as they are transmitted to the Centre to further reduce the potential of receiving information that should not have been sent;
- The new Casino Disbursement Report form has built-in enhanced front-end screening that will further assist in preventing this type of information from entering the Centre's database; and,
- In addition, FINTRAC regularly reviews and updates the guidance offered to reporting entities (REs). This guidance is the source of information for REs to support their understanding of their obligations under the *Act*. This guidance outlines the information that is to be sent to FINTRAC, and what elements are not to be sent.

In the near future, the Centre will be undertaking a review of its reporting forms to assess the analytical value of data elements being captured and to minimize the reporting burden to reporting entities. FINTRAC feels that this exercise, combined with the steps already taken, will be effective in further reducing the amount of information that is incorrectly sent to the Centre.

No mechanism exists to confirm terrorist affiliation

61. A Terrorist Property Report (TPR) must be submitted when a reporting entity has in its possession property that it knows or believes is owned or controlled by a terrorist or terrorist group. To assist in this determination, FINTRAC directs reporting entities to the "listed entities" on Public Safety Canada's website or the "Terrorism Financing" link on the Office of the Superintendent of Financial Institutions' website.

62. Once terrorist affiliation is established, reporting entities are required to notify the RCMP and CSIS. Under circumstances where entities suspect but are not sure they are dealing with a terrorist or terrorist group, they must submit a Suspicious Transaction Report (STR) whether the transaction was completed or attempted.

63. We examined all TPRs to determine the extent to which reporting entities confirmed that the subjects of the reports were, in fact, listed individuals or entities. We found that almost half of the reports were filed on the basis of a "possible match" to terrorist entity listings.

64. Although FINTRAC attempts to verify the individual's affiliation, it is difficult to do so because vital information, such as a date of birth, is not recorded on the TPR. Where identity cannot be confirmed, the Centre does not pursue further analysis; however, the information remains in FINTRAC's database. The practice, by default, is to retain TPRs and STRs regardless of whether or not there is knowledge, belief or suspicion of terrorist affiliation.

65. As the custodian of these reports, FINTRAC should limit the receipt and retention of TPRs and STRs to instances where the identity of the subject is verified.

Recommendation: FINTRAC should explore avenues with its intelligence partners to ensure, to the extent possible, that terrorist affiliations are confirmed prior to retaining this data, and making it available for analytical purposes.

The Centre's response. FINTRAC welcomes this recommendation. To the extent possible, the Centre will enter into a dialogue with its intelligence partners to explore ways to mitigate the risk that information about individuals is retained once it has been confirmed that no terrorist affiliation exists.

Use and disclosure practices comply with governing legislation

66. Sections 7 and 8 of the *Privacy Act* govern the use and disclosure of personal information. In general terms, government institutions can only use information for the purposes for which it was collected or for a use consistent with that purpose. The *Act* also limits the circumstances under which personal information can be disclosed without consent. FINTRAC's authority to use and disclose information is derived from sections 55 to 65.1 of the PCMLTFA.

67. We examined a sample of files, including analytical reports that accompanied disclosure recommendations. We found no evidence of personal information having been used for a purpose other than that for which it was obtained, or for a use consistent with that purpose. Moreover, we found that disclosures are tightly controlled and made in accordance with the PCMLTFA.

Criteria for certain types of disclosures need to be formalized

68. Once FINTRAC has established reasonable grounds to suspect that designated information (see Appendix B) would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, the Centre must disclose the information to the appropriate police force(s). If FINTRAC has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada, it must disclose that information to CSIS.

69. The Centre must also disclose designated information to the Canada Border Services Agency (CBSA), the Communications Security Establishment of Canada (CSEC) and the Canada Revenue Agency (CRA) when separate statutory tests are met. First, the Centre must have reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering or terrorist activity financing offence, and then determine that the information at issue meets the criteria enumerated in subsection 55(3) of the PCMLTFA. Using CBSA as an example, the Centre must also determine that the information is relevant to:

    - 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*;
    - determining whether a person is a person described in sections 34 to 42 of the *Immigration and Refugee Protection Act* or relevant to an offence under any of sections 117 to 119, 126 or 127 of that *Act*; or,

- an offence of evading or attempting to evade paying taxes or duties imposed under an *Act* of Parliament administered by CBSA.

70. While FINTRAC is working with CRA to formalize indicators for the identification of transactions that could also be relevant to an offence of evading or attempting to evade taxes, we note that no written criteria exist regarding when disclosures to CBSA or CSEC are required. The absence of such renders it difficult to recreate the logic that informed disclosures and increases the risk of an unintended disclosure.

Recommendation: FINTRAC should establish a set of written criteria to guide in the determination of when the threshold for disclosures to CBSA and CSEC has been met.

The Centre's response. FINTRAC agrees with this recommendation.

Information sharing agreements lack key provisions

71. FINTRAC may, pursuant to section 56.1 of the PCMLTFA, disclose designated information to foreign states or international organizations with powers and duties similar to its own.

72. The PCMLTFA requires that a written agreement or arrangement exist regarding the exchange of such information. The agreements must stipulate that the exchanged information will be treated in a confidential manner, will not be further disclosed without the Centre's consent, and will be used only for the purpose for which it has been provided.

73. We examined all 47 Memoranda of Understanding (MOU) between FINTRAC and its foreign counterparts. While the agreements contained the elements prescribed under the PCMLTFA, we found that they lack a number of key clauses: namely, a requirement for both parties to notify the other in the event of a breach, and an audit provision.

74. While an MOU establishes the terms and conditions of a sharing agreement, it does not necessarily ensure that the privacy risks associated with the arrangement are identified and mitigated. Periodic audits provide such a mechanism. In addition to providing a level of assurance that the parties are, in fact, respecting the agreement, they provide a means of verifying that appropriate privacy safeguards are in place.

75. As noted in our audit of the Canada Border Services Agency in 2006, reciprocal or mutual assurance regarding privacy is important not only for information about Canadians that is shared with

foreign governments, but also for foreign nationals whose personal information is disclosed to Canada.[1]

Recommendation: FINTRAC should ensure that all information sharing agreements include a requirement for both parties to notify the other in the event of unauthorized access, use or disclosure of personal information shared under the MOU. In addition, the Centre should implement a means of obtaining ongoing assurance that the data handling practices of its foreign Financial Intelligence Unit partners are consistent with the terms of its information sharing agreements.

The Centre's response. FINTRAC conducts periodic reviews of MOU partners' information protection activities through bilateral visits as well as by soliciting input from other domestic partners with respect to any concerns they may have regarding the protection of information in a given jurisdiction. FINTRAC also consults its Canadian counterparts (Department of Foreign Affairs and International Trade, CSIS, RCMP, and the Department of Finance) to support its work in this field. This information is shared among FINTRAC's analysts to ensure that they are aware of any sensitivities that should be considered prior to FINTRAC exercising its discretion to disclose to an MOU partner.

Current practices contravene the limiting retention principle

76. The PCMLTFA establishes retention periods for reports received by FINTRAC. The retention period for undisclosed and disclosed reports had been set at five years and eight years respectively. However, amendments which came into force February 10, 2007 establishes a minimum ten year retention period for all reports.

77. Undisclosed reports received from October 31, 2001 to February 9, 2002 were subject to the initial five year retention period. As such, these reports were set to "inactive" in February 2007, rendering them inaccessible for analytical purposes. We were told that these reports were destroyed in May 2007, and were provided documents supporting this assertion. Our testing confirmed that these reports are no longer in the database.

78. Fundamental to privacy is the principle that personal information should only be obtained if there is a legitimate and authorized need. Under the *Privacy Act*, collection must be relevant to an operating program or activity. Relevance is determined by statutory authority. As reported previously, FINTRAC has received information beyond what the PCMLTFA allows, including:

1 OPC Audit of the Personal Information Management Practices of the Canada Border Services Agency — Trans-Border Data Flows (June 20, 2006), paragraphs 3.26 and 3.27.

- financial transaction reports which do not meet the $10,000 threshold;
- Suspicious Transaction Reports and Voluntary Information Records which do not demonstrate reasonable grounds to suspect money laundering or terrorist financing; and,
- extraneous information including, but not restricted to, Social Insurance Numbers and Health Card numbers, where prohibited by provincial legislation.

The extent to which FINTRAC's information holdings contain such reports is unknown.

79. Any acquisition of personal information beyond statutory authority, by extension, contravenes the limiting retention principle. This presents an unquestionable risk to privacy by making available for use or disclosure personal information which should never have been obtained.

Recommendation: To bring itself into compliance with the PCMLTFA and the *Privacy Act*, FINTRAC should permanently delete from its holdings all information which it did not have the statutory authority to receive.

The Centre's response. As mentioned in our response after paragraph 60, FINTRAC has taken concrete steps to limit the reception of information that should not have been sent to the Centre. The information that was received prior to these changes, and information that FINTRAC was not able to filter, currently remains in our database. We welcome the recommendation from the OPC to remove these records. The Centre recognizes the importance of ensuring that its database contains only information that FINTRAC is authorized to hold and we will continue to explore and develop new ways to achieve this goal.

The destruction of extraneous information that FINTRAC currently holds in its database, presents a technical challenge. The Centre is developing a strategy and a work plan to move forward the work in this area as quickly as possible. In addition, the upcoming undertaking of a data quality assessment exercise should support this work by assisting in developing ways to identify information that should be deleted. Being mindful that this work could require a long time span and represent a significant investment of resources, FINTRAC remains confident that risks of unauthorized use or disclosure of such information, whether through use in the Centre's processes, or by intrusion, are well mitigated by FINTRAC's policies and procedures and its highly secured IT systems, as was acknowledged by your office earlier in this report.

Privacy Management Framework

80. A privacy management framework refers to the checks and controls in place to ensure that personal information is managed appropriately. In previous audits, we have determined that the privacy management frameworks of government institutions are at varying levels of maturity.

81. While a model privacy management framework for federal departments has yet to be established, core elements include effective governance, clear accountability, a process for managing privacy breaches, identification and management of privacy risks, ongoing compliance monitoring and awareness training.

82. FINTRAC has implemented a suite of policies to manage information under its control. We reviewed the Centre's overarching privacy policy, as well as its security and information management policies. Although we noted examples of positive privacy practices, we did identify opportunities for improvement.

Accountability for privacy compliance needs to be established

83. The principles that govern the protection of personal information are set out in FINTRAC's privacy policy. While the policy assigns general responsibility to all employees, it does not establish overall strategic direction and oversight of privacy compliance activities at an executive level. As we have reported in other audits, a Chief Privacy Officer (CPO) is crucial as a central locus for privacy compliance and leadership.

84. While FINTRAC has a CPO in name, the incumbent is not a member of the Executive Committee. Moreover, although the position description includes a strategic function, it is primarily focused on managing the Centre's ATIP program, rather than on establishing and overseeing privacy compliance activities across the organization.

Process for managing privacy breaches is under development

85. A key feature of privacy management is the ability to identify, investigate and report on breaches involving the inappropriate collection, use, disclosure or disposal of personal information. The Treasury Board Secretariat has issued guidance to manage breaches appropriately.

86. Under FINTRAC's security policy, security breaches must be reported to the appropriate manager, even if there is only a suspicion of an occurrence. Managers are then required to assess the incident and

report to the Departmental Security Officer to resolve the matter, minimize the impact on all parties involved, and implement measures to mitigate future occurrences.

87. The security policy does not specifically address security incidents which result in a violation of privacy, nor does it set out a role for the privacy coordinator. At the time of the audit, FINTRAC was in the process of addressing this gap. Guidelines have been drafted that establish defined roles and processes to manage security incidents involving personal information.

Privacy risk management process needs to be formalized

88. In 2002, the Treasury Board Secretariat introduced a policy on Privacy Impact Assessments (PIAs) designed to ensure that privacy principles were considered for all new or substantially redesigned programs and services with privacy implications. The extent to which departments are compliant with the policy is dependent on the framework in place to effectively report all activities that may require privacy impact analysis.

89. We asked FINTRAC how and when it determines whether a PIA is required. We were told that any changes in IM/IT would immediately trigger a PIA, and that officials throughout the organization continually monitor the need for such assessments. A formal infrastructure to support PIA policy objectives and requirements has yet to be implemented and documented, with responsibilities and accountabilities fully defined. Until this is done, there remains the possibility that privacy risks will go undetected.

Privacy awareness training should be improved

90. Compliance with the spirit and requirements of the *Privacy Act* depends largely on how well it is understood by those responsible for handling personal information. Awareness and training are two elements essential to achieving the *Act*'s objectives.

91. Privacy and security awareness training is provided as part of FINTRAC's employee orientation program. In addition, a number of privacy-related training documents are available on the Centre's intranet site. These include a video discussing the importance of protecting personal information, fact sheets regarding privacy requests, and links to relevant websites. Although the Centre's efforts in this regard are noteworthy, we found that the course content lacks information on items such as core privacy principles in sufficient detail.

92. While the privacy coordinator has been engaged in training activities including regional compliance personnel, awareness sessions dedicated specifically to the obligations established under the *Privacy Act* have not been provided to all staff who handle personal information.

Personal information index is being updated

93. An individual's right to privacy includes control over the uses made of their information. When exceptions to this exist, the individual has a right to know what uses can be made of the information and for what purposes.

94. The *Privacy Act* requires that all uses and disclosures of personal information are recorded and accounted for publicly in an index of personal information. This index, *Info Source*, informs the public of what personal information is held by the government, how it is managed, and facilitates access to it.

95. The current edition of *Info Source* lists three unique Personal Information Banks for FINTRAC, two of which relate to human resources and were not part of this review. The description of the third, the Financial Intelligence Analysis Database, is out of date. Moreover, the management of personal information under the Centre's compliance program is not reflected in the index.

96. Although FINTRAC has yet to provide a full accounting of its personal information holdings in *Info Source*, we are satisfied that it is in the process of doing so. In April 2008, the Centre submitted a draft Personal Information Bank to Treasury Board Secretariat regarding the management of personal information collected under its compliance mandate, as well as an update to the Financial Analysis Database.

Recommendation: To strengthen its privacy management framework, FINTRAC should:

- appoint a senior executive as Chief Privacy Officer to provide strategic privacy leadership, and to coordinate and oversee privacy related activities;
- ensure that all initiatives and programs requiring privacy impact analysis are identified, reported and tracked;
- finalize and implement privacy incident guidelines to comply with breach reporting expectations established by the Treasury Board Secretariat; and,
- expand its security awareness initiatives to ensure that all employees that handle personal information or have privacy responsibilities receive specific training on core privacy principles and requirements surrounding privacy impact analysis.

The Centre's response. FINTRAC welcomes this recommendation. The Centre has already taken steps to strengthen its privacy management structure, and a member of its Executive Committee will be appointed Chief Privacy Officer.

As well, FINTRAC's ATIP Coordination team has been working on the development of privacy incident guidelines, and is also in the process of updating its privacy awareness training session to include more privacy-specific information for employees.

FINTRAC's Compliance Mandate

97. In addition to satisfying the client identification, record-keeping, third party determination and reporting requirements imposed by the PCMLTFA, reporting entities must implement a compliance program for meeting their obligations under the *Act*. FINTRAC has a mandate to ensure reporting entities comply with these statutory requirements, which it fulfils through various means, including compliance examinations.

98. We reviewed the Centre's management of personal information in the context of the on-site compliance examinations it undertakes, with specific emphasis on the collection and use of such information. We also examined the issue of consent. To that end, we selected a random sampling of files, with representation from various reporting sectors.

99. In keeping with established privacy principles, we expected FINTRAC to limit collection of personal information to that which is necessary to fulfil its compliance mandate, limit the use of such information to purposes authorized under the PCMLTFA and, where applicable, obtain the consent of the person to whom the information relates.

100. While we found FINTRAC collects and uses compliance-related personal information for the purpose of ensuring reporting entities meet their obligations under the PCMLTFA, a number of issues surfaced that warrant attention.

Data minimization practices are not consistently observed

101. Limiting the collection of personal information, or data minimization, is a fundamental element of data protection statutes. Data minimization, restricting the collection of information to that which is strictly necessary to fulfil an identified purpose, mitigates privacy risks. Simply stated, data not collected is data not at risk.

102. We examined a random sample of compliance examination files, the majority of which highlighted client identification, record-keeping, reporting and other deficiencies while observing data minimization practices. Notwithstanding, we found instances where there was no demonstrated need to retain certain types of records, examples of which appear in Exhibit D.

Exhibit D

- Letters to individuals capturing details of their investment portfolios;
- Listing of credit union members, dates of birth, dates accounts were opened, account numbers and types;
- Records relating to non-reportable transactions which included customer names, addresses, and currency amounts involved; and,
- Employee training records.

103. With the exception of records that are subject to solicitor-client privilege, FINTRAC has the undisputed authority to collect any information it requires to fulfil its compliance mandate. However, as noted above, we observed instances where examination files captured personal information in significant detail, and the information did not appear to be required in order to substantiate findings. To the extent possible, FINTRAC should collect only data that is necessary to assess an entity's adherence to the PCMLTFA even if the legal authority to collect more exists.

Recommendation: In keeping with privacy best practices, we encourage FINTRAC to observe the principle of data minimization in the execution of its compliance activities.

The Centre's response. FINTRAC agrees with this recommendation. The Centre recognizes that data minimization is an important principle and that is why it has specific policies and procedures in place to help frame the retention of information gained through compliance examinations. The Centre will continue reinforcing the importance of respecting this principle when training its compliance officers and when reviewing and updating its policies and procedures.

Consent is not meaningful

104. Consent is generally required for the collection of personal information and its subsequent use or disclosure. To make consent meaningful, the purposes must be stated in such a way that the individual can reasonably understand how information will be used or disclosed. Accordingly, an organization needs to describe its proposed practices in plain language, and advise the individual of the consequences of not providing consent.

105. FINTRAC relies upon the statutory authority provided under the PCMLTFA for its compliance-related collection activities, and any related use and disclosure of personal information. Consent is not sought from the parties whose financial transactions are the subject of reports, nor from individuals who act as contacts for reporting entities.

106. There is one exception. Where a reporting entity is located in a dwelling house (place of residence), FINTRAC must obtain consent prior to entering such premises to conduct a compliance examination. Otherwise, it must obtain a warrant issued under section 63(2) of the PCMLTFA.

107. The consent form requires, among other things, the individual's name, address and date of birth. While there is a provision to cancel consent, it is not clear that consent may be refused, nor the ramification of such a refusal. Moreover, the consent form does not indicate the purpose of collecting the date of birth, nor what uses will be made of it. This should be addressed in order to provide individuals with all information needed to make an informed decision.

Recommendation: The "Consent to enter a dwelling house for compliance examination" form should be amended to indicate the authority under which the information is being collected, the purpose of the collection, and the uses that will be made of the information.

The Centre's response. FINTRAC welcomes this recommendation, and in line with the *Privacy Act* and Code of Fair Information practices, will amend its "Consent to enter a dwelling house for compliance examination" form.

Personal information in transit at risk of interception

108. Prior to commencing an on-site compliance examination, FINTRAC requests copies of certain documents. The request, made via a standard notification of examination letter, instructs reporting entities to provide various documents (e.g. compliance policies and procedures and training materials), none of which contain personal information. Entities are directed to forward the records to the Centre by mail, e-mail or fax.

109. The letter also instructs the reporting entity to have certain records available for FINTRAC's perusal on the date of examination. These typically include financial transactions greater than $10,000, foreign currency exchange tickets, client information records and other documents which may include personal information. Notwithstanding the instruction provided in the letter, we found one instance where a reporting entity forwarded client records – containing names, addresses, social insurance numbers, account numbers and account activity – to the Centre by e-mail.

110. The use of encryption is critical to safeguarding information in transit. In the absence of specific instructions to the contrary, reporting entities may transmit unencrypted personal information to FINTRAC via open channels, running the risk of interception.

Recommendation: FINTRAC amend the notice of examination to include explicit instructions that reporting entities are not to transmit records containing personal information. In the event that there is a requirement to do so, FINTRAC should work with reporting entities to ensure that only secure transmission methods are used.

The Centre's response. FINTRAC welcomes this recommendation, and in line with the *Privacy Act* and Code of Fair Information practices, will take all reasonable steps to ensure that Reporting Entities do not use unsecured transmission methods to transmit personal information to FINTRAC.

Guidance provided by regulatory partners has not been reviewed for accuracy

111. To assist with its compliance activities, the Centre has entered into agreements with 17 national and provincial regulatory agencies. These agreements facilitate the exchange of:

    - the results of examinations undertaken by both parties relating to compliance with Part 1 of the PCMLTFA; and,
    - the actions taken by the entities to address compliance deficiencies.

112. Several regulators have issued Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) guidance to their respective memberships. We reviewed the guidelines issued by three of the 17 regulators with whom FINTRAC has an information sharing agreement. We found instances where guidelines encouraged client identification, monitoring and reporting activities which exceeded the requirements of the PCMLTFA.

113. Sharing compliance information between regulatory bodies assists organizations in meeting their respective mandates, minimizes potential duplication, and reduces the administrative and regulatory burden on reporting entities. However, the responsibility for ensuring compliance with Part 1 of the PCMLTFA ultimately rests with FINTRAC. It is therefore incumbent upon the Centre to ensure that any guidance issued in that regard does not exceed what the *Act* requires.

114. We requested that FINTRAC provide AML/ATF guidance that had been issued by its compliance partners. With the exception of the two national agencies, no other documents were found to be in the Centre's possession. Without reviewing all existing PCMLTFA guidelines FINTRAC cannot be assured that they promote practices that are consistent with the *Act*.

Recommendation: FINTRAC should analyze all PCMLTFA guidance issued by its federal and provincial regulatory partners to ensure that such guidance does not promote client identification, record-keeping and reporting obligations that extend beyond the requirements of the *Act*.

The Centre's response. While being mindful of respecting other regulators' fields of competency and powers, FINTRAC will continue working with its partners to ensure that any guidance issued regarding compliance with the PCMLTFA is consistent with the requirements established under that *Act*.

Conclusion

115. The *Privacy Act* and the PCMLTFA impose obligations on FINTRAC to respect the privacy rights of Canadians by placing limits on the receipt, collection, use and disclosure of personal information.

116. A privacy management framework is a means by which institutions ensure that their privacy obligations are met. FINTRAC has developed the elements of such a framework. However, it still needs to establish clear accountability and strategic privacy leadership, formalize risk-management processes and enhance privacy training and awareness.

117. We found that personal information obtained by FINTRAC is used solely for the purpose for which it had been acquired. Disclosures are tightly controlled and are made in accordance with the PCMLTFA. Therefore, we conclude that the Centre's use and disclosure practices respect privacy.

118. While FINTRAC is disposing of records in accordance with the PCMLTFA, we noted deficiencies in terms of the information the Centre has acquired and retains. Although FINTRAC has developed and implemented processes to manage personal information, they lack the rigour required to ensure its holdings are both relevant and not excessive. Consequently, the Centre has information under its control that extends beyond what the PCMLTFA allows.

119. FINTRAC fosters a strong corporate culture regarding matters of security and confidentiality and deploys various measures to protect its information holdings. We found no evidence that personal information could be compromised because of inadequate security safeguards. Notwithstanding, it is important to note that security is not synonymous with privacy.

120. Although sound security is a prerequisite for protecting privacy, the presence of security does not, in and of itself, guarantee it. It is not sufficient for organizations to assert that they have addressed privacy by ensuring that information is obtained and stored securely, and only used and disclosed for authorized purposes. It must consider the obvious – whether the information should ever have been obtained.

121. The Privacy Commissioner has previously stated that,

> We have no reason to doubt that FINTRAC does an excellent job of protecting the information it holds, but privacy involves more that protecting personal information. Privacy entails ensuring the amount of information that is collected is kept to an absolute minimum…[2]

122. To fully comply with the *Privacy Act*, FINTRAC must take steps to limit the acquisition of personal information to only that which is authorized under the PCMLTFA.

2 Submission to the Senate Standing Committee on Banking, Trade and Commerce on June 21, 2006.

About the Audit

Authority

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to undertake compliance reviews of the manner in which government institutions manage their personal information holdings and make recommendations that the Commissioner considers appropriate.

Pursuant to section 72.(2) of the PCMLTFA, the Privacy Commissioner is required to conduct a biennial review of measures taken by FINTRAC to protect information it receives or collects and report the results of such reviews to Parliament.

Objective

The objective of this audit was to assess whether FINTRAC has appropriate controls in place to protect personal information, and whether its processes and practices for managing such information comply with sections 4 through 8 of the *Privacy Act*.

Criteria

The criteria used to conduct the audit are based on the relevant authorities of the *Privacy Act*, the PCMLTFA, associated TBS policies and, where applicable, the ten fair information principles contained in Schedule 1 of the *Personal Information Protection and Electronic Documents Act.*

We expected FINTRAC to:

- have appropriate security measures in place to ensure that personal information is protected throughout its life cycle;
- limit the receipt, collection and use of personal information to that which is necessary for the execution of its mandate;
- restrict the disclosure of personal information to that which is authorized under the PCMLTFA;
- retain and dispose of personal information in accordance with governing authorities; and,

- clearly define roles and responsibilities for the protection of personal information and implement measures to ensure compliance with its privacy obligations.

Scope and approach

The audit included a review of FINTRAC's programs and information management processes to identify the areas where the impact on privacy was deemed to be significant.

We interviewed FINTRAC staff and reviewed policies, guidelines, analytical tools, training materials, physical and IT threat and risk assessments, information sharing agreements and privacy impact assessments. We also examined reporting processes, a sampling of reports, and disclosures to domestic organizations and foreign intelligence units.

We did not conduct an Electronic Vulnerability Assessment, nor undertake penetration testing of FINTRAC's network environment since these activities had been performed by the Communication Security Establishment of Canada and the results of which were included in the reports we examined.

Amendments to the PCMLTFA in December 2006 increased FINTRAC's ability to ensure reporting entities comply with their obligations under the *Act*. The amendments included the establishment of a registration system for money services businesses and the creation of an Administrative Monetary Penalty regime. As these programs were evolving at the time of the audit, they were not examined in significant detail.

We conducted audit activities at FINTRAC headquarters and at regional offices in Toronto and Vancouver. The audit work was substantially completed on March 30, 2009.

Audit team

Director General: Steven Morgan

Michael Fagan

Leslie Fournier-Dupelle

Raymond Brault

Kie Delgaty

Bill Wilson

Appendices

Appendix A: Reporting Entities

- Financial entities of all types (banks, credit unions, caisses populaires, etc.)
- Life insurance companies, brokers or agents
- Securities dealers, portfolio managers, provincially authorized investment counsellors
- Foreign exchange dealers
- Money services businesses
- Crown agents accepting deposit liabilities and/or selling money orders
- Accountants/accounting firms, real estate brokers/sales representatives involved in certain client-related activities such as receiving or paying funds on behalf of a client
- Casinos (except some temporary charity casinos)
- British Columbia notaries public (including notary corporations) and dealers in precious metals and stones
- Real estate developers

Source: FINTRAC Annual Report, 2007, p. 20.

Appendix B: Designated Information

FINTRAC case disclosures consist of *designated information* that identifies individuals or entities and their transactions. A disclosure includes any or all of the following:

- Name of person(s) and entity/entities involved in the transaction(s)
- Address of person(s) and entity/entities involved in the transaction(s)
- Date of birth and Citizenship
- Passport, record of landing or permanent resident card number
- Name address and type of business where the transaction(s) occurred
- Date and time of the transaction(s)
- Type and value of the transaction(s) including the amount and type of currency or monetary instruments involved
- Transaction, transit and account number(s)
- Name of importer or exporter, in the case of importation or exportation of currency or monetary instruments

On June 30, 2007 the definition of "designated information" was expanded to include:

- Attempted suspicious transactions
- Telephone number of the place of business where the transaction occurred
- Type of account involved in a financial transaction, and
- Name and address of all persons authorized to act in respect of the account (signing authority, power of attorney, etc.)
- Financial interest of person/entity involved for whom transaction was completed
- Name, address, electronic mail address and telephone number of each partner, director or officer of an entity involved in transactions or of an entity acting on their behalf, address and phone number of principle place of business
- Relationships between persons or entities involved in the transactions – or persons or entities acting on their behalf – and any other persons or entities
- Details of criminal records and charges laid against person(s) or entity/entities involved in the transactions or any person or entity acting on their behalf
- Name of person or entity suspected of directing the transaction

- Grounds on which a person or entity reported a suspicious transaction report
- Number and types of reports on which a disclosure is based
- Number and categories of persons or entities that made the reports
- Money laundering or terrorist financing indicators that FINTRAC relied upon to justify a disclosure

Source: FINTRAC Annual Report, 2007, p. 13.