Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Financial Transactions and Reports Analysis Centre of Canada

Table of Contents

Section 37 of the *Privacy Act*
Section 72(2) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

Final Report 2017

Main Points

What we examined

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) created the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC or the Centre), and requires it to ensure that personal information under its control is protected from unauthorized disclosure. Sections 4 to 8 of the *Privacy Act* govern how federal institutions, including FINTRAC (Financial Transactions and Reports Analysis Centre of Canada), can collect, use and retain personal information. The Office of the Privacy Commissioner of Canada (OPC) examined whether the policies, practices and processes FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has in place for managing the personal information it receives, collects, and retains comply with the Centre's obligations under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) and the *Privacy Act*. Our review included an analysis of the amount and type of personal information FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) collects directly from reporting entities when it monitors compliance with the reporting obligations imposed by the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).

We interviewed selected FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and Shared Services Canada (SSC) officials, reviewed pertinent documents, and analyzed a sample of transaction reports received by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) between April 2014 and July 2016. We also looked at a sample of compliance examination files compiled by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) between the period of April 2014 and March 2016. All examination activities were conducted in the National Capital Region.

Our review included an assessment of whether there are adequate technical safeguards in place to protect the personal information received, collected and retained by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) from inappropriate or unauthorized use and disclosure. Given that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s electronic data holdings reside on technical infrastructure now operated by SSC (Shared Services Canada), we assessed the measures FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken to ensure that SSC (Shared Services Canada) has satisfactory information technology (IT) safeguards in place.

We also assessed the progress made by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to address the observations and recommendations made in our 2013 audit report. We specifically examined how FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has addressed our observation that it received and retained personal information that did not meet legislated reporting thresholds set out in the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act). This observation had also been made in our 2009 report. Both previous audit reports recommended that in order to mitigate that risk, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should screen incoming reports before they enter the database so that such information is identified and destroyed at the earliest stage possible.

We did not review FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s disclosure of personal information to regime partners, such as police services, the Canadian Security Intelligence Service (CSIS), the Canada Border Services Agency (CBSA) the Canada Revenue Agency (CRA), and provincial and territorial securities commissions. The Centre's handling of personal information about its employees and the personal information handling practices of entities reporting to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) were also out of scope.

Why it is important

According to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s 2015-2016 Annual Report, financial transaction reporting has increased by 63 percent over the past five years, with the Centre receiving nearly 24 million reports in the past fiscal year alone. As of March 31, 2016, there were approximately 212 million reports containing personal information in FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s databases.

Reports are submitted by reporting entities without the knowledge or consent of the individuals concerned [1](#fn1), and are retained in FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) databases for a minimum of 10 years. These records contain sensitive financial and other personal information, and a breach could potentially have serious implications for the individuals involved. The receipt of reports that do not meet legal thresholds and the lengthy retention period for these reports increases the risk of unwarranted scrutiny of law abiding individuals by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). Additionally, the personal information in FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s data holdings (other than Cross Border Currency Reports) is not accessible under *Privacy Act* requests, and individuals have no ability to check records or ask for corrections. [2](#fn2)

These factors heighten the need for FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to be diligent in ensuring it retains only the information it is legislatively entitled to possess, that the information it retains is as accurate as possible, and that such information is protected against inappropriate use and/or disclosure with safeguards commensurate to its sensitivity.

What we found

We concluded during this audit that the Centre has made significant efforts to enhance its personal information handling practices, resulting in improvements to privacy protections. However, we found issues related to the monitoring of internal user activity and the assignment of IT (Information Technology) security roles and responsibilities that are now shared between SSC (Shared Services Canada) and FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). We also found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) continues to receive and retain personal information that does not meet legal reporting thresholds.

In addition, we found indications that the vast majority of the reports received by the Centre may never be used. As of March 31, 2016, 37 million reports received by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had reached the end of their 10-year retention periods and had been disposed of without having been used in a disclosure. This is almost the entire quantity of reports received by the Centre from its inception to March 31, 2006.

Our main findings are summarized below.

- There is no formal assurance that the personal information acquired, retained and transmitted by the Centre is appropriately protected on the Shared Services Canada IT (Information Technology) infrastructure. As of 2012, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s electronic data holdings have been housed on the SSC (Shared Services Canada) IT (Information Technology) infrastructure, as mandated by the *Shared Services Canada Act*. [3](#fn3) In recent years FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has experienced some difficulties in obtaining assurances from SSC (Shared Services Canada) that certain required technical safeguards are in place. In addition, Electronic Funds Transfers data, which is received from reporting entities by both FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and CRA (Canada Revenue Agency), is transmitted to CRA (Canada Revenue Agency) using a mandated Government of Canada technical system for which SSC (Shared Services Canada) has not renewed the authority to operate [4](#fn4). As a result, the sensitive personal information that is being transmitted to CRA (Canada Revenue Agency) via the SSC (Shared Services Canada) solution is no longer assured to be adequately protected from unauthorized use and/or disclosure.

- FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) continues to receive and retain personal information outside of the legislated thresholds for reporting. This presents risks to privacy by making personal information that should never have been provided to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) available for FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s use and potential disclosure to other institutions. It is unlikely this issue will be resolved unless and until FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) augments its current controls with more robust front-end screening to help ensure the reports it retains in its database meet reporting thresholds and do not contain unnecessary and/or excessive personal information.
- FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) also collects and retains unnecessary amounts and types of personal information from entities while evaluating their compliance with Part 1 or 1.1 of the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).

Introduction

1. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC, or the Centre) is responsible for facilitating the detection, prevention, and deterrence of money laundering, terrorist activity financing and other threats to the security of Canada. It is an independent agency reporting to the Minister of Finance who is accountable to Parliament for the activities of the Centre. It was established by and operates under the legislative authority of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA, or the Act) and its regulations. [5](#fn5)
2. Under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), specified businesses are required to collect information about their clients and transactions. They report some or all of this information to the Centre under prescribed circumstances. The number and type of entities which are required to report to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) [6](#fn6) are extensive and include:
    - Accountants;
    - Notaries (in British Columbia);
    - Casinos;
    - Dealers in precious metals and stones;
    - Financial entities (banks, credit unions, caisses populaires, financial services cooperatives, trust and loan companies);
    - Life insurance brokers and agents;
    - Real estate brokers and agents;
    - Money services businesses (foreign currency exchange, money transfers); and
    - Securities dealers.
3. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) receives the following types of reports. All reports contain personal information.
    - Suspicious Transaction Report (STR): An STR (Suspicious Transaction Report) must be submitted in relation to an attempted or completed financial transaction for which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence. There is no monetary threshold for the reporting of a suspicious transaction.
    - Large Cash Transaction Report (LCTR): A large cash transaction report is submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) when a reporting entity receives $10,000 or more in cash in the course of a single transaction, or when it receives two or more cash amounts totaling $10,000 or more made within 24 hours by or on behalf of the same individual or entity.
    - Electronic Funds Transfer Report (EFTR): An electronic funds transfer report is submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) upon a transmission of instructions for the transfer of $10,000 or more out of or into Canada in a single transaction or in two or more transactions totaling $10,000 or more made within 24 hours by or on behalf of the same individual or entity, through any electronic, magnetic or optical device, telephone instrument or computer.

- Casino Disbursement Report (CDR): Casinos must report to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) when a disbursement of $10,000 or more is made in the course of a single transaction, or when two or more disbursements totaling $10,000 or more are made within 24 hours on behalf of the same individual or entity.
- Terrorist Property Report (TPR): Reporting entities must submit a terrorist property report for property that they know is owned or controlled by or on behalf of a terrorist or terrorist group, or that they have reason to believe is owned or controlled by or on behalf of a person listed under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. [7](#fn7) Real estate, cash, bank accounts, insurance policies, money orders, securities, precious metals and stones and other types of assets are considered property.
- Cross Border Currency Report (CBCR): A cross-border currency report is filed with the CBSA (Canada Border Services Agency) by a person entering or leaving Canada carrying a sum of currency or monetary instruments of $10,000 or more, or by a person mailing or sending such sums into or out of Canada. The CBSA (Canada Border Services Agency) then submits the report to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). A cross-border seizure report is also submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) by CBSA (Canada Border Services Agency) when unreported cash or monetary instruments are seized or upon the seizure of suspected proceeds of crime.
- Voluntary Information Record (VIR): Individuals may voluntarily report their suspicions about money laundering or terrorist financing activities to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). Law enforcement, government institutions and intelligence partners may also provide information to the Centre through the submission of a VIR (Voluntary Information Record).

4. A variety of large but potentially legitimate purchases may be reported to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) as a matter of course. LCTR (Large Cash Transaction Report)s, EFTR (Electronic Funds Transfer Report)s and STR (Suspicious Transaction Report)s submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) by reporting entities subject to the Act could include transactions such as down payments and mortgage arrangements for home purchases, car, boat and recreational vehicle purchases, funds sent to family members abroad and money received by international students studying in Canada.
5. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) analyzes and assesses information it receives and matches the information with other law enforcement and intelligence data, as well as publicly available information. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) analysts may conclude that the information to be disclosed provides “reasonable grounds to suspect” that it would be “relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence”.
6. When this is the case, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) must disclose defined information to the appropriate police force at the federal, provincial or municipal levels, to be used in the investigation of money laundering and/or terrorist activity financing. When FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has reasonable grounds to suspect the information to be disclosed is relevant to threats to the security of Canada, it must disclose the information to CSIS (Canadian Security Intelligence Service). If, in addition, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) also meets other specific legal thresholds set out under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), the Centre must disclose the designated information to additional disclosure recipients including, the CRA (Canada Revenue Agency), CBSA (Canada Border Services Agency), the Communications Security Establishment, and any agency or body that administers the securities legislation of a province. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) may also disclose information to international foreign intelligence units where there are reasonable grounds to suspect that the information to be disclosed would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, or an offence that is substantially similar to either offence.
7. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) also collects information directly from entities while evaluating their compliance with Part 1 or 1.1 of the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), as it is required to do under the Act.

What we found in previous audits

8. The PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) requires the Privacy Commissioner of Canada to undertake a biennial review of the measures taken by the Centre to protect the information it receives or collects and to report on those measures to Parliament. [8](#fn8) This is the third such review undertaken by the Commissioner; the previous reviews were completed in 2009 and 2013. Both of these reviews found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) received and retained reports that did not comply with reporting thresholds established under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act). A table outlining recommendations made in 2013 and our assessment on the progress made to address them can be found at Annex A (#toc5) to this document.

Events since our last audit

9. The Standing Senate Committee on Banking, Trade and Commerce undertook a statutory review of the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) in 2013. [9](#fn9) The Committee report made recommendations related to the evaluation of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s effectiveness and value in the prosecution of terrorist and money laundering offences, the need for expanded information sharing, and discussed the need for an appropriate balance between information sharing and the protection of personal information.
10. In 2014, the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) was amended by Bill C-31 [10](#fn10) to, among other things, provide more flexibility to reporting institutions when verifying client identity, enhance record keeping and registration requirements for financial institutions and intermediaries, include an express reference to online casinos in the Act, and extend the application of the Act to persons and entities that deal in virtual currencies and foreign money services businesses, though these provisions are not yet in force. Bill C-31 also enabled FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to disclose information relating to compliance with Part 1 of the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) to the CRA (Canada Revenue Agency).
11. Of particular note for this audit, Bill C-31 also added subsection 54(2) to the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act). [11](#fn11) This provision requires the Centre to destroy information it receives from reporting entities that it determines, in the normal course of its activities, is not required to be reported to the Centre. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) must similarly destroy any information voluntarily provided by the public that it determines, in the normal course of its activities, is not about suspicions of money laundering or the financing of terrorist activities. The information must be destroyed "within a reasonable time after the determination is made"; the statute does not define what is reasonable in these circumstances.
12. In 2015, Bill C-59 [12](#fn12) amended subsection 55(3) of the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) to require FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to disclose certain information to provincial and territorial securities regulators if it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, as well as offences set out in securities legislation administered by the agency to which the disclosure is made.
13. The 2015 *Security of Canada Information Sharing Act* (SCISA) [13](#fn13) encourages and facilitates broader sharing of personal information among federal government departments for the purposes of protecting Canada against activities "undermining the security of Canada." According to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada), the SCISA (Security of Canada Information Sharing Act) has not had a significant impact on its activities as FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) can only receive and disclose information under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).
14. In June 2015, the House of Commons Standing Committee on Finance released its report on terrorist financing in Canada and abroad. [14](#fn14) The Committee made a number of recommendations focused on increasing the effectiveness of global efforts to combat terrorist financing and of Canada's Anti-Money Laundering/Anti-Terrorist

Financing (AML/ATF) regime. Among other recommendations, it advised FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to urge financial institutions in Canada to improve the training provided to their compliance officers, in order ensure the correct identification of suspicious transactions.

15. The Financial Action Task Force's (FATF) most recent assessment report of Canada's ALM (Anti-Money Laundering)/ATF (Anti-Terrorist Financing) regime was issued in September 2016. The FATF (Financial Action Task Force) is an inter-governmental body with representation from jurisdictions around the world, including Canada. Its objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. [15](#fn15) The report [16](#fn16) analysed Canada's compliance with international obligations, and the level of effectiveness of Canada's ALM (Anti-Money Laundering)/ATF (Anti-Terrorist Financing) system. There were no recommendations related to privacy issues or the use of personal information.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) data holdings on Shared Services Canada IT (Information Technology) infrastructure

16. Shared Services Canada (SSC) was created in 2011 to centrally manage information technology infrastructure for 42 other Government of Canada institutions, including FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). Ownership of the infrastructure supporting FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) core systems and electronic data holdings was transferred to SSC (Shared Services Canada) in 2012. The two institutions have a shared responsibility relating to the protection of systems and personal information received, collected and electronically managed in the context of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s mandated activities. SSC (Shared Services Canada) is responsible under the *Shared Services Canada Act* for providing IT (Information Technology) infrastructure. [17](#fn17) FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) is responsible for ensuring the personal information which it collects is managed and protected in compliance with both the *Privacy Act* and the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).

Focus of this audit

17. The audit focused on whether FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken adequate measures to ensure there are appropriate safeguards in place to protect the personal information in FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s electronic data holdings, which reside on the IT (Information Technology) infrastructure for which SSC (Shared Services Canada) is now the service provider. This transition, which took place in 2012, was not examined during our 2013 audit.
18. The audit also evaluated the collection of personal information from reporting entities by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) during its compliance assessment activities, and reviewed the progress made by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) in response to the observations and recommendations in our 2013 audit.
19. We did not audit disclosures from FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to regime partners, the Centre's handling of personal information about its employees, or the personal information handling practices of the entities reporting to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada).
20. Audit evidence was obtained through the examination of records, interviews, and audit tests. We reviewed a sample of Suspicious Transaction Reports (STRs), Voluntary Information Records (VIRs), and examined all Terrorist Property Reports (TPRs) in the FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) database. We also looked at how reports with certain financial reporting thresholds are managed, and made inquiries to SSC (Shared Services Canada) with regards to the protection of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) information.

21. More information about the audit objective, criteria, scope and approach is found at Annex B (#toc6) to this document.

Observations and Recommendations

22. Sections 4 through 8 of the *Privacy Act* limit the collection of personal information by federal government institutions and govern how that information can be used and disclosed. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) requires FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to ensure that appropriate safeguards are in place to protect the personal information it collects and retains.
23. We looked at how FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) manages the personal information that it obtains, through reports and records submitted to it by financial institutions and other reporting entities, or through direct collection by the Centre during compliance assessment activities. We also looked at the measures FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) takes to ensure that the personal information it acquires is protected with appropriate and sufficient safeguards while it is housed on the SSC (Shared Services Canada) IT (Information Technology) infrastructure and when being transmitted to the CRA (Canada Revenue Agency).
24. We expected to find that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) receives and retains only that personal information which is directly related to its operating programs and activities and for which it has legislative authority; that the safeguards in place to protect such information comply with the relevant Government of Canada IT (Information Technology) security policies, directives and standards and are sufficient to mitigate the risk of breaches and inappropriate disclosures; and that personal information is disposed of at the end of its scheduled retention period.

- **There is no formal assurance that the personal information collected, retained and transmitted by the Centre is appropriately protected on the Shared Services Canada IT (Information Technology) infrastructure.**

25. The Treasury Board of Canada Secretariat's (TBS) *Policy on Government Security* (the Policy) [18](#fn18) prescribes safeguards to protect and preserve the confidentiality and integrity of government assets, including personal information, and establishes minimum mandatory security requirements. Federal institutions must conduct their own assessments to determine whether safeguards above baseline levels are necessary. The Policy also calls for continuous monitoring of the threat environment to ensure appropriate security measures are maintained.
26. The Policy is given effect by standards and directives which must be followed by government institutions. The TBS (Treasury Board Secretariat) *Operational Security Standard: Management of Information Technology Security* (MITS) [19](#fn19) requires IT (Information Technology) systems to be certified and accredited through a Security Assessment & Authorization (SA&A) process before they begin operating. An SA&A (Security Assessment and Authorization) is used to assess and mitigate risks to an acceptable level. The process could include conducting Threat and Risk Assessments to determine security requirements, Statements of Sensitivity to assess the sensitivity of information or assets and Privacy Impact Assessments to assess and mitigate potential privacy risks.
27. Ownership of the infrastructure supporting FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) core systems was transferred to SSC (Shared Services Canada) in 2012. We noted that no SA&A (Security Assessment and Authorization) had been completed by SSC (Shared Services Canada) for this legacy infrastructure. SSC (Shared Services Canada) will initiate a SA&A (Security Assessment and Authorization) process for legacy systems only when significant changes are required or upon receipt of a formal request from the partner institution; however, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has not made such a request. We found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had itself updated previous security assessments for its systems in consultation with SSC (Shared

Services Canada) personnel specifically assigned to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) premises but without engaging SSC (Shared Services Canada) management. While SSC (Shared Services Canada) advised our office that they have security practices in place to help mitigate the risk of unauthorized access to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) data, such as the conduct of vulnerability scanning, these practices are not meant to replace the SA&A (Security Assessment and Authorization) process. There is therefore no formal assurance that all privacy and security risks to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) information holdings on the SSC (Shared Services Canada) infrastructure have been appropriately identified and mitigated.

28. Reporting entities are required to submit reports about Electronic Funds Transfers (EFTRs) of $10,000 or more to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and to the Canada Revenue Agency (CRA). Operationally, reports are transmitted to CRA (Canada Revenue Agency) through the Managed Secure File Transfer (MSFT), which is a centralized SSC (Shared Services Canada) service. We noted that the accreditation letter, which is required for the system to operate, expired in February 2015. SSC (Shared Services Canada) confirmed that the accreditation for this government-wide system has expired. Therefore, the MSFT (Managed Secure File Transfer) system used to transmit EFTR (Electronic Funds Transfer Report)s to CRA (Canada Revenue Agency) does not currently have authority to operate.

Recommendation

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should submit a formal request to SSC (Shared Services Canada) to initiate the Security Assessment and Authorization process to ensure that the SSC (Shared Services Canada) IT (Information Technology) infrastructure on which FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s data resides or flows is certified and accredited, in keeping with the TBS (Treasury Board Secretariat) *Operational Security Standard: Management of Information Technology Security* (MITS).

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken a number of measures to ensure the information that it receives is appropriately protected in the context of Shared Services Canada's mandated infrastructure service delivery. For example, the Director of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has articulated, in writing, his expectations and concerns in relation to IT (Information Technology) security to the President of SSC (Shared Services Canada); a Memorandum of Understanding has been established to ensure that all SSC (Shared Services Canada) personnel assigned to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) are appropriately screened; and the Centre has formally assessed and accredited its legacy infrastructure, which has not changed significantly since infrastructure operations were transferred to SSC (Shared Services Canada).

Although SSC (Shared Services Canada) is accountable for the infrastructure and must ensure that such infrastructure aligns with the requirements of the TBS (Treasury Board Secretariat) Operational Security Standard: Management of Information Technology Security (MITS), FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will formally request SSC (Shared Services Canada) to initiate the Security Assessment and Authorization process to update certification and accreditation of the IT (Information Technology) infrastructure on which FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s data resides or flows.

- **The roles and responsibilities between FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) for privacy and security are not clearly defined**

29. Subsection 29.2(2) of the *Financial Administration Act* [20](#fn20) requires written agreements to govern the provision of internal support services by one department to another. Such agreements should include specific clauses for the protection of personal information in order to ensure compliance with the *Privacy Act* and relevant TBS (Treasury Board Secretariat) policies, directives, and standards. The TBS (Treasury Board Secretariat) *Guideline on Service Agreements: Essential Elements* [21](#fn21) provides guidance regarding the content of and governance structure for service agreements, including those between two federal government departments. Privacy and security are recommended as essential elements of such agreements.
30. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s *Privacy Policy* states that personal information must be protected from improper access, loss, use, disclosure or destruction through the inclusion of specific confidentiality provisions in contracts or other arrangements with third parties.
31. We reviewed the business arrangement between FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) which describes, in general terms, their ongoing business relationship. However, this document does not specify the roles and responsibilities of each department for the protection of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) data. It does not include privacy or security clauses outlining requirements for privacy and security risk assessments, management of access rights and monitoring, control and custody of personal information, or guidance on how to deal with privacy breaches. While FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) have entered into a number of other agreements covering specific services, these agreements are not comprehensive and do not adequately address security and privacy for FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s data holdings.
32. The business arrangement between FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) outlines an option for entering into an Operating Protocol to ensure that particular or specialized business needs or circumstances are accommodated, enabling the parties to deliver their respective programs and services in full compliance with legal requirements, policy obligations and management controls. Such a Protocol would provide an opportunity for clearly defining the roles and responsibilities of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) in relation to privacy and data security. However, an Operating Protocol has not been entered into by the parties.
33. SSC (Shared Services Canada), in consultation with partner departments including FINTRAC (Financial Transactions and Reports Analysis Centre of Canada), has developed a table that outlines responsibilities and accountabilities between itself and its partners regarding the security of their information holdings. The table covers areas such as the development of security standards and departmental IT (Information Technology) security risk management processes. While the table provides guidance on roles and responsibilities for securing partners' information holdings, it is not binding and it is not intended to include relevant clauses that are normally included in an agreement, which is required by subsection 29.2(2) of the *Financial Administration Act*.
34. The FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) *Privacy Breach Incident Guidelines* describe a general process to follow in case of a breach of personal information, but are silent regarding the roles and responsibilities of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) if a breach of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) data occurs on SSC (Shared Services Canada)'s infrastructure. Section 6 of the SSC (Shared Services Canada) *Directive on Privacy Breaches* indicates that roles and responsibilities will be shared when breaches involve SSC (Shared Services Canada)'s IT (Information Technology) infrastructure and a partner institution's data, but does not elaborate on how this sharing of responsibility will be carried out.

Recommendation

In accordance with the *Financial Administration Act* and the TBS (Treasury Board Secretariat) *Guideline on Service Agreements: Essential Elements*, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should work with SSC (Shared Services Canada) to put in place an agreement which clearly defines IT (Information Technology) security roles and responsibilities and relevant privacy and security clauses for the protection of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) information holdings.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken a number of measures to ensure the information that it receives is appropriately protected in the context of Shared Services Canada's mandated infrastructure service delivery. For example, the Director of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has articulated, in writing, his expectations and concerns in relation to IT (Information Technology) security to the President of SSC (Shared Services Canada); a Memorandum of Understanding has been established to ensure that all SSC (Shared Services Canada) personnel assigned to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) are appropriately screened; and the Centre has formally assessed and accredited its legacy infrastructure, which has not changed significantly since infrastructure operations were transferred to SSC (Shared Services Canada). When issues are encountered, solutions are brought forward through the SSC (Shared Services Canada) Service Delivery Manager and other formal channels.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will engage Shared Services Canada to establish an agreement which clearly defines IT (Information Technology) security roles and responsibilities and relevant privacy and security clauses for the protection of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) information holdings.

- **FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) does not regularly monitor activity logs for IT (Information Technology) systems to identify inappropriate access, use, or disclosure of personal information.**

35. Section 6.2.21 of the TBS (Treasury Board Secretariat) *Directive on Privacy Practices* [22](#fn22) requires departments to adopt appropriate measures to ensure that the access, use and disclosure of personal information are monitored and documented, so that inappropriate or unauthorized activity in this regard can be identified and rectified in a timely fashion.
36. Similarly, section 17 of the MITS (Management of Information Technology Security) requires departments to continuously monitor system performance in order to quickly detect attempted or actual unauthorized access to a system, or attempted or actual bypassing of security mechanisms. At a minimum, departments must include a security audit log function in all IT (Information Technology) systems. Departments must incorporate automated, real-time, incident detection tools in high risk systems.
37. The personal information received and collected by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to fulfill its intelligence role is stored on several systems. This includes all reports submitted to the Centre. These systems contain detailed financial information and other sensitive personal information elements.

38. A record is created and logged when users log in, create, modify, view or delete files on any of the networks. However, not all logs are actively monitored to ensure the timely identification of inappropriate or unauthorized access to, or disclosure of, personal information that is accessible to internal users.

Recommendation

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should ensure that the activity logs of all IT (Information Technology) systems are regularly monitored for indications of inappropriate access, use, or disclosure, and for attempts to defeat security protocols, in order to ensure that such activity is detected and addressed in as timely a fashion as possible.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) is committed to protecting its data holdings. As noted in previous Office of the Privacy Commissioner (OPC) audits, the Centre has a robust and comprehensive approach to security, including a sound IT (Information Technology) security infrastructure to protect its networks and applications. Following the 2013 OPC (Office of the Privacy Commissioner of Canada) audit, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) undertook additional measures to further enhance the Centre's monitoring capabilities in relation to activity on FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) systems, including an IT (Information Technology) Security Enhancements project and a Data Loss Prevention initiative.

Going forward, the Centre's new Departmental Security Plan identifies a second phase of the Data Loss Prevention initiative. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will also continue to evaluate options and implement appropriate measures to enhance its ability to proactively detect inappropriate or malicious internal activity.

- **FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) continues to receive and retain personal information that does not meet reporting thresholds set out in the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).**

39. The PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) authorizes FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to receive reports from reporting entities and the CBSA (Canada Border Services Agency). By July 31, 2016, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had received almost 257 million such reports.
40. Our 2009 and 2013 audits found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) received and retained personal information that did not meet legal reporting thresholds. We issued recommendations calling on FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to mitigate this risk by implementing a process to screen incoming reports prior to retention.
41. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) implemented several measures to validate incoming reports. As the majority of reports received by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) are submitted electronically, fields on incoming reports are automatically reviewed to validate, through a number of "validation rules" whether required information is provided, and whether it is in the correct format. Checks are also conducted for some types of personal information that should not be provided --

such as Social Insurance Numbers (SIN) and some provincial health card numbers. Reports may be rejected outright, or a warning message may be issued to the reporting entity.

42. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s validation rules apply to the electronic submission of Suspicious Transaction Reports (STRs), Large Cash Transaction Reports (LCTRs), Electronic Funds Transfer Reports (EFTRs) and Casino Disbursement Reports (CDRs). As a result of the validation rules related to personal information, we noted that approximately 18,600 LCTR (Large Cash Transaction Report)s, EFTR (Electronic Funds Transfer Report)s, and CDR (Casino Disbursement Report)s submissions were rejected between June 1, 2014 and May 31, 2016.
43. STR (Suspicious Transaction Report)s are not rejected, even if the validation rules flag issues, as the Centre considers their content to be valuable. In some cases where STR (Suspicious Transaction Report)s contained unnecessary information, warning messages were sent to reporting entities. Voluntary Information Records are not subject to automatic validation.
44. These measures have been somewhat effective in identifying and deflecting non-compliant reports in some reporting categories. However, we found evidence through sampling that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) continues to receive and retain personal information that does not meet reporting thresholds.

Suspicious Transaction Reports

45. We noted five STR (Suspicious Transaction Report)s from a sample of 280 such reports which did not include any description of or justification for suspected money laundering or terrorist financing activities. The absence of such information in a report makes it difficult to assess whether the "reasonable grounds" threshold has been met.
46. We identified STR (Suspicious Transaction Report)s related to transactions that did not demonstrate "reasonable grounds to suspect" that they related to money laundering or terrorist financing activities; see examples below in **Exhibit A**. In each case a report was sent to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) – and FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) retained the report in its database.

Exhibit A

- A number of individuals identified themselves with Middle Eastern passports during a real estate transaction. The reporting entity filed an STR (Suspicious Transaction Report). No further details or justification for suspicion were provided.
- An individual intended to conduct a financial transaction. When the individual said he had invested in the stock market, particularly in medical marijuana companies, the reporting entity filed a STR (Suspicious Transaction Report) on the basis that "a person who is involved in the government regulated medical marijuana industry is also at high risk and may also have some relation to the illicit marijuana trade."
- A client of a financial institution wrote a cheque for more than $20,000 to a close relative. The entity filed a STR (Suspicious Transaction Report) because it did "not know the reason why the cheque was issued nor for such an amount". No further information justifying the report was given.

47. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has a process in place for segregating and subsequently disposing of reports which do not meet reporting thresholds. However, we found this process is not consistently followed. We were informed by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) that the Centre's analysts may decide to retain reports that do not meet thresholds, in case additional information is received in the future that could make the report useful.

Voluntary Information Records

48. We also examined a sample of Voluntary Information Records (VIRs). VIR (Voluntary Information Record)s submitted by entities other than law enforcement, government entities or foreign agencies similar to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) must be about suspicions of money laundering or the financing of terrorist activities. However, we found a number of VIR (Voluntary Information Record)s that were not submitted by these entities where there was no suspicion of money laundering or terrorist financing. **Exhibit B** below shows an example of such a situation.

Exhibit B

A financial institution's client was charged with a fraud related offence, which came to the attention of the institution through a media report. The financial institution filed a VIR (Voluntary Information Record), indicating that "an STR (Suspicious Transaction Report) was not filed because the transaction activity on the account was not deemed suspicious or indicative of money laundering."

49. The PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) states that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) shall receive information provided to the Centre by law enforcement agencies or government institutions or agencies. There is no reporting threshold associated with these VIR (Voluntary Information Record)s. However, VIR (Voluntary Information Record)s are routinely used to ask for information. **Exhibit C** shows an example of how a VIR (Voluntary Information Record) is used in this regard.

Exhibit C

A VIR (Voluntary Information Record) sent by a police force asked FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) for information on members of an Indigenous protest group opposing pipeline development. The VIR (Voluntary Information Record) noted that none of the individuals listed in the report was suspected to be a member of an organized crime or terrorist group. Despite this, the VIR (Voluntary Information Record) requested information on each individual's fundraising activities and charitable contributions.

50. These examples indicate that VIR (Voluntary Information Record)s - subject to a reporting threshold - and STR (Suspicious Transaction Report)s that do not meet legislated thresholds for reporting continue to be submitted to and retained by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). We acknowledge that the recent amendment adding subsection 54(2) to the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) obliges the Centre to destroy information that does not meet reporting thresholds when this determination is made in the normal course of its activities. However, in the absence of a more stringent front-end screening mechanism, such reports will continue to be received by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and retained in its databases, potentially for long periods of time, before they may be discovered and purged.

Recommendation

We encourage FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to continue its efforts to implement robust and comprehensive front-end screening for incoming submissions to ensure the records and reports it retains in its database meet legislated reporting thresholds and do not contain unnecessary and/or

excessive personal information.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) recognizes the importance of ensuring that its data holdings only contain information that the Centre has the legislative authority to receive. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will continue to implement the robust and comprehensive front-end screening measures that have been established in recent years to minimize the receipt of unnecessary personal information.

Terrorist Property Reports

51. Pursuant to the *Criminal Code* [23](#fn23) Reporting entities are required to file a Terrorist Property Report (TPR) to the RCMP and CSIS (Canadian Security Intelligence Service) if they have property in their possession or under their control that they know is owned or controlled by or on behalf of a terrorist group within the meaning of the legislation. This information must also be given to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) pursuant to the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act). Similarly, reporting entities must file a TPR (Terrorist Property Report) if they have property in their possession or control that they believe is owned or controlled by or on behalf of a person listed under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. As of December 2016, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had received a total 109 TPR (Terrorist Property Report)s since its inception.
52. We found in previous audits that almost half the TPR (Terrorist Property Report)s submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) were filed on the basis of a “possible match” to terrorist listings. It is FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) practice to retain these reports regardless of whether “possible” terrorist affiliation is later confirmed. We previously recommended that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) explore avenues with its intelligence partners to ensure, to the extent possible, that terrorist affiliations were confirmed prior to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)’s retention of this data.
53. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) committed to entering into a dialogue with its intelligence partners to explore ways to mitigate the risk of retaining information about individuals when it has been confirmed that no terrorist affiliation exists. Based on this commitment, our 2013 audit rated progress on this recommendation as satisfactory.
54. Our inquiries during this audit found no evidence that such a dialogue took place, and FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) confirmed that it has not received any communication from its law enforcement partners repudiating suspicions of terrorist affiliation for individuals named in TPR (Terrorist Property Report)s. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) informed us that it is unable by law to contact law enforcement partners to confirm or refute terrorist affiliation unless the threshold for disclosure of information to partners has been met.
55. We reviewed a sample of TPR (Terrorist Property Report)s and noted that the type of issues observed in 2009 and 2013 remain. Reporting entities continue to submit reports on the basis of a “possible match” to terrorist listings. In addition, we found a TPR (Terrorist Property Report) filed in 2007 on the basis of a “possible name match”; two months later, the reporting entity sent a correction to the first report indicating the individual was not affiliated with terrorism. Both the initial TPR (Terrorist Property Report) and the subsequent correction remain in the database.
56. We also observed that, as of December 2016, 42 TPR (Terrorist Property Report)s – almost half the number that had been submitted to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) since its

inception – reached the end of their ten-year retention periods and were disposed of by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) without ever having been used in a disclosure.

Recommendation

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should manually review all TPR (Terrorist Property Report)s, and immediately dispose of those which are identified as not meeting reporting thresholds.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will conduct a manual review of all Terrorist Property Reports in its data holdings. Should the Centre have, or receive, information from a reporting entity that has submitted a report or the appropriate authorities that a terrorist affiliation is no longer suspected to exist, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will immediately segregate and dispose of that report.

Reports with financial thresholds

57. We found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) continues to receive and retain reports that do not meet the specific financial thresholds set out in legislation. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) receives four types of reports for which precise and objective financial thresholds apply. These are: Electronic Fund Transfer Reports (EFTRs), Large Cash Transaction Reports (LCTRs), Casino Disbursements Reports (CDRs), and Cross Border Currency Reports (CBCRs). FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) is authorized under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) to collect reports only about transactions of $10,000 or more for these categories.
58. If two or more transactions of less than $10,000 each are made by or on behalf of the same individual or entity within 24 hours, and together total $10,000 or more, these must also be reported. This is referred to as the “24 hour rule” and applies to EFTR (Electronic Funds Transfer Report)s, LCTR (Large Cash Transaction Report)s and CDR (Casino Disbursement Report)s.
59. During our 2009 and 2013 audits, we found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) did not have the capacity to match incoming reports under the 24 hour rule. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) was unable to match EFTR (Electronic Funds Transfer Report)s and LCTR (Large Cash Transaction Report)s under $10,000 to others submitted by or on behalf of the same individual or entity within the 24 hour time period. The same issue was found again in this audit.
60. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has made efforts to develop an automated solution for this problem; however, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) acknowledges that its attempted solution has not been successful. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has advised us that an automated solution may not be possible. As a result, the risk level in this area has not improved since our first audit in 2009.
61. As of July 31, 2016, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had received over 254 million EFTR (Electronic Funds Transfer Report)s and LCTR (Large Cash Transaction Report)s since its inception. Among these are approximately 80,000 EFTR (Electronic Funds Transfer Report)s and 150,000 LCTR (Large Cash Transaction Report)s that are under the $10,000 reporting threshold and do not fall under the 24-hour rule. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) does not have the legislative

authority to retain transactions under $10,000 unless they are matched to another transaction made within 24 hours by or on behalf of the same individual or entity.

Recommendation

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should dispose of EFTR (Electronic Funds Transfer Report)s and LCTR (Large Cash Transaction Report)s that are below the $10,000 reporting threshold and that do not fall under the 24-hour rule, as the Centre has no legislative authority to retain this information.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) recognizes the importance of ensuring that its data holdings only contain information that the Centre has the legislative authority to receive. The Centre has taken a number of concrete steps in recent years to limit the receipt of reports that do not meet the legislated threshold for reporting. For example, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has put in place robust validation rules that reject the submission of purported reports that do not meet reporting thresholds. In addition, a well-defined process has been put in place to ensure that any such purported reports found in the Centre's data holdings in the normal course of activities are segregated in order to ensure they are not used for the purpose of analysis and are not disclosed. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) destroys information it identifies as not meeting the threshold for reporting as per its disposition process and related schedules.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) also undertakes numerous engagement and training activities with reporting entities to underscore the importance of ensuring that all reports sent to the Centre meet the legislative and regulatory thresholds. As well, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) is in the process of updating its guidelines for reporting entities with an enhanced focus on the 24-hour rule requirement in order to help further minimize the submission of information that does not meet the thresholds.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will also continue to ensure that its financial intelligence disclosures are made strictly in accordance with the legislation and do not contain reports that the Centre should not have received.

Going forward, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) will explore options to identify, segregate and destroy information that it should not have received.

- **FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) collects and retains unnecessary amounts and types of client personal information from entities that fall under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) while performing compliance examinations.**

62. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) carries out a compliance program to ensure reporting entities meet their obligations under the PCMLTFA (Proceeds of Crime (Money Laundering) and

Terrorist Financing Act). As of March 31, 2016, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had performed 7,450 compliance examinations. The PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) allows FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to collect information as part of its compliance examinations. The TBS (Treasury Board Secretariat) *Directive on Privacy Practices* [24](#fn24) requires government institutions to limit collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities.

63. Our 2013 audit found that FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) had collected and retained unnecessary personal information as part of its compliance files. This included photocopies of the tax records of deceased individuals, medical records, Proof of Death statements, credit reports, drivers' licenses, passports, and Social Insurance Number (SIN) cards.
64. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken measures to address our 2013 recommendations related to these issues, including implementing a policy that only the specific records or information needed to support deficiencies should be kept. However, the sample of compliance examination files we reviewed for this audit indicated that information which is not needed to support deficiencies continues to be retained.
65. We found that compliance examination files contained information that did not relate to the noted deficiency, and that information was retained where no deficiencies were found at all. Some of the information we noted in this regard included:
    - A business database showing multiple online payments with individuals' names, addresses, dates of birth, and SIN (Social Insurance Number)s;
    - Information on account openings including photocopies of drivers' licences;
    - Forms containing personal information, including information on identity cards, hire date, occupation;
    - Photocopies of account opening forms, including name, date of birth, SINs, citizenship information;
    - Employee names, emails and performance comments.

Recommendation

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should expand its outreach efforts to specifically address the issue of personal information unnecessarily provided by entities during compliance examinations. In addition, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should undertake an internal data minimization and purging exercise in order to dispose of personal information in its compliance examination files that is not needed to support deficiencies.

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

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) accepts the recommendation.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has in place a comprehensive outreach program to inform reporting entities of their obligations under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), including the types of information that should and should not be provided during compliance examinations. The Centre is currently revising its notification letters to make it even clearer to reporting entities that they are to provide only the information that is requested in the letter and that they are not to submit personal information that is not required.

Going forward, the Centre will look to expand its outreach efforts to address the issue of personal information unnecessarily provided by reporting entities during compliance examinations. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) is also implementing a Quality Assurance process that will underpin a data minimization and destruction exercise aimed at disposing of information received and collected in the context of its compliance examinations that does not support identified deficiencies.

Conclusion

66. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has made significant efforts to mitigate the risks of collecting information that is irrelevant to its mandate and/or exceeds its legislative authority. Progress has been made.
67. This includes the implementation of automated front-end screening to ensure that mandatory fields in reports sent to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) are completed. The screening process has rejected thousands of transactions that did not meet reporting thresholds. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has also undertaken compliance outreach activities to educate reporting entities as to what information is required, and what information should not be reported. In addition, there is a process in place by which information that should not have been reported can be segregated and destroyed when it is encountered by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) analysts in the course of their regular activities.
68. However, our examination findings indicate that many thousands of reports containing information that should not have been reported to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) remain in its database. This risk will remain until FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) enhances its current comprehensive front-end screening system that effectively filters out reports that do not clearly meet applicable legislative thresholds.
69. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) needs to work with Shared Services Canada to ensure that the personal information acquired, retained and transmitted by the Centre is appropriately protected when being stored and while being transmitted on SSC (Shared Services Canada) IT (Information Technology) infrastructure. This will require a collaborative effort between FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada), as the two institutions have shared responsibilities relating to the protection of the information received and collected by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and the certification and accreditation of the IT (Information Technology) systems on which it resides and through which it is transmitted.

ANNEX A

Assessment of Progress Related to Previous Recommendations

Based on our assessment of the actions taken by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) in addressing the recommendations from our 2013 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.

Our assessment of the actions taken by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) in addressing the recommendations from our 2009 audit was included in our 2013 audit report available at Audit of the Financial Transactions and Reports Analysis Centre of Canada. Final Report 2013 (/en/opc-actions-and-decisions/audits/ar-vr_fintrac_2013/).

2013 Recommendations	2017 Assessment
Protection of information holdings	

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should implement measures to ensure that all its staff members possess a sound awareness of FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s privacy and security policies to safeguard personal information and their obligation to comply with them at all times.	Satisfactory Various training and awareness sessions on Privacy, Information Management and Security have been provided.
Compliance with the Code of Fair Information Practices	
To reconcile its obligations under the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) with those under the *Privacy Act*, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should analyze and assess incoming reports to ensure that it receives and retains only information that meets legislated thresholds for reporting and which it needs or uses in an ongoing program or activity.	Unsatisfactory Our review found various instances of reports that did not meet reporting thresholds and therefore, should not be retained.
FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) 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 (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).	Satisfactory FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has conducted significant outreach activity. Likewise, it provides information and advice through its web site.
FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should identify and dispose of information that it should not have received and is not directly related to its operating programs and activities.	Unsatisfactory Reports that did not meet reporting thresholds are being retained.
FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should: a) finalize an agreement with LAC regarding terms and conditions for the transfer of its archival records, and b) implement a formal policy for information and records whose retention and disposal periods are not specifically covered by the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).	Satisfactory The agreement with LAC was signed. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has implemented retention and disposal schedules.
FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)'s Compliance Mandate	
In keeping with privacy best practices and to ensure consistent data minimization by compliance officers, FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) should update its policies and procedures to clearly identify what information compliance officers should record and retain on compliance files to support deficiencies.	Satisfactory Policies were updated to indicate that only information relevant to support deficiencies is to be retained on examination files.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) 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.	Unsatisfactory A QA program is not yet in place. Our review found that information not relevant to support deficiencies was kept.
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.	Satisfactory The form was amended as recommended.
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 (Financial Transactions and Reports Analysis Centre of Canada) should take action to ensure that guidance issued by regulatory partners is consistent with PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) requirements.	Satisfactory FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) sent correspondence to regulatory partners with emphasis to avoid over reporting and to achieve consistency in guidance issued to reporting entities.

ANNEX B

About the Audit

Authority

Section 37 of the *Privacy Act* authorizes the Privacy Commissioner to undertake compliance reviews of the manner in which government institutions manage their personal information holdings and make recommendations where appropriate. Under 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 audit objective was to assess whether FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has appropriate controls in place to protect the personal information it collects and retains, and whether FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) manages this information in compliance with sections 4 through 8 of the *Privacy Act*. In addition, we focused on whether FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) has taken adequate measures to ensure there are appropriate safeguards in place to protect the personal information in FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)’s electronic data holdings, which reside on Shared Services Canada’s (SSC) IT (Information Technology) infrastructure.

The audit also evaluated the collection of personal information from reporting entities by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) during its compliance assessment activities, and reviewed the progress made by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) in response to the

observations and recommendation in our 2009 and 2013 audits.

Criteria

The criteria for conducting the audit are based on the authorities of the *Privacy Act* and associated Treasury Board Secretariat (TBS) policies, as well as the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act). We expected FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) to:

- limit the receipt, collection and use of personal information to that which is necessary for the execution of its mandate;
- retain and dispose of personal information in accordance with governing authorities;
- have appropriate security measures in place for its information holdings, systems and infrastructure.

Scope and approach

The audit team examined FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) programs and processes where the impact on privacy was deemed to be significant. In addition, the role of SSC (Shared Services Canada) in safeguarding FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) information that resides or flows on its information technology infrastructure was reviewed.

We evaluated policies, guidelines, training materials, physical and IT (Information Technology) threat and risk assessments, memoranda of understanding (MOUs), and privacy control checklists. We also interviewed FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) and SSC (Shared Services Canada) staff members, examined reporting processes, and reviewed samples of reports and compliance examination files. All examination activities were conducted in the National Capital Region and our audit work was substantially completed on March 31, 2017.

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 Chartered Professional Accountants of Canada.

Audit Team

Acting Director General: Lara Ives

Sarah MacKay
Tauqeer Shaik
Ivan Villafan
Lindsay Scotton

Footnotes

1 While information on the reports that must be filed by reporting entities is laid out in the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), submissions, such as Suspicious Transaction Reports and Voluntary Information Records, may be made on an individual without them being aware that they have been the subject of a specific submission.

2 FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) standard practice in responding to *Privacy Act* requests is to neither confirm nor deny that an individual's records are in its database.

3 *Shared Services Canada Act*, S.C. 2012, c. 19

4 The Managed Secure File Transfer service.

5 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 [PCMLTFA]

6 Who Must Report. FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) webpage; Reporting

7 Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360

8 PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act), supra, subsection 72(2), Review by the Privacy Commissioner.

9 "Follow the money: is Canada making progress in combatting money laundering and terrorist financing? Not really." March 2013 report.

10 *Bill C-31, An Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures, 41st Parliament SC 2014*

11 Proceeds of Crime (Money Laundering) Terrorist Financing Act.

12 *Bill C-59, An Act to implement certain provisions of the budget tabled in Parliament on April 21, 2015 and other measures, 41st Parliament SC 2015*

13 Security of Canada Information Sharing Act, S.C. 2015, c. 20, s. 2

14 House of Commons Standing Committee on Finance. Terrorist Financing in Canada and Abroad: Needed Federal Actions. Second Session, 41st Parliament, 2015. Committee Report 13.

15 The Financial Action Task Force.

16 Financial Action Task Force Report: Canada's measures to combat money laundering and terrorist financing. September 2016

17 *Shared Services Canada Act*, Statues of Canada, 2012, c. 19

18 Treasury Board Secretariat. Policy on Government Security, 2009.

19 Treasury Board Secretariat. Operational Security Standard: Management of Information Technology Security (MITS)

20 Financial Administration Act, R.S.C., 1985, c. F-11

21 Treasury Board Secretariat. Guideline on Service Agreements: Essential Elements

22 Treasury Board Secretariat. Directive on Privacy Practices, 2014

23 Criminal Code, R.S.C., 1985, c. C-46.

24 Treasury Board Secretariat. Directive on Privacy Practices. 2014

Date modified:

2017-09-21