Office of the
Privacy Commissioner
of Canada

# FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA

**Audit Report of the
Privacy Commissioner of Canada**

**Section 37 of the *Privacy Act***

**Section 72(2) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act***

FINAL REPORT

2013

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

613-947-1698, 1-800-282-1376
Fax 613-947-6850
TDD 613-992-9190
Follow us on Twitter: @PrivacyPrivee



Cat No. IP54-29/2013
ISBN 978-1-100-54619-3

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

# Table of Contents

# Main Points

## WHAT WE EXAMINED

The Office of the Privacy Commissioner (OPC) examined the progress that the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) made to address the recommendations from our 2009 audit. We also examined how FINTRAC manages personal information collected, received, used and disclosed in its capacity as a financial intelligence unit and also while carrying out its compliance function as required by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA or the Act).

We reviewed FINTRAC's personal information management policies, procedures and guidelines modified or established since the last audit. In addition, we examined privacy impact analyses, training materials, compliance examination files, security assessments and information sharing agreements. We also reviewed a purposive sample drawn through a statistical random selection of all types of reports that FINTRAC receives, as well as information it discloses to law enforcement agencies, federal departments and foreign financial intelligence units.

Finally, we examined changes in 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

As of March 2012 there were approximately 165 million reports containing personal information in FINTRAC's databases. The databases include reports: where there is a suspicion of money laundering or terrorist activity financing; cash transactions over a prescribed threshold; certain electronic funds transfers; movements of currency or monetary instruments in specified circumstances or their seizure; and information provided by foreign or domestic counterparts. These reports might include transactions such as, but not limited to, down payments for house and vehicle purchases, wire transfers received by international students residing in Canada, or funds sent by parents in Canada to children who are studying abroad.

Persons and entities in various sectors (see Appendix 1), which are subject to the Act, must scrutinize and report on the financial transactions of clients. These entities, potentially up to 300,000 in number, transmit reports containing Canadians' sensitive personal information to FINTRAC. Some of these reports may be submitted without the knowledge of the individuals concerned. Reporting entities do not require the individuals' consent to submit the reports and the information may not be accessible to those individuals.

Our 2009 audit identified weaknesses in FINTRAC's personal information management practices and recommended that they be addressed. Our previous recommendations and those included in this report are intended to assist FINTRAC in meeting its obligations under the *Privacy Act*.

## WHAT WE FOUND

While FINTRAC continues to have sound security controls, we found that it has made limited progress in addressing five of ten audit recommendations made in 2009.

We examined two of FINTRAC's areas of responsibility. The first is its role to analyze and disclose financial intelligence. The second is a compliance function where it verifies whether reporting entities are meeting their obligations under the PCMLTFA and its regulations.

In carrying out its analysis and disclosure functions, FINTRAC continues to receive and retain personal information not directly related to its mandate. Plans to enhance current controls, including front-end screening and ongoing monitoring of reports, have yet to be implemented. Until these controls are implemented, FINTRAC will be unable to provide assurance that its information holdings are relevant to its mandate and not excessive.

We found that FINTRAC has enhanced its process to manage threat and risk assessments. Likewise, it has a comprehensive approach to security, including controls to safeguard personal information. However, instances of non-compliance with established security policies were noted during the audit.

FINTRAC has enhanced its privacy management program. It has created a formal Chief Privacy Officer position, a privacy impact assessment process and privacy breach guidelines have been developed. FINTRAC has also enhanced employee awareness of core privacy principles.

FINTRAC receives inquiries that deal with interpretation and practical application of the PCMLTFA and its regulations from reporting entities. We found an instance where FINTRAC's guidance could be interpreted as encouraging the reporting of information that is not required by the PCMLTFA.

As part of its compliance function, FINTRAC obtains records from reporting entities. Although FINTRAC issued internal guidelines to ensure that the collection of data is limited to what is directly related to its operating programs and activities, we found instances where this practice is not consistently applied, resulting in the collection of data where there was no demonstrated need to collect and retain it.

FINTRAC has responded to our findings. Its 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. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA or the Act) was enacted in 2000. This legislation established the Financial Transactions and Reports Analysis Centre (FINTRAC) as Canada's financial intelligence unit.

2. Amendments to the PCMLTFA in 2006 increased both the number of organizations subject to the *Act* and the types of transactions which are analyzed and reported. The amendments also enabled FINTRAC to disclose more information to law enforcement and security organizations, as well as to the Canada Border Services Agency (CBSA) and the Canada Revenue Agency (CRA). In February 2011, the *Jobs and Economic Growth Act* amended the thresholds of designated information that FINTRAC can disclose to CRA and CBSA.

3. At the time of our audit, the PCMLTFA was undergoing a five-year parliamentary review, as required under section 72(1) of the Act.

4. The Act requires persons and entities, potentially up to 300,000 in number, which fall into one of ten sectors (see Appendix 1) to collect and maintain specific information about their clients and their transactions. These persons and entities are also required to transmit reports containing sensitive personal information to FINTRAC.

5. The Act also establishes a requirement to report the cross border movement of currency or monetary instruments with a value equal to or greater than $10,000, or its equivalent in foreign currency. Currency or monetary instruments that are seized by CBSA, regardless of value, are also reported to FINTRAC.

## ABOUT THE AUDIT ENTITY

6. FINTRAC is an independent agency reporting to the Minister of Finance and operating at arm's length from law enforcement and other entities to which it is authorized to disclose information. Created in 2001, FINTRAC's mandate is to receive, collect, analyze, assess and disclose information on financial transactions, and to disseminate intelligence in order to assist in the detection, prevention and deterrence of money laundering and terrorist financing activities. FINTRAC's legislative responsibilities under the PCMLTFA include protecting the personal information under its control.

7. FINTRAC is also required to analyze and disclose information relevant to its mandate and it must undertake a compliance program to ensure reporting entities meet their obligations under the PCMLTFA and regulations.

8. FINTRAC has approximately 352 employees. As of June 30, 2012, FINTRAC had an annual budget of $54.0 million. Further information about FINTRAC is available on its website at http://www.fintrac-canafe.gc.ca.

## WHAT WE FOUND IN OUR 2009 AUDIT

9. In 2009 the OPC found that FINTRAC had received and retained information that exceeded its legislative authority. FINTRAC's controls, including the screening and ongoing monitoring of reports, needed to be improved to ensure that FINTRAC's information holdings are both relevant and not excessive. FINTRAC had a robust and comprehensive approach to security. It had put into place elements of a privacy management framework; however, there were gaps which needed to be addressed. We had also found that FINTRAC was unable to provide assurance that the guidance provided by regulatory partners to reporting entities is consistent with PCMLTFA requirements.

10. The progress made by FINTRAC to address the 2009 audit recommendations is presented in the Observations and Recommendations section of this Report.

## FOCUS OF THE CURRENT AUDIT

11. The audit objective was to assess whether FINTRAC has adequate controls to protect personal information, and whether its processes and practices for managing such information comply with the fair information practices embodied in sections 4 through 8 of the *Privacy Act*. The act of "collection" under the terms of the *Privacy Act* includes both the passive receipt and the active collection of personal information.

12. The audit focused on reviewing the progress made by FINTRAC to address the recommendations from our 2009 audit. We also examined FINTRAC's management of personal information acquired, used and disclosed in its capacity as a financial intelligence unit and also while carrying out its compliance function as required by the PCMLTFA.

13. We did not review FINTRAC's handling of personal information about its employees nor did we assess the control frameworks implemented by reporting entities to manage their personal information holdings.

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

# Observations and Recommendations

## COMPLIANCE WITH THE CODE OF FAIR INFORMATION PRACTICES

15. The *Privacy Act* sets out the rules governing the management of personal information held by federal government institutions. Sections 4 through 8 of the *Privacy Act*, referred to as the "Code of Fair Information Practices", restrict the collection of personal information and limit how that information, once collected, can be used and disclosed. The *Privacy Act* also addresses the retention and disposal of personal information. It balances the legitimate collection and use requirements necessary to government programs with an individual's right to privacy.

16. To assess the extent to which FINTRAC is meeting its obligations under the *Privacy Act*, we looked at how FINTRAC manages personal information that it acquires. We expected to find that:

    - the receipt and collection of personal information is limited to what is directly related to its operating programs or activities;
    - the information is used and disclosed for authorized purposes; and,
    - records are retained and disposed of in accordance with established schedules.

### Little progress has been made to address over reporting

17. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA or the Act) authorizes FINTRAC to receive information, including personal financial information, from individuals, reporting entities and other sources, such as the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and other police forces. It also permits FINTRAC to collect information it considers relevant to money laundering or terrorist financing activities, as well as information required to fulfill its compliance mandate. In March 2009, FINTRAC's databases contained approximately 101 million reports; this number increased to approximately 165 million reports by March 2012.

18. The Act requires that certain financial transactions undertaken by or on behalf of a single person or entity be reported to FINTRAC. Among the data that must be supplied to FINTRAC are cash transactions, international electronic funds transfers and casino disbursements worth $10,000 or more, as well as transactions that, while individually lower than $10,000, collectively exceed this amount within a 24-hour period, also known as the 24-hour rule. Terrorist property reports and suspicious transactions, regardless of value, must also be reported. Reported transactions might include down payments for house and vehicle purchases, wire transfers received by international students residing in Canada, or funds sent by parents in Canada to children who are studying abroad. Reporting entities that do not file reports as required by the PCMLTFA are in non-compliance and could face civil or criminal sanctions.

19. Cross border movements of currency or monetary instruments worth $10,000 or more are also reported to FINTRAC by the Canada Border Services Agency (CBSA).

20. Information concerning suspicions of money laundering and terrorist financing activities is also provided on a voluntary basis by members of the public. As well, FINTRAC receives information from law enforcement and security agencies as part of their own investigations.

21. In our 2009 audit we found that FINTRAC received and retained personal information that it had no legislative authority to receive and that it did not need or use. This information included:

    - Reports that did not meet the $10,000 reporting threshold and therefore should not have been reported;
    - Suspicious Transaction Reports (STRs) that did not demonstrate "reasonable grounds to suspect" money laundering or terrorist financing;
    - Voluntary Information Records (VIRs) where no grounds for suspicion of money laundering or terrorist financing were evident; and,
    - Extraneous personal information, such as Social Insurance Numbers (SIN), health card numbers and medical information that should not have been reported.

22. Our 2009 audit also found that with the exception of VIRs, FINTRAC's screening processes were designed primarily to address issues of data quality—whether all required fields in reports were completed—and did not address whether the information was relevant to FINTRAC's mandate or whether the information was excessive in nature.

23. We recommended that FINTRAC take steps to limit the acquisition of personal information to that which is authorized under the PCMLTFA and that it needs or uses. In responding, FINTRAC agreed to the recommendation and advised that through its new reporting system it would improve ways to validate reports as they are transmitted to it and further reduce the potential of receiving information that should not have been sent. It also stated that it had built-in enhanced front-end screening in the new Casino Disbursement Report form which should further assist in preventing this type of information from entering FINTRAC's database and that it regularly reviewed and updated the guidance offered to reporting entities. FINTRAC indicated that it felt that this plus the other steps already taken would be effective in reducing the amount of information which it acknowledged is incorrectly sent to it. FINTRAC committed to undertake a review of its reporting forms to evaluate the analytical value of data elements being captured and minimize the reporting burden to reporting entities. To assess progress, we interviewed FINTRAC officials and reviewed a purposive random sample of reports and VIRs received by FINTRAC, as well as internal reports and operational plans.

24. Ninety-eight percent of the reports FINTRAC receives are comprised of Large Cash Transaction Reports (LCTR) and international Electronic Funds Transfer Reports (EFTR). We selected a purposive sample of LCTRs and EFTRs drawn through statistical random selection to verify that the reports met the $10,000 threshold (either, as 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). We identified a number of reports that did not meet the threshold and asked FINTRAC to provide the corresponding reports that would collectively meet or exceed $10,000. In responding, FINTRAC indicated that the situation had not changed since our 2009 audit, i.e. it still does not have the technological capacity to match reports electronically. FINTRAC further stated that the process of matching the reports we identified would have to be conducted manually and such a review would be resource intensive and time consuming. Accordingly, the extent to which FINTRAC's information holdings are populated with reports that do not meet the $10,000 reporting threshold remains unknown.

25. Similarly, we found international Electronic Funds Transfer Reports and Canada Border Services Agency (CBSA) cross border currency and monetary instruments reports that did not meet the $10,000 reporting threshold.

26. In addition, we identified STRs where there was no reasonable grounds to suspect money laundering or terrorist financing activities; see examples below in Exhibit A. In each case, a report was sent to FINTRAC and FINTRAC retained the report in its database.

**Exhibit A – Examples of excessive reporting to FINTRAC**

- A young professional cashed three bank drafts worth almost US$ 100,000 purchased from a major Canadian bank. The issuing bank confirmed the validity of the drafts. The manager of the Money Services Business where the drafts were cashed obtained satisfactory answers to various questions on the transaction but filed a Suspicious Transaction Report (STR) with the explanation that "*the amount of money simply did not match his age.*"
- An individual, who purchased a home from his childhood friend, released the deposit directly to the seller instead of to the seller's lawyer. The notary who reported the transaction stated: "*this is a long time client of mine and I have no reason to suspect money laundering or terrorist activity but as I was not sure whether the following (as described above) needed to be reported or not, I thought it best to do so.*"
- An individual wanted to exchange €5,000 to Canadian currency. The STR stated that in order to dissuade the individual from completing the transaction, the individual was informed that the full amount would be frozen for 21 days. The report further stated that the client decided not to proceed with the transaction.

27. We also noted that a number of reports did not include the entity's reason for suspected money laundering or terrorist financing activities. The absence of such information renders it difficult to assess whether the "reasonable grounds" threshold has been met. Examples of such reports are provided below in Exhibit B:

**Exhibit B – Examples of reports lacking reasonable grounds for suspicion**

- A financial institution filed an STR when a storekeeper deposited $570 in $100, $50 $20 and $5 bills without indicating why the transaction was considered suspicious.
- A jackpot worth $10,000 was won but was not awarded due to the winner not having photo identification at the time it was claimed. An STR was filed by the casino.

28. 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. The guidelines also provide that although the Social Insurance Number (SIN) can be used to verify the identity of a client, the number is not to be provided to FINTRAC on any type of report. Notwithstanding this guidance, we found instances where FINTRAC received and retained SINs and certain health card numbers in some reports we examined.

29. FINTRAC has implemented a front-end screening system to ensure all mandatory fields are completed in reports when submitted electronically. When such fields are incomplete, the reports are returned to the reporting entity. All other reports and records are accepted regardless of whether the monetary reporting threshold is met, or there are reasonable grounds to suspect money laundering or terrorist financing activities. FINTRAC indicated in the event that one of its analysts notes a report that does not meet the various reporting thresholds specified in the PCMLTFA, the report is segregated.

However, as previously stated, we found a number of reports that FINTRAC was unable to demonstrate met the reporting threshold. The full extent of FINTRAC's databases that are populated with such reports remains unknown.

30. Although FINTRAC has stated that it has an obligation under the PCMLTFA to receive and retain any report or information that it has been provided, regardless of whether it should have been reported, Section 4 of the *Privacy Act* requires government institutions to limit the collection of information to only that which relates directly to an operating program or activity. In other words, institutions should not collect information that is not required to fulfill their mandates. Furthermore, Treasury Board Secretariat policy states that government institutions must have a demonstrable need for each piece of personal information collected in order to carry out the program or activity. Given both the volume and the sensitivity of the information it receives and collects we would expect that FINTRAC ensures that the information is both relevant and not excessive.

31. The PCMLTFA obligates FINTRAC to analyse and assess reports it receives. FINTRAC has stated that its obligation in this regard is to analyse and assess reports to determine whether the information should be disclosed to law enforcement or security partners as part of a financial intelligence disclosure. To reconcile the PCMLTFA with the requirements of the *Privacy Act*, FINTRAC is obligated to analyse and assess reports for the purpose of ensuring that it does not accept and retain information that is not within the parameters and thresholds set out by the PCMLTFA. Unless there is a process in place for doing so, FINTRAC will continue to receive and retain information that it does not need or use in an operating program or activity.

32. In 2009, we recommended that FINTRAC should continue to enhance the processes for front-end screening of reports and develop a complementary program of ongoing monitoring and review. FINTRAC agreed to this recommendation. As little action has been made in this regard, we assess FINTRAC's progress to address the recommendation, regarding excessive reporting, as unsatisfactory (See Exhibit C).

## 33. RECOMMENDATION

To reconcile its obligations under the PCMLTFA with those under the *Privacy Act,* FINTRAC should analyse and assess incoming reports to ensure that it receives and retains only information that it has the legislative authority to receive and which it needs or uses in an ongoing program or activity.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC meets its obligations under the PCMLTFA and the* Privacy Act *while fulfilling its mandate to assist in the detection, prevention and deterrence of money laundering and terrorist financing. Paragraph 54(a) of the PCMLTFA provides the obligation and requirement for FINTRAC to receive incoming reports, and paragraphs 54(d) and 54(e) require FINTRAC to keep the information contained in those reports for a minimum of 10 years. FINTRAC acknowledges that within the required reports, reporting entities do, in some instances, send personal information that should not be included. FINTRAC has a defined analytical process to ensure that this personal information is not used for the purpose of analysis and is thus not disclosed to police, law enforcement or security partners, as recognized by the OPC at paragraph 53 of this report.*

*With respect to reports that do not meet the legislated threshold for reporting, a process is in place to destroy them according to FINTRAC's disposition schedules. FINTRAC will review its disposition schedules in the near term to ensure that this information is assessed and destroyed in the most practical timeframe possible.*

*FINTRAC will review its disposition schedules, which is expected to be completed in the fall of 2014.*

34. When a person in Canada or Canadian outside Canada has knowledge that property is owned or controlled by a terrorist or terrorist group, they must, pursuant to the *Criminal Code*, disclose this information to the RCMP and CSIS. Entities subject to the PCMLTFA must also complete and submit a Terrorist Property Report (TPR) to FINTRAC. Two situations can trigger the requirement to send a TPR to FINTRAC: a) knowing that property is owned or controlled by or on behalf of a terrorist or terrorist group, or b) believing that property is owned or controlled by or on behalf of a listed person. Lists of designated persons and groups that are known terrorists are published by Public Safety Canada and the Office of the Superintendent of Financial Institutions for verification purposes to assist entities in making such determinations.

35. In our 2009 audit we found that almost half of the TPRs were filed on the basis of a "possible match" to terrorist listings. Where identity could not be confirmed, FINTRAC did not pursue further analysis; however, the information remained in FINTRAC's database. The practice, by default, was to retain these reports regardless of whether or not there was knowledge, belief or suspicion of terrorist affiliation.

36. We reviewed a sample of TPRs and, as in our previous audit, we found instances where these reports were submitted to FINTRAC on the basis of a "possible match to terrorist entity listings." As reported in 2009, FINTRAC retains all such reports and keeps them accessible in its databases.

37. In 2009 we recommended that FINTRAC 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. In its response, FINTRAC indicated it welcomed the recommendation and committed to enter into dialogue with its intelligence partners to explore ways to mitigate the risk of retaining information about an individual once it has been confirmed that no terrorist affiliation exists.

38. FINTRAC advised us that it requested law enforcement and security agencies to inform it when, in the course of their investigations, they confirm that there is no terrorist affiliation with regard to a specific individual. FINTRAC is notified of this through a Voluntary Information Record (VIR). We were further informed that when an individual is confirmed as not being a terrorist, the VIR would be flagged in FINTRAC's database so that an analyst would not proceed with further analysis on that individual. As efforts have been made to confirm whether terrorist affiliations exist, we assess progress on our recommendation as satisfactory (Exhibit C).

39. FINTRAC has an outreach program for providing guidance to reporting entities. This includes the publication of guidelines, interpretation notices, annual workshops, and brochures, as well as a call centre and an email address to respond to specific questions and clarifications on PCMLTFA obligations. Despite these efforts, our audit has found that excessive reporting continues to be an issue. Specifically, as reported above, entities continue to submit:

    - Reports that did not meet the $10,000 reporting threshold; and,
    - Suspicious Transaction Reports (STRs) that did not demonstrate "reasonable grounds to suspect" money laundering or terrorist financing activities.

In addition, as noted in our 2009 audit, FINTRAC has received Voluntary Information Records from the public where no suspicion of money laundering or terrorist financing activity was evident.

## 40. RECOMMENDATION

FINTRAC should assess the effectiveness of its outreach programs and strengthen them where necessary to mitigate the risk of receiving personal information beyond the parameters and thresholds specified by the PCMLTFA.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC assesses the effectiveness of its outreach program and continually strengthens it through additional and/or revised components that detail reporting entities' obligations under the PCMLTFA. This comprehensive outreach program also informs reporting entities of information that they are not required to report to FINTRAC. Ways in which FINTRAC provides this outreach, in addition to the items outlined include:*

- *Having a Major Reporters Unit responsible for managing FINTRAC's relationship with the largest of the reporting entities in the banking sector;*
- *Holding sector-specific consultations, such as with the Credit Union sector on guidance related to the implementation of a risk based approach and the upcoming regulations for customer due diligence, and with the Money Services Businesses, which prompted MSB specific guidance being published;*
- *Making sector-specific information on reporting entities' obligations, formal guidelines, and FINTRAC Interpretation Notices available on FINTRAC's website;*
- *Participating in meetings with industry associations, regulators, and law enforcement partners, including the bi-annual Public/Private Sector Advisory Committee.*

*While FINTRAC provides outreach on personal information that reporting entities are required to send, the obligation remains with the individual reporting entities to not send information not required by the legislation and regulations. FINTRAC agrees that this issue should be addressed and it therefore will continue to support the OPC in their efforts to ensure that those reporting entities which are subject to the* Personal Information Protection and Electronic Documents Act *meet the requirements set out in that Act. Given the above, FINTRAC has addressed this recommendation and will continue to do so in the future.*

41. FINTRAC provides guidance to reporting entities on its website. It has also cooperated with this Office to develop guidance for financial institutions regarding privacy and the PCMLTFA (http://www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp). In addition, FINTRAC regularly receives inquiries from reporting entities regarding the interpretation and practical application of the PCMLTFA and its regulations. Periodically, FINTRAC summarizes the questions and answers provided to reporting entities in the financial sector and this information is shared with the sector regulator.

42. We examined whether FINTRAC's guidance documents and communications provided to regulators and reporting entities were fully compliant with PCMLTFA and the *Privacy Act*. This guidance is important as it is used by the reporting entities to meet their obligations under the PCMLTFA.

43. We found that in responding to a major financial institution's question regarding the submission of documentation supporting a Large Cash Transaction Report, FINTRAC acknowledged that although the data in question was information that technically should not be included and would certainly cause problems in regards to privacy, it may be of added value to have additional information on the transaction for intelligence or analytical purposes.

44. FINTRAC's reply to the financial institution indicated that the acquisition of additional information not directly related to its operating programs or activities could have value for intelligence purposes. In this instance, FINTRAC did not discourage the institution from reporting additional information. There is a risk that a reporting entity could interpret the message conveyed by FINTRAC in the above example as applying to other types of reports and information.

45. Moreover, this guidance had the potential to be disseminated within a wide audience of the financial sector. Given that reports submitted by reporting entities in the financial sector represent more than 90% of the reports received by FINTRAC, this advice could have a significant impact on FINTRAC's information holdings by increasing the risk of personal information being sent that is not directly related to its operating programs and activities.

46. Although this instance is not indicative of a systemic problem, we raised the matter with FINTRAC. In responding, officials indicated that in order to minimize the likelihood of any misinterpretation FINTRAC will strive to provide clear wording in compliance documents it issues.

**Exhibit C – Progress in addressing our 2009 Audit Report recommendations on compliance with the Code of Fair Information Practices—Information Acquisition**

| 2009 RECOMMENDATIONS | PROGRESS |
|---|---|
| FINTRAC should work with reporting entities to ensure that FINTRAC 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.<br>(Recommendation following paragraph 60 of the *2009 Audit Report of the Privacy Commissioner of Canada, Financial Transactions and Reports Analysis Centre*) | Unsatisfactory |
| 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.<br>(Recommendation following paragraph 65 of the 2009 audit report) | Satisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

## Criteria for FINTRAC to disclose certain information have been formalized

47. Under section 55 of the PCMLTFA, once FINTRAC has determined that reasonable grounds to suspect that information would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, FINTRAC must disclose the information to the appropriate police force. Under section 55.1, 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.

48. FINTRAC must also disclose "designated information" (see Appendix 2) to the Canada Border Services Agency (CBSA), the Communications Security Establishment of Canada (CSEC) and the Canada Revenue Agency (CRA) when there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence and when other government institution specific criteria stated in subsection 55(3) of the PCMLTFA are met.

49. At the time of our 2009 audit, FINTRAC was developing criteria that would identify transactions indicative of potential evasion to pay taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue, for disclosures to CRA. However, we found that no written criteria existed to guide when the threshold for disclosures to CBSA or CSEC had been met. We recommended that FINTRAC establish a set of written criteria to guide in the determination of when the threshold for disclosures to CBSA and CSEC had been met.

50. To assess progress, we obtained a copy of the written guidelines that FINTRAC developed for disclosures to the CBSA, CSEC and CRA. These guidelines are now in place and outline the considerations and criteria that must be met before disclosing designated information (see Appendix 2) to these organizations as specified in subsection 55 (3) of the PCMLTFA.

51. Therefore, we found progress on our recommendation regarding formalization of criteria for these types of disclosures as satisfactory (See Exhibit D).

**Exhibit D – Progress in addressing our recommendation on compliance with the Code of Fair Information Practices—Information Use and Disclosure**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| 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.<br>(Recommendation following paragraph 70 of the 2009 audit report) | Satisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

## Use and disclosure practices comply with governing legislation

52. 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 those purposes. The *Privacy Act* also limits the circumstances under which personal information can be disclosed without consent. FINTRAC's authority to use and disclose information is outlined in sections 54 to 65.1 of the PCMLTFA.

53. During our previous audit, we examined a sample of files, including analytical reports that accompanied disclosure recommendations. We found no evidence that personal information had been used for a purpose other than that for which it was obtained, or for a use inconsistent with that purpose. Moreover, we found that disclosures were tightly controlled and made in accordance with the PCMLTFA.

54. As part of this audit, we examined a purposive sample of files. As was the case in our previous audit, we found that disclosures were controlled and made in accordance with the PCMLTFA.

## Current practices continue to contravene the limiting retention principle

55. The *Privacy Act* requires that the collection of personal information must be directly relevant to an operating program or activity of an institution. Relevance is determined by statutory authority. Treasury Board Secretariat policy states that government institutions must have a demonstrable need for each piece of personal information collected in order to carry out the program or activity.

56. As mentioned in paragraphs 24 to 29 in this report, FINTRAC continues to receive and retain information that exceeds the parameters and thresholds specified in the PCMLTFA. Retaining personal information beyond what is directly related to a mandate contravenes the *Privacy Act*, Treasury Board Secretariat policy, and the limiting retention principle. This presents a significant risk to privacy by making accessible personal information which should never have been obtained.

57. FINTRAC's Privacy Policy states that, in accordance with paragraph 54(d) of the PCMLTFA, it must retain all reports received from reporting entities and all other information received or collected for a minimum of 10 years. Fifteen years following the receipt of a report, FINTRAC must destroy any identifying information contained in that report if the report was not disclosed.

58. In our 2009 audit, we recommended that FINTRAC permanently delete from its holdings all information that it did not have the statutory authority to receive. In responding, FINTRAC welcomed the recommendation to remove the records. It did, however, indicate that the destruction of the information presented a technical challenge. At that time, FINTRAC indicated that it was developing a strategy and work plan to address the recommendation as quickly as possible.

59. To assess progress, we reviewed disposal reports, operational plans, the level of implementation for retention and disposition projects, and interviewed officials. We found that FINTRAC has developed a plan to identify and either segregate or dispose of information.

60. The first phase of this project involved the identification and disposal of reports that have not been part of a disclosure and are 10 years or older. In March 2012 FINTRAC manually identified and ran a one-time disposal of reports received from February 10, 2002 to March 16, 2002 that had reached their ten-year anniversary date and had not been disclosed. No further disposal activity has taken place. FINTRAC advised us that the process of identifying and disposing of these types of reports is to be automated in the second phase of the project.

61. The second phase is in the planning stage and includes the segregation of reports or information that should not be in FINTRAC's databases. FINTRAC has advised us that this data will not be deleted, but rather kept in a separate database that will not be accessible to analysts.

62. FINTRAC acknowledged that only a very limited number of records will be identified through this process, which will be manually completed, since it will only isolate reports that are actually accessed as part of its analysis and disclosure program. As a result, many reports, including those that are not directly related to an operating program or activity, will remain accessible in FINTRAC's data holdings until they are destroyed according to the previously described disposition requirements—for a minimum of 10 years.

63. FINTRAC's plan to segregate records into a separate database does not address our 2009 recommendation. Personal information that FINTRAC should not have received under the PCMLTFA and the *Privacy Act* is retained in its databases. Accordingly, we assess progress on our recommendation regarding the limiting retention principle as unsatisfactory (See Exhibit E).

**Exhibit E – Progress in addressing our recommendation on compliance with the Code of Fair Information Practices—Information Retention and Disposal**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| To bring itself into compliance with the PCMLTFA and the *Privacy Act,* FINTRAC should permanently delete from its holdings all information for which it does not have the statutory authority to receive.<br>(Recommendation following paragraph 79 of the 2009 audit report) | Unsatisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

## 64. RECOMMENDATION

FINTRAC should identify and dispose of information that it should not have received and is not directly related to its operating programs and activities.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC has a process in place for addressing information that reporting entities should not have sent to FINTRAC. Paragraph 54(a) of the PCMLTFA requires FINTRAC to receive reports sent by reporting entities. Paragraphs 54(d) and 54(e) also set authorities with respect to retention and disposition of the information contained in incoming reports. While FINTRAC is required to receive and retain this information, it also has a defined analytical process that ensures that personal information that should not have been included in reports by reporting entities is not used for the purpose of analysis.*

*With respect to reports that do not meet the legislated threshold for reporting, a process is in place to destroy them according to FINTRAC's disposition schedules. FINTRAC will review its disposition schedules in the near term to ensure that this information is assessed and destroyed in the most practical timeframe possible.*

*FINTRAC will review its disposition schedules, which is expected to be completed in the fall of 2014.*

### Retention policy has not been developed for some records

65. We found that a retention policy has not been developed for records and information that are not covered under the retention and disposition set out in the PCMLTFA, such as compliance examination files and financial analysis and disclosure administrative files (excluding financial transaction reports).

66. The retention and disposition of this data is managed in accordance with FINTRAC's Information Management Policy. FINTRAC is currently negotiating a Records Disposition Authority (RDA) with Library and Archives Canada (LAC) to address the archiving and disposal of operational records. Accordingly, no retention and disposal policy can be implemented until the Terms and Conditions document with Library and Archives Canada is formalized.

## 67. RECOMMENDATION

FINTRAC should: a) finalize an agreement with LAC regarding terms and conditions for the transfer of its archival records, and b) implement a formal retention and disposal policy for information and records whose retention and disposal periods are not specifically covered by the PCMLTFA.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. With respect to a), FINTRAC will work with LAC to finalize an agreement. However, it should be noted that FINTRAC and LAC jointly came to agreement on Terms and Conditions (T&Cs) required for FINTRAC to obtain its Records Disposition Authority (RDA) in the spring of 2012. The T&Cs were signed by FINTRAC and forwarded to LAC for their signature and approval. Since then, LAC's processes in regards to the issuance of RDAs have changed, and therefore, additional revision is underway to ensure that the finalized Disposition Authorization reflects the new process.*

*With respect to b), FINTRAC is actively working with internal stakeholders and LAC in defining the record disposition schedules that will be in compliance with the Treasury Board Record-keeping directive. FINTRAC would like to clarify that all reports in its database remain within the 15-year timeframe prescribed by the PCMLTFA at which point it is required to destroy the identifying information contained in financial transaction reports that have not been disclosed.*

*FINTRAC commits to working with LAC to finalize an agreement and to define record disposition schedules and draft the necessary policies. Timeframe for completion of this commitment is dependent on LAC.*

## SAFEGUARDING PERSONAL INFORMATION

68. Safeguarding personal information is a key component in meeting the protection requirements established under the *Privacy Act*. Appropriate measures and controls ensure that personal data is not subject to unauthorized use, disclosure, alteration or destruction.

69. The Treasury Board Secretariat's Policy on Government Security (PGS), which prescribes safeguards to protect and preserve the confidentiality and integrity of government assets including personal information, establishes baseline (mandatory) security requirements. This policy requires federal departments and agencies to conduct their own assessments to determine whether safeguards above baseline levels are necessary. The PGS also calls for ongoing monitoring of the threat environment to ensure appropriate security measures are maintained.

70. We expected to find that FINTRAC maintains a sound physical security infrastructure and personnel security screening process, as well as a comprehensive Information Technology (IT) security management framework to safeguard personal information it collects or receives. We examined policies, procedures, risk assessments and access controls. We also conducted physical inspections at headquarters and during our visits to regional sites.

71. **Physical security.** We found that FINTRAC uses protection mechanisms such as alarms, cameras and guards to secure its facilities and assets. Sensitive information is stored and operations are conducted within secure zones. A clean desk policy is enforced through regular security sweeps; violations are recorded and reported to the Departmental Security Officer.

72. **Personnel security.** We found that FINTRAC has established processes to grant, remove and modify access to assets for new and departing personnel, including those on extended leave or changing roles within the organization. We reviewed a sample of personnel files for current and former employees, contractors and students; and found that personnel screening and termination processes are in accordance with policy.

73. **IT applications and systems.** We found that FINTRAC maintains a sound IT security infrastructure to protect its networks and applications. This includes perimeter security, segregation of networks and strong access controls. Physical and technical controls are complemented by processes including risk and vulnerability assessment and remediation, incident response, change management and a mature Certification and Accreditation (C&A) program. As required by Treasury Board Secretariat policy, certification verifies that mandatory security requirements for an IT system are applied. It also verifies that controls and safeguards to protect data are functioning as intended. Accreditation signifies that management has authorized operation of the system and has accepted any residual risk.

## Management of security and threat and risk assessments has been enhanced

74. In our previous audit, we observed that FINTRAC commissioned third parties to conduct physical security and threat and risk assessments (TRAs). Although FINTRAC demonstrated that the issues raised by these assessments were addressed, in 2009 we found that 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.

75. We recommended that FINTRAC ensure that all actions taken to address observations noted in TRAs or security assessments are appended to the documents of record. In addition, we recommended that management formally acknowledge and accept the risks identified in these assessments.

76. To assess progress we examined the Security Recommendations Repository, status reports presented to senior management, records of decision, certification reports and accreditation letters. We also held meetings with FINTRAC security officials.

77. We found that FINTRAC has made satisfactory progress on this recommendation. It has implemented an oversight process to document all aspects of the security reviews and TRAs and tracks progress against all recommendations. FINTRAC was in the process of implementing procedures to manage observations highlighted in these security reviews and TRAs. These procedures assign responsibility and accountability for ensuring recommendations are addressed, and include a process to verify that any residual risks are accepted by senior management.

78. We, therefore, assess progress on our recommendation on the management of observations from security assessments as satisfactory (See Exhibit F).

**Exhibit F – Progress in addressing our recommendations on safeguarding personal information**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| 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.<br>(Recommendation following paragraph 18 of the 2009 audit report) | Satisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

## Security procedures not always followed

79. FINTRAC's security policy defines restricted items as those that may constitute a threat to the security of its assets. FINTRAC provided documentation and confirmed that all electronic devices, such as unauthorized cell phones, are prohibited in FINTRAC's restricted areas and must be left at its reception. FINTRAC also confirmed that contractors must be escorted at all times. We expected to find full compliance with these security requirements.

80. However, during our visit at one of the regional offices we observed that a contractor was unescorted while working and had unrestricted access to a secure area. We also observed the contractor using his cell phone in this work area, which as noted above, is prohibited under FINTRAC's security policy.

81. In preparation for an on-site examination of a reporting entity, Compliance Officers may be required to extract information from FINTRAC's databases. They may also record information from the reporting entity's files during the on-site examination. The officers are provided encrypted laptops for these purposes. FINTRAC has established policies regarding the use of laptops, as well as the management of information obtained from FINTRAC's analytical databases in preparation for the on-site examination. The policy governs the type of information that can be stored on the laptop, and includes guidelines for protecting the laptop while away from the office. According to policy, information from the analytical databases may be removed from FINTRAC premises as long as it does not contain personal information and it is adequately protected.

82. FINTRAC informed us that the use of portable storage devices (flash drives) is prohibited by its policy. This policy is consistent with the guidance issued by the Communications Security Establishment Canada. When personal information is transported on portable storage devices it runs the risk of being accessed inappropriately. During this audit, such a breach did occur. A briefcase containing a Compliance Officer's laptop and unencrypted USB key was stolen from the trunk of a car. This breach affected 777 individuals. Personal information of 295 of these individuals was stored on the unencrypted USB key or recorded within hardcopy documents.

## 83. RECOMMENDATION

FINTRAC should implement measures to ensure that all its staff members possess a sound awareness of FINTRAC's privacy and security policies to safeguard personal information and their obligation to comply with them at all times.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC has individual policies on Privacy, on Security, and on Information Management, comprised in the Centre's Privacy Framework. This framework is available to all employees from FINTRAC's intranet. Furthermore, an updated FINTRAC Code of Conduct, Values and Ethics came into effect in June 2012 and includes specific references to the protection of personal information, the* Privacy Act *and FINTRAC's Privacy, Security, and Information Management policies. Every FINTRAC letter of offer encloses a Terms and Conditions of Employment document that includes a requirement to read and accept, by signing, the FINTRAC Code of Conduct, Values and Ethics. Acceptance of the FINTRAC Code of Conduct, Values and Ethics, along with adherence to its values, expected behaviours and responsibilities, is a condition of employment for all FINTRAC employees. On an annual basis, all FINTRAC employees are reminded of their obligations with regard to the Code. Finally, FINTRAC provided mandatory training on the Centre's security programs to all employees in the winter of 2013.*

*Given these measures are already in place, FINTRAC has addressed this recommendation.*

## PRIVACY MANAGEMENT PROGRAM

84. A privacy management program refers to the structures, policies, procedures and processes in place to ensure a government institution meets its obligations under the *Privacy Act*. Core elements include effective governance, clear accountability, a privacy breach protocol, a process for the identification and management of privacy risks, and awareness training.

85. During the course of our previous audit we looked at how FINTRAC organized itself through structures, policies, systems and procedures to distribute privacy responsibilities, coordinate privacy work, manage privacy risks, and ensure compliance with the *Privacy Act*.

86. We found that FINTRAC had put in place some elements of a privacy management program. However, there were gaps which needed to be addressed in the areas of privacy governance and accountability, risk management and staff training.

87. To address these issues, we recommended that FINTRAC appoint an individual who would be accountable for privacy; identify, report and track all initiatives requiring Privacy Impact Assessments; comply with breach reporting expectations established by the Treasury Board Secretariat; and ensure that all employees handling personal information and/or responsible for privacy receive appropriate training. To assess progress, we reviewed FINTRAC's privacy governance structure, risk management and training programs. We also interviewed officials in headquarters and the regions.

## Accountability for privacy compliance established

88. FINTRAC appointed a Chief Privacy Officer (CPO) in mid-2010. Additionally, FINTRAC created a Privacy Committee, which is chaired by the CPO. The role of the CPO is to provide strategic privacy leadership and oversee privacy-related activities within FINTRAC. The Privacy Committee's objectives include ensuring a coordinated approach to privacy related issues, including implementation of the OPC's audit recommendations and strengthening privacy awareness throughout FINTRAC.

## Process for identifying privacy risk formalized

89. The Treasury Board Secretariat's (TBS) Directive on Privacy Impact Assessment (PIA) came into effect on April 1, 2010 and is designed to ensure that privacy principles are taken into account for all new or substantially redesigned programs and services with privacy implications. FINTRAC has developed a Privacy Impact Checklist, which must be completed during the design phase of any project, and a PIA approval procedure. Together, they assist in evaluating the level of impact a program may have on an individual's privacy and provide guidance on the development of PIAs. With these in place, FINTRAC's PIA process meets the core requirements established by TBS.

## Privacy breach guidelines finalized

90. During our previous audit, we noted that FINTRAC's Security Policy included a section on the procedures to follow in the event of a security breach. However, the procedures did not specifically address what steps to take if the incident also involved the inappropriate collection, use, disclosure or disposal of personal information. FINTRAC has updated its privacy policy to address this gap. It now includes additional information on how to address security breaches that impact individuals' privacy rights.

91. FINTRAC has developed Privacy Breach Incident Guidelines that provide employees with information on what constitutes personal information and a privacy breach incident, what must be done when a privacy breach occurs, roles and responsibilities, and how to prevent privacy breaches. We reviewed the guidelines and found that they comply with the breach reporting recommendations established by TBS.

## Privacy awareness training enhanced

92. In our previous audit we found that privacy and security awareness training is provided to all employees as part of FINTRAC's orientation program. We also noted that FINTRAC addressed privacy-related matters in a number of different ways, such as fact sheets and an on-line video. However, we also noted that the training course content lacked information on the core privacy principles to ensure employees were aware of their obligations under the *Privacy Act*.

93. To assess progress, we reviewed the content of FINTRAC's training and awareness programs and interviewed staff involved in the development and delivery of those programs. We also conducted interviews with regional staff to assess their awareness of their obligations with respect to privacy.

94. We found that FINTRAC's Privacy Policy has been updated and circulated to all employees. FINTRAC's orientation for new employees also includes a section covering privacy protection, indicating that employees must be familiar with the requirements set out in FINTRAC's Privacy Policy and emphasizes the consequences of non-compliance with it. Security and Information Management awareness training, which includes a privacy module, has also been updated and is mandatory for all employees.

95. Staff who we interviewed indicated that privacy and security were covered at the outset of employment with FINTRAC as part of their orientation. However, most indicated that they had received security training but had not received formal training on core privacy principles; were not aware that privacy breach guidelines had been developed; and were not fully aware of what constitutes a privacy breach. Subsequent to our interviews FINTRAC's *Code of Conduct*, *Values and Ethics* was distributed to all employees. This document includes references to the protection of personal information, the *Privacy Act* and FINTRAC's *Privacy Policy*. It was noted that all employees were required to read the code and acknowledge the acceptance of it as a continuing condition of their employment.

96. As a result of FINTRAC's actions to address the four elements of the 2009 recommendation, we assess its progress on this recommendation as satisfactory (See Exhibit G).

**Exhibit G – Progress in addressing the four parts of the 2009 recommendation on FINTRAC's privacy management program**

| 2009 RECOMMENDATIONS | PROGRESS |
|---|---|
| To strengthen its privacy management framework, FINTRAC should:<br>• appoint a senior executive as Chief Privacy Officer to provide strategic privacy leadership, and to coordinate and oversee privacy related activities;<br>• ensure that all initiatives and programs requiring privacy impact analysis are identified, reported and tracked;<br>• finalize and implement privacy incident guidelines to comply with breach reporting expectations established by the Treasury Board Secretariat; and,<br>• 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. | Satisfactory |

(Recommendations following paragraph 96 of the 2009 audit report)

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

## FINTRAC'S COMPLIANCE MANDATE

97. In addition to its analysis and disclosure functions, FINTRAC carries out a compliance program to ensure reporting entities meet their obligations under the PCMLTFA and its regulations.

### Inconsistent data minimization practices remain an issue

98. Limiting the collection of personal information, or data minimization, is a fundamental element of data protection statutes. Restricting the collection of information to that which is strictly necessary to fulfil an identified purpose mitigates privacy risks.

99. During our previous audit, we found instances where there was no demonstrated need for FINTRAC to retain certain types of records to execute its compliance function. 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. We recommended that FINTRAC observe the principle of data minimization.

100. To assess progress, we examined a purposive sample of FINTRAC's compliance examination files, reviewed internal policies and procedures, held interviews with Compliance Officers in the regions and interviewed officials in headquarters.

101. In July 2009, FINTRAC issued a policy whereby all documentation received from reporting entities must be scanned and the original paper format record destroyed. Due to the increased volume of compliance examinations, in June 2011, FINTRAC issued guidance to its compliance staff that only records or documents needed to support deficiencies must be scanned, and all other records/documents could be destroyed.

102. FINTRAC has not updated the relevant policies and procedures to formally reflect the June 2011 guidance described above. We observed inconsistencies within regional offices in how the scanning policy and guidance were being implemented. Original paper documents were: not shredded after being scanned; not shredded after the examination file was closed; and, retained on file for different timeframes after being scanned.

103. FINTRAC officials advised that no criteria or guidelines have been developed to assist Compliance Officers in determining what documents are considered "relevant" to support deficiencies.

104. We also found inconsistent approaches in terms of how personal identifiable information is collected and reproduced in working copies of reports and records. For example, some compliance officers check off in their working reports that a SIN or health card number was used by the entity to identify an individual while other officers recorded the specific numbers and photocopied the actual identification cards. We observed that these and other personal identifiers were recorded or photocopied in instances where they did not support a related deficiency.

105. We reviewed a purposive random sample of compliance examination files and found instances where there was no demonstrated need to retain certain types of records. Examples appear in Exhibit H.

**Exhibit H – Examples of personal information unnecessarily retained on compliance files:**

- Executor information, tax records of deceased individuals, medical records, Proof of Death Statements;
- Photocopies of identification documents, such as driver's licenses, passports, social insurance cards, and third-party personal information that did not relate to deficiencies;
- Credit reports;
- Employee training records;
- Working copies of Canadian Police Information Centre (CPIC) checks taken from the Money Services Businesses registration database with personal information not redacted.

106. Therefore, we assess progress on our recommendation regarding data minimization as unsatisfactory (See Exhibit I).

**Exhibit I – Progress in addressing our 2009 Audit Report recommendations on FINTRAC's compliance mandate—data minimization**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| In keeping with privacy best practices, we encourage FINTRAC to observe the principle of data minimization in the execution of its compliance activities.<br>(Recommendation following paragraph 103 of the 2009 audit report) | Unsatisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

## 107. RECOMMENDATION

In keeping with privacy best practices and to ensure consistent data minimization by compliance officers, FINTRAC should update its policies and procedures to clearly identify what information compliance officers should record and retain on compliance files to support deficiencies.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC has a policy in place with respect to what information compliance officers should record and retain. The policy was communicated to all compliance officers in June 2011. The policy states that "only records/documents that are used to support deficiencies must be scanned. All other records/documents can now be destroyed; however, clear documentation must be included in the examination notes to confirm what types of records were received." Since its introduction, the policy has become common practice and continues to be an integral part of the examination process. On an ongoing basis, it is also communicated to all new compliance officers as part of the regional examination training. In addition, FINTRAC is in the process of further strengthening its policies and procedures in regards to the handling of reporting entity information. The updated policies and procedures will clearly outline that any official hardcopy records that are related to compliance deficiencies/violations must be scanned and that records that are not related to compliance deficiencies/violations will have to be disposed of. The updated procedures will also require that information supporting deficiencies/violations be scanned on-site using portable scanners.*

*FINTRAC commits to finalize the updating of the policy on scanning / retention / disposition of examination documents, which is expected to be completed by the end of 2013.*

## Quality control lacks privacy component

108. FINTRAC implemented a Quality Assurance (QA) program in late 2010 to look at the presence and content of key elements of FINTRAC's compliance examination files. This program focused on the compliance examination function.

109. We expected the QA program to include a review of whether personal information received and collected by Compliance Officers is necessary to substantiate deficiencies noted during compliance examinations. We reviewed QA assessments and other relevant documents, held interviews with participating officers and with officials in Headquarters. As a result of our interviews and file reviews we found that the quality assurance program does not include verifying whether Compliance Officers are acquiring and retaining unnecessary personal information, such as the information presented in Exhibit H.

### 110. RECOMMENDATION

FINTRAC should include a privacy compliance monitoring process in its QA program to determine if information collected and retained while performing compliance examinations is limited to that which is necessary to establish compliance with the Act.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC's compliance examination program already seeks to minimize the amount of information that is collected to adequately assess a reporting entity's compliance. As part of continuous improvement initiatives, FINTRAC is modernising its examination program. Planned improvements will help ensure that any information kept is limited to only that which is necessary to properly document non-compliance found during the course of an examination.*

*FINTRAC commits to finalize the updating of compliance program policies and procedures, which is expected to be completed by the end of 2013.*

## Additional work is required to ensure consent is meaningful

111. Where a reporting entity is located in a 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. The "Consent to enter a dwelling house for compliance examination" form not only seeks the individual's consent (to permit FINTRAC entry), it also requires that the individual provide their name, gender, date of birth and address. For the individual's consent to be meaningful, the purpose(s) for the collection of this personal information must be stated in such a way that the individual can reasonably understand how his or her information will be used or disclosed.

112. In our audit of 2009, we found that the consent form did not indicate whether consent may be refused, or the ramifications of such a refusal. Moreover, the consent form did not indicate the purpose of collecting the date of birth or its contemplated uses, such as to confirm the identity of an individual and to conduct a criminal background check.

113. We recommended that FINTRAC amend the form 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.

114. Although FINTRAC amended the form, the revised version does not indicate the purpose for collecting or what uses will be made of the individual's date of birth collected in the form.

115. Therefore, we assess progress on our recommendation regarding the consent form as unsatisfactory (See Exhibit J).

**Exhibit J – Progress in addressing our 2009 Audit Report recommendations on FINTRAC's compliance mandate—consent form**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| 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.<br>(Recommendation following paragraph 107 of the 2009 audit report) | Unsatisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

## 116. RECOMMENDATION

The "Consent to enter a dwelling house for compliance examination" form should be further amended to indicate the purpose of collecting the date of birth on the form and the uses that will be made of it.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. The purpose of collecting the date of birth on the "Consent to enter a dwelling house for compliance examination" form is to verify the identity of the person that resides in the dwelling house. The form was updated in order to reflect the purpose of collecting such information and has been in use since May 22, 2013.*

## Revised process mitigates the risks associated with the transmission of personal information

117. FINTRAC requests copies of certain documents prior to commencing an on-site or desk compliance examination. At the time of our previous audit, the request instructed reporting entities to forward the records to FINTRAC by mail, e-mail or fax. In 2009 we found that a reporting entity forwarded client records containing names, addresses, SINs, account numbers and account activity to FINTRAC by e-mail.

118. We recommended that FINTRAC amend the 'notice of examination' to include explicit instructions that reporting entities refrain from transmitting records containing personal information. In the event that there was a requirement to do so, we recommended that FINTRAC work with reporting entities to ensure that only secure transmission methods are used.

119. To assess progress we reviewed policies for transmission of information, notification letters and a purposive sample of compliance examination files. We also held interviews with Compliance Officers in the regional offices.

120. We observed that the information request letter was amended. Information is now required to be sent only by mail or courier from reporting entities as opposed to fax or e-mail. Our review of the Examination Handbook for Compliance Officers confirmed that the change was formally implemented.

121. Therefore, we assess progress on our recommendation regarding the secure transmission of personal information as satisfactory (See Exhibit K).

**Exhibit K – Progress in addressing our 2009 Audit Report recommendations on FINTRAC's compliance mandate—transmission of personal information**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| 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.<br>(Recommendation following paragraph 110 of the 2009 audit report) | Satisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

## Guidance provided by some regulatory partners continues to encourage over reporting

122. To assist with its compliance activities, FINTRAC advised that it has entered into information-sharing agreements with 18 national and provincial regulatory agencies. Several of them have issued Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) guidance to members of their regulated sector.

123. During our previous audit we found instances where guidelines issued by some regulatory agencies encouraged client identification, monitoring and reporting activities which clearly exceeded the requirements of the PCMLTFA. The responsibility for ensuring compliance with Part 1 of the PCMLTFA ultimately rests with FINTRAC. Without reviewing all PCMLTFA reporting guidelines issued by partner agencies, FINTRAC cannot be assured that they promote practices that are consistent with the Act.

124. We recommended that FINTRAC analyze all PCMLTFA guidance issued by its federal and provincial regulatory partners to ensure that such guidance does not promote practices that extend beyond the requirements of the Act. To assess progress we reviewed internal documents, operational plans and regulatory guidance, and interviewed FINTRAC officials.

125. FINTRAC informed us that it has not reviewed regulators' guidance. Furthermore, with the exception of two national agencies, FINTRAC does not have in its possession AML/ATF guidance issued by its regulatory partners. Therefore, FINTRAC is still unable to demonstrate that those guidance documents promote practices that are consistent with the Act.

126. Despite FINTRAC's 2009 commitment to continue working with its partners to ensure that any guidance issued by regulatory partners is consistent with PCMLTFA requirements, we found instances where regulatory bodies issued updated AML/ATF guidance documents that instructed members to report activities which exceed the requirements of the PCMLTFA.

127. Therefore, we assess progress on our recommendation regarding FINTRAC's review of guidance provided by regulatory partners as unsatisfactory (See Exhibit L).

**Exhibit L – Progress in addressing our 2009 Audit Report recommendations on FINTRAC's compliance mandate—regulatory partners' guidance**

| 2009 RECOMMENDATION | PROGRESS |
|---|---|
| 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*.<br>(Recommendation following paragraph 114 of the 2009 audit report) | Unsatisfactory |

**Satisfactory**—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

**Unsatisfactory**—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

## 128. RECOMMENDATION

As regulators have issued *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) guidance that instructs entities to report transactions below the legislated threshold, FINTRAC should take action to ensure that guidance issued by regulatory partners is consistent with PCMLTFA requirements.

**FINTRAC's response:**

*FINTRAC accepts the recommendation. FINTRAC already works with regulatory partners to assist sectors in meeting the obligations prescribed by the PCMLTFA. FINTRAC will continue to work with these regulatory partners to help ensure communication is consistent across all sectors, respecting the legal authorities and mandates under which each regulator operates. Through this work, FINTRAC will reiterate to its regulatory partners the information that is to be reported to FINTRAC in accordance with the PCMLTFA.*

*FINTRAC will reiterate to its regulatory partners the information that is to be reported to FINTRAC in accordance with the PCMLTFA, which will be done on an ongoing basis.*

# Conclusion

129. The *Privacy Act* imposes obligations on federal government organizations to manage personal information and respect the privacy rights of Canadians. The *Privacy Act*, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and Treasury Board Secretariat policy place limits on what personal information the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) can receive, collect, use and disclose while it carries out its mandate. Our previous audit made a number of recommendations, the majority of which FINTRAC committed to address.

130. FINTRAC has made limited progress in meeting its 2009 commitments to enhance controls in an effort to ensure that its information holdings are both relevant and limited to that which it needs or uses. Until FINTRAC reconciles the requirements of the *Privacy Act* with the PCMLTFA, it will continue to receive, collect and retain information that it does not need or use in its operating programs and activities.

131. FINTRAC has made satisfactory progress by providing criteria to guide whether the threshold to disclose designated information to certain domestic partners is met. Disclosures of intelligence to financial intelligence units and police forces continue to be tightly controlled and made in accordance with the PCMLTFA.

132. FINTRAC continues to foster a culture regarding matters of security and confidentiality and deploys a variety of measures to protect its information holdings. FINTRAC enhanced its threat and risk assessment and security review documentation process and has taken steps to ensure examined entities transmit information in a secure manner. Notwithstanding, work needs to be done to ensure full compliance with its security policies.

133. FINTRAC has taken action to address its commitments to our recommendations regarding its privacy management program. As well, it committed to continue to reinforce the importance of respecting the data minimization principle when training its compliance officers and when updating its policies. However, some personal information continues to be collected and used without a clear need to do so and policies have not been updated to formally reflect data minimization guidance.

134. While FINTRAC continues to perform outreach activities and to regularly update its published guidelines to reporting entities, FINTRAC does not review guidelines issued by its regulatory partners to ensure that such guidance does not promote record keeping and reporting practices that extend beyond the requirements of the PCMLTFA. Similarly, it is important that FINTRAC ensure that its responses to reporting entities' inquiries do not lead to over-reporting.

135. Overall, we conclude that the Centre has sound controls in place to protect personal information. However, we found that it has made limited progress in addressing five of ten audit recommendations made in 2009. To fully comply with its obligations under the *Privacy Act*, FINTRAC must take steps to limit the receipt, collection and retention of personal information to only that which is directly relevant to the execution of its mandate.

# 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 where appropriate.

Pursuant to section 72.(2) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), the Privacy Commissioner is required to conduct a biennial review of measures taken by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to protect information it receives or collects, and to report the results of such reviews to Parliament.

## OBJECTIVE

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

The audit focused on reviewing the progress toward commitments that FINTRAC had made in response to the recommendations and relevant observations from our 2009 audit.

## CRITERIA

The criteria used to conduct the audit are based on the relevant authorities of the *Privacy Act*, the PCMLTFA and, associated Treasury Board Secretariat (TBS) policies. We expected FINTRAC to:

- 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 *Privacy Act* and the PCMLTFA;
- retain and dispose of personal information in accordance with governing authorities;
- have appropriate security measures in place to ensure that personal information is protected throughout its life cycle; and
- clearly define roles and responsibilities for the protection of personal information and implement measures to ensure compliance with its privacy obligations.

Based on our assessment of the actions taken by FINTRAC in addressing the recommendations from our 2009 audit we assigned one of the following ratings:

- Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made; or
- Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation paragraph was made.

In determining the ratings given for each recommendation, the audit team considered such factors as the following:

- the inherent conditions embedded in the recommendation;
- whether the action(s) taken by FINTRAC related directly and deliberately to the recommendation;
- the complexity of the recommendation;
- the time that has elapsed since the recommendation was made;
- the extent to which existing and planned actions will address the recommendation;
- the balance between activities and results; and
- any significant changes in circumstances that have occurred since the 2009 audit.

## SCOPE AND APPROACH

The audit included a review of FINTRAC's programs and information management processes 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, memoranda of understanding (MOUs), and privacy impact assessments. We also examined reporting processes, a sample of reports, and disclosures to domestic organizations and foreign intelligence units. A purposive sample strategy was used to determine the audit samples, with consideration given to the nature, volume and impact on privacy of the population being sampled. The number of files selected was guided by the assessment of privacy risk and the number of files available. To ensure an unbiased selection of files, a statistical random sample was used to select files where all files were not selected.

At the time of writing this report, the Standing Committee on Banking, Trade and Commerce was working on a draft report regarding the five-year Parliamentary review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Therefore, this audit has not considered the impact of any potential amendments to the PCMLTFA.

We conducted audit activities at FINTRAC headquarters and at regional offices in Montreal, Toronto and Vancouver. The audit work was substantially completed on October 31, 2012.

## STANDARDS

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

## AUDIT TEAM

Director General: Steven Morgan

Garth Cookshaw
Sylvie Gallo Daccash
Anne Overton
Ivan Villafan

# Appendix 1: Persons or entities covered under PCMLTFA

- Accountants
- British Columbia notaries
- Casinos
- Dealers in precious metals and stones
- Financial entities
- Lawyers[1]
- Life insurance
- Money services businesses
- Real estate
- Securities dealers

*Source: FINTRAC Annual Report, 2012, page 20*

[1] The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated regulations provide that lawyers must undertake client identification and due diligence, record-keeping and internal compliance measures when undertaking designated financial transactions. Lawyers are not required to transmit reports to FINTRAC. These provisions are in force but are inoperative as a result of a court ruling and related injunctions. The Government is assessing the most recent court ruling.

# Appendix 2: Designated information

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

## Person involved

- Name (including alias), date of birth, address, telephone number, e-mail address
- Citizenship, passport number, record of landing number or permanent resident card number
- Relevant details of the criminal record and any criminal charges of a person/entity involved or acting on their behalf
- Relationships between persons/entities suspected on reasonable grounds of being involved
- Financial interest of a person in an entity on whose behalf suspected transactions were made or attempted
- Name of person suspected on reasonable grounds of directing the transaction, attempted transaction, importation or exportation
- Name and address of any person on whose behalf the transaction or attempted transaction is conducted or on whose behalf the importation or exportation is carried out

## Entity involved

- Corporation name and number, incorporation date and jurisdiction, address, telephone number, e-mail address
- Name, address, e-mail address and telephone number for each partner, director or officer of an entity suspected of being involved
- Name of any person or entity acting on their behalf
- Address and telephone number of principal place of business
- Relevant details of the criminal record and any criminal charges of an entity involved or any person or entity acting on their behalf
- Relationships between persons/entities suspected on reasonable grounds of being involved
- Financial interest of an entity on whose behalf suspected transactions were made or attempted
- Name of entity suspected on reasonable grounds of directing the transaction, attempted transaction, importation or exportation
- Name and address of any entity on whose behalf the transaction or attempted transaction is conducted or on whose behalf the importation or exportation is carried out

## Account/transaction information

- Transit and account number, type of transaction or attempted transaction, date and time of transaction or attempted transaction
- Value of transaction, attempted transaction or of funds that are the subject of the transaction or attempted transaction
- Name, address and telephone number of the place of business where the transaction or attempted transaction occurred
- Type of account and transaction number
- Full name of every account holder and names of parties involved in the transaction
- Name and address of all persons authorized to act in respect of the account

## Reports

- Number and types of reports on which a disclosure is based
- Number and categories of persons or entities that made these reports

## Importation or exportation

- Address of the customs office where the importation or exportation occurred
- Date the importation or exportation occurred
- Amount and type of currency or monetary instruments involved

## Other information

- Relevant grounds on which a person or entity made a suspicious transaction or attempted suspicion transaction report
- Indicators of a money laundering or terrorist activity financing offence related to the transactions, attempted transactions, importation or exportation

*Source: FINTRAC Annual Report, 2012, pages 8 and 9*

# Appendix 3: List of Recommendations and FINTRAC's response

| Compliance with the Code of Fair Information Practices | |
|---|---|
| **RECOMMENDATION** | **FINTRAC'S RESPONSE** |
| To reconcile its obligations under the PCMLTFA with those under the *Privacy Act*, FINTRAC should analyse and assess incoming reports to ensure that it receives and retains only information that it has the legislative authority to receive and which it needs or uses in an ongoing program or activity. | FINTRAC accepts the recommendation.<br><br>FINTRAC meets its obligations under the PCMLTFA and the *Privacy Act* while fulfilling its mandate to assist in the detection, prevention and deterrence of money laundering and terrorist financing. Paragraph 54(a) of the PCMLTFA provides the obligation and requirement for FINTRAC to receive incoming reports, and paragraphs 54(d) and 54(e) require FINTRAC to keep the information contained in those reports for a minimum of 10 years. FINTRAC acknowledges that within the required reports, reporting entities do, in some instances, send personal information that should not be included. FINTRAC has a defined analytical process to ensure that this personal information is not used for the purpose of analysis and is thus not disclosed to police, law enforcement or security partners, as recognized by the OPC at paragraph 53 of this report.<br><br>With respect to reports that do not meet the legislated threshold for reporting, a process is in place to destroy them according to FINTRAC's disposition schedules. FINTRAC will review its disposition schedules in the near term to ensure that this information is assessed and destroyed in the most practical timeframe possible.<br><br>FINTRAC will review its disposition schedules, which is expected to be completed in the fall of 2014. |

| RECOMMENDATION | FINTRAC'S RESPONSE |
|---|---|
| FINTRAC should assess the effectiveness of its outreach programs and strengthen them where necessary to mitigate the risk of receiving personal information beyond the parameters and thresholds specified by the PCMLTFA. | FINTRAC accepts the recommendation.<br><br>FINTRAC assesses the effectiveness of its outreach program and continually strengthens it through additional and/or revised components that detail reporting entities' obligations under the PCMLTFA. This comprehensive outreach program also informs reporting entities of information that they are not required to report to FINTRAC. Ways in which FINTRAC provides this outreach, in addition to the items outlined include:<br><br>• Having a Major Reporters Unit responsible for managing FINTRAC's relationship with the largest of the reporting entities in the banking sector;<br><br>• Holding sector-specific consultations, such as with the Credit Union sector on guidance related to the implementation of a risk based approach and the upcoming regulations for customer due diligence, and with the Money Services Businesses, which prompted MSB specific guidance being published;<br><br>• Making sector-specific information on reporting entities' obligations, formal guidelines, and FINTRAC Interpretation Notices available on FINTRAC's website; and<br><br>• Participating in meetings with industry associations, regulators, and law enforcement partners, including the bi-annual Public/Private Sector Advisory Committee.<br><br>While FINTRAC provides outreach on personal information that reporting entities are required to send, the obligation remains with the individual reporting entities to not send information not required by the legislation and regulations. FINTRAC agrees that this issue should be addressed and it therefore will continue to support the OPC in their efforts to ensure that those reporting entities which are subject to the *Personal Information Protection and Electronic Documents Act* meet the requirements set out in that Act.<br><br>Given the above, FINTRAC has addressed this recommendation and will continue to do so in the future. |

| RECOMMENDATION | FINTRAC'S RESPONSE |
|---|---|
| FINTRAC should identify and dispose of information that it should not have received and is not directly related to its operating programs and activities. | FINTRAC accepts the recommendation.<br><br>FINTRAC has a process in place for addressing information that reporting entities should not have sent to FINTRAC. Paragraph 54(a) of the PCMLTFA requires FINTRAC to receive reports sent by reporting entities. Paragraphs 54(d) and 54(e) also set authorities with respect to retention and disposition of the information contained in incoming reports. While FINTRAC is required to receive and retain this information, it also has a defined analytical process that ensures that personal information that should not have been included in reports by reporting entities is not used for the purpose of analysis.<br><br>With respect to reports that do not meet the legislated threshold for reporting, a process is in place to destroy them according to FINTRAC's disposition schedules. FINTRAC will review its disposition schedules in the near term to ensure that this information is assessed and destroyed in the most practical timeframe possible.<br><br>FINTRAC will review its disposition schedules, which is expected to be completed in the fall of 2014. |
| FINTRAC should: a) finalize an agreement with LAC regarding terms and conditions for the transfer of its archival records, and b) implement a formal retention and disposal policy for information and records whose retention and disposal periods are not specifically covered by the PCMLTFA. | FINTRAC accepts the recommendation.<br><br>With respect to a), FINTRAC will work with LAC to finalize an agreement. However, it should be noted that FINTRAC and LAC jointly came to agreement on Terms and Conditions (T&Cs) required for FINTRAC to obtain its Records Disposition Authority (RDA) in the spring of 2012. The T&Cs were signed by FINTRAC and forwarded to LAC for their signature and approval. Since then, LAC's processes in regards to the issuance of RDAs have changed, and therefore, additional revision is underway to ensure that the finalized Disposition Authorization reflects the new process.<br><br>With respect to b), FINTRAC is actively working with internal stakeholders and LAC in defining the record disposition schedules that will be in compliance with the Treasury Board Recordkeeping directive. FINTRAC would like to clarify that all reports in its database remain within the 15-year timeframe prescribed by the PCMLTFA at which point it is required to destroy the identifying information contained in financial transaction reports that have not been disclosed.<br><br>FINTRAC commits to working with LAC to finalize an agreement and to define record disposition schedules and draft the necessary policies. Timeframe for completion of this commitment is dependent on LAC. |

| Safeguarding of Canadians' Personal Information | |
|---|---|
| **RECOMMENDATION** | **FINTRAC'S RESPONSE** |
| FINTRAC should implement measures to ensure that all its staff members possess a sound awareness of FINTRAC's privacy and security policies to safeguard personal information and their obligation to comply with them at all times. | FINTRAC accepts the recommendation.<br><br>FINTRAC has individual policies on Privacy, on Security, and on Information Management, comprised in the Centre's Privacy Framework. This framework is available to all employees from FINTRAC's intranet. Furthermore, an updated FINTRAC Code of Conduct, Values and Ethics came into effect in June 2012 and includes specific references to the protection of personal information, the *Privacy Act* and FINTRAC's Privacy, Security, and Information Management policies. Every FINTRAC letter of offer encloses a Terms and Conditions of Employment document that includes a requirement to read and accept, by signing, the FINTRAC Code of Conduct, Values and Ethics. Acceptance of the FINTRAC Code of Conduct, Values and Ethics, along with adherence to its values, expected behaviours and responsibilities, is a condition of employment for all FINTRAC employees. On an annual basis, all FINTRAC employees are reminded of their obligations with regard to the Code. Finally, FINTRAC provided mandatory training on the Centre's security programs to all employees in the winter of 2013.<br><br>Given these measures are already in place, FINTRAC has addressed this recommendation. |

| FINTRAC's Compliance Mandate | |
|---|---|
| **RECOMMENDATION** | **FINTRAC'S RESPONSE** |
| In keeping with privacy best practices and to ensure consistent data minimization by compliance officers, FINTRAC should update its policies and procedures to clearly identify what information compliance officers should record and retain on compliance files to support deficiencies. | FINTRAC accepts the recommendation.<br><br>FINTRAC has a policy in place with respect to what information compliance officers should record and retain. The policy was communicated to all compliance officers in June 2011. The policy states that "only records/documents that are used to support deficiencies must be scanned. All other records/documents can now be destroyed; however, clear documentation must be included in the examination notes to confirm what types of records were received." Since its introduction, the policy has become common practice and continues to be an integral part of the examination process. On an ongoing basis, it is also communicated to all new compliance officers as part of the regional examination training. In addition, FINTRAC is in the process of further strengthening its policies and procedures in regards to the handling of reporting entity information. The updated policies and procedures will clearly outline that any official hardcopy records that are related to compliance deficiencies/violations must be scanned and that records that are not related to compliance deficiencies/violations will have to be disposed of. The updated procedures will also require that information supporting deficiencies/violations be scanned on-site using portable scanners.<br><br>FINTRAC commits to finalize the updating of the policy on scanning / retention / disposition of examination documents, which is expected to be completed by the end of 2013. |
| FINTRAC should include a privacy compliance monitoring process in its QA program to determine if information collected and retained while performing compliance examinations is limited to that which is necessary to establish compliance with the Act. | FINTRAC accepts the recommendation.<br><br>FINTRAC's compliance examination program already seeks to minimize the amount of information that is collected to adequately assess a reporting entity's compliance. As part of continuous improvement initiatives, FINTRAC is modernising its examination program. Planned improvements will help ensure that any information kept is limited to only that which is necessary to properly document non-compliance found during the course of an examination.<br><br>FINTRAC commits to finalize the updating of compliance program policies and procedures, which is expected to be completed by the end of 2013. |

| RECOMMENDATION | FINTRAC'S RESPONSE |
|---|---|
| The "Consent to enter a dwelling house for compliance examination" form should be further amended to indicate the purpose of collecting the date of birth on the form and the uses that will be made of it. | FINTRAC accepts the recommendation.<br><br>The purpose of collecting the date of birth on the "Consent to enter a dwelling house for compliance examination" form is to verify the identity of the person that resides in the dwelling house. The form was updated in order to reflect the purpose of collecting such information and has been in use since May 22, 2013. |
| As regulators have issued *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) guidance that instructs entities to report transaction below the legislated threshold, FINTRAC should take action to ensure that guidance issued by regulatory partners is consistent with PCMLTFA requirements. | FINTRAC accepts the recommendation.<br><br>FINTRAC already works with regulatory partners to assist sectors in meeting the obligations prescribed by the PCMLTFA. FINTRAC will continue to work with these regulatory partners to help ensure communication is consistent across all sectors, respecting the legal authorities and mandates under which each regulator operates. Through this work, FINTRAC will reiterate to its regulatory partners the information that is to be reported to FINTRAC in accordance with the PCMLTFA.<br><br>FINTRAC will reiterate to its regulatory partners the information that is to be reported to FINTRAC in accordance with the PCMLTFA, which will be done on an ongoing basis. |