



FINTRAC

2022–23 Annual Report on the Administration of the *Privacy Act*

September 1, 2023



Safe Canadians,
Secure Economy

Table of Contents

1. Introduction.....	1
2. About FINTRAC	1
3. The Access to Information and Privacy Office	2
4. Delegation of Authority.....	2
5. Statistical Overview and Accomplishments	3
Performance of Privacy Request Case Activity	3
Disposition of Completed Privacy Requests.....	3
Completion Times and Extensions of Privacy Requests	4
Consultations under the Act.....	4
Corrections and Notations.....	4
Impact of COVID-19	4
Complaints and Investigations	4
Material Privacy Breaches	4
Privacy Impact Assessments (PIA).....	5
Disclosures of Personal Information under Subsection 8(2)(m) of the Act	5
6. Training and Education.....	5
7. New Privacy-related Policies, Guidelines, Procedures, or Initiatives	7
FINTRAC’s ATIP Office established a procedure to ensure that it has adequate measures in place for verifying the identity of applicants, and authorized individuals, when processing personal information requests under the Act and the <i>Access to Information Act</i>	7
8. Privacy Request Program Performance and Compliance Monitoring.....	7
9. Closing	8
10. ANNEX A – Director and Chief Executive Officer’s Delegation Order	9
11. ANNEX B – Statistical Report	10

Financial Transactions and Reports Analysis Centre of Canada

234 Laurier Avenue West
Ottawa, Ontario K1P 1H7 Canada
Telephone: 1-866-346-8722
Facsimile: 613-943-7931

www.fintrac-canafe.gc.ca

ISSN 2563-7339
Cat. No. FD2-6/2E-PDF

1. Introduction

This report to Parliament, which is prepared and tabled in accordance with Section 72 of the *Privacy Act* (hereafter the “Act”), describes the activities of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) in administering the Act during fiscal year 2022–23. This report should be considered along with FINTRAC’s 2022–23 *Annual Report on the Administration of the Access to Information Act*, which is tabled separately.

The purpose of the Act is to protect the privacy of individuals with respect to personal information about themselves held by government institutions and to provide individuals with a right of access to that information.

2. About FINTRAC

FINTRAC is Canada’s financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor and plays a critical role in combatting money laundering, terrorist activity financing, and threats to the security of Canada. The Centre has two core responsibilities framed around a duty to protect the personal information to which it is entrusted.

First, FINTRAC is responsible for ensuring compliance with Part 1 and 1.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations. This legal framework establishes obligations for specified businesses to develop a compliance regime in order to identify clients, monitor business relationships, keep records and report certain types of financial transactions to FINTRAC. These obligations allow for certain economic activities to be more transparent, which helps prevent and deter nefarious individuals and organizations from using Canada’s legitimate economy to launder the proceeds of their crimes or finance terrorist activities. FINTRAC is committed to working with businesses to help them understand and comply with their obligations. The Centre also takes firm action when it is required to ensure that businesses take their responsibilities seriously. This includes undertaking compliance enforcement action such as follow-up examinations, the development and monitoring of action plans imposed on businesses and the levying of administrative monetary penalties. The Centre also maintains a registry of Canadian-based money services businesses and foreign money services businesses that direct and provide services to persons and entities in Canada.

Second, FINTRAC generates actionable financial intelligence that assists Canada's law enforcement, national security agencies and international partners in combatting money laundering, terrorist activity financing and threats to the security of Canada. In addition, the Centre produces strategic financial intelligence for federal policy and decision-makers, the security and intelligence community, businesses across the country, international partners and other stakeholders. FINTRAC's strategic intelligence provides a wide analytic perspective on the nature, scope and threat posed by money laundering and terrorism financing.

3. The Access to Information and Privacy Office

FINTRAC's Access to Information and Privacy (ATIP) Office is responsible for leading, coordinating and undertaking the Centre's access to information and privacy responsibilities. The ATIP Office is part of FINTRAC's Communications Group and led by the Centre's Head of Communications, who reports directly to FINTRAC's Director and Chief Executive Officer. The Head of Communications, who is also the Centre's Chief Privacy Officer, is responsible for the overall management of all access to information and privacy matters within FINTRAC.

FINTRAC's ATIP Office consists of an ATIP Coordinator and two Senior ATIP Advisors. Key responsibilities of the ATIP Office include:

- developing and implementing policies, procedures, and guidelines to ensure FINTRAC's compliance with the Act and the *Access to Information Act*;
- ensuring the timely processing of privacy and access to information requests, and meeting proactive disclosure obligations;
- providing advice, guidance, and awareness activities to FINTRAC employees, contractors, and students on ATIP-related matters;
- representing FINTRAC in its discussions and negotiations with external stakeholders, including other government departments, third parties, the Treasury Board of Canada Secretariat, the Office of the Privacy Commissioner, the Office of the Information Commissioner and the general public;
- maintaining Personal Information Banks and conducting privacy impact assessments; and
- preparing annual reports on the administration of the Act and the *Access to Information Act* to Parliament and publishing FINTRAC's Info Source Chapter.

To support the ATIP Office in meeting its legislative obligations, FINTRAC has established a collaborative network comprised of representatives from all sectors and relevant units within the Centre. These representatives are responsible for coordinating requests, providing guidance on the Act within their work units, and liaising with the ATIP Office on all ATIP-related matters. FINTRAC is not party to any service agreements under section 73.1 of the Act.

4. Delegation of Authority

Order in Council P.C. 2000-1066 designates the Director and Chief Executive Officer of the Centre as head of FINTRAC for the purposes of administering the Act and FINTRAC's privacy program. Pursuant to Section 73 of the Act, FINTRAC's Director and Chief Executive Officer delegated the authority to exercise the powers, functions, and duties under the Act to FINTRAC's Head of Communications and its ATIP Coordinator. These functions have full-delegated authority under the Act and the *Access Information Act*, in accordance with the delegation of authority instrument approved by the Director and Chief Executive Officer in March 2023.

A copy of the Director and Chief Executive Officer's Delegation Order is available at Annex A.

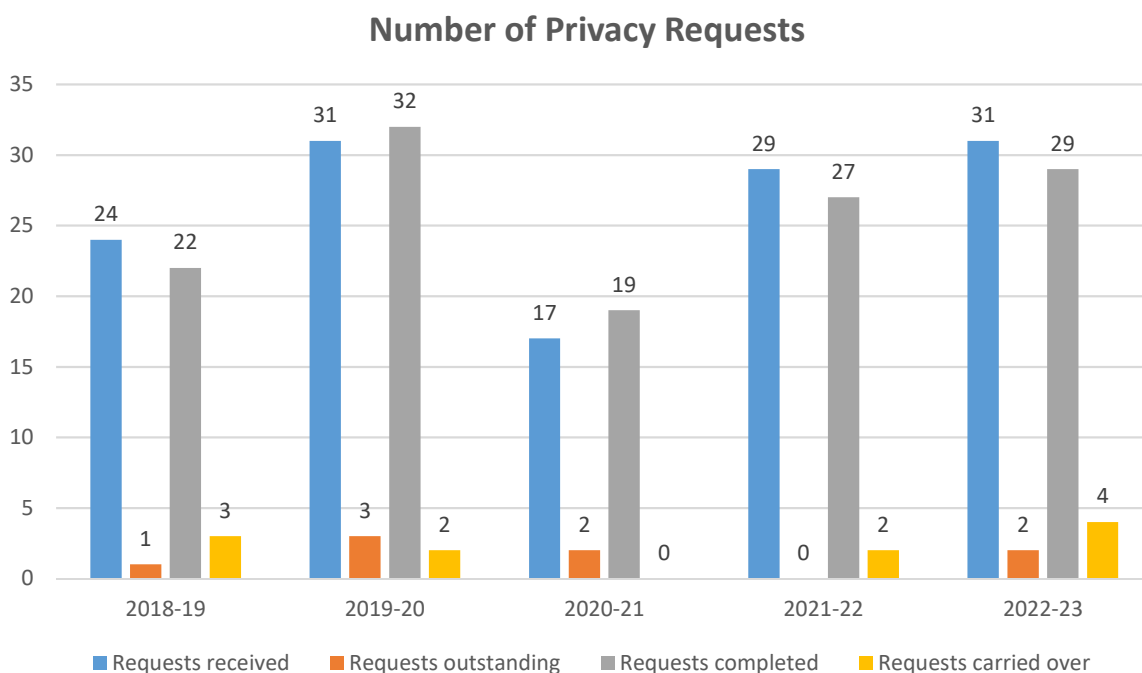
5. Statistical Overview and Accomplishments

Annex B contains FINTRAC’s detailed Statistical Report on the *Privacy Act* for April 1, 2022 to March 31, 2023.

Performance of Privacy Request Case Activity

During the reporting period of April 1, 2022 to March 31, 2023, there was a slight increase in the number of requests received by FINTRAC (31) under the Act compared to the previous reporting year (29). With 2 outstanding requests from the previous fiscal year, FINTRAC had a total caseload of 33 requests in 2022–23, of which 29 were closed, as follows:

- 16 requests were completed in 1-15 days; and
- 13 requests were completed in 16-30 days.



Four remaining requests were carried over to 2023–24 and completed within the legislated timeline. FINTRAC maintained an on-time response rate of 100% for all privacy requests in 2022–23, well above the federal government’s overall average response rate of 70% in 2021–22.

Disposition of Completed Privacy Requests

FINTRAC completed 29 requests in 2022–23:

- In 3 cases, representing 10% of the overall cases, the applicant received full disclosure of the information.

- In 3 cases, representing 10% of the overall cases, the applicant received partial disclosure of the information.
- In 19 cases, representing 66% of the overall cases, FINTRAC responded that it was unable to acknowledge the existence of information.
- In 2 cases, representing 7% of the overall cases, it was determined that no records existed within FINTRAC's information holdings.
- In 2 cases, representing 7% of the overall cases, the applicant abandoned their request.

Completion Times and Extensions of Privacy Requests

The Act allows an additional 30-day extension beyond the 30-day statutory period for specific reasons. During the reporting period, FINTRAC completed all requests within the 30-day statutory deadline.

Consultations under the Act

Consultations undertaken between institutions are an essential part of processing requests under the Act. They provide institutions that have an interest in the records proposed for disclosure with an opportunity to make recommendations to the processing institution. For this reporting period, FINTRAC did not receive any consultation requests from other government institutions.

Corrections and Notations

For this reporting period, FINTRAC did not receive any requests for corrections of personal information.

Impact of COVID-19

FINTRAC's Access to Information and Privacy Office was fully operational, working both remotely and on-site, and able to receive, process, and respond to requests under the Acts.

Complaints and Investigations

Subsection 29(1) of the Act describes how the Office of the Privacy Commissioner receives and investigates complaints from individuals regarding the processing of requests under the Act.

FINTRAC did not receive any new complaints under the Act in the reporting period.

Material Privacy Breaches

A privacy breach involves improper or unauthorized collection, use, disclosure, retention, or disposal of personal information. As required by the Treasury Board of Canada Secretariat's *Directive on Privacy Practices*, institutions and their delegated authorities are required to establish plans and procedures for addressing privacy breaches. During the reporting period, no material privacy breaches occurred and, therefore, none were reported by FINTRAC to the Office of the

Privacy Commissioner, or to the Information and Privacy Policy Division of the Treasury Board of Canada Secretariat.

Privacy Impact Assessments (PIA)

The Government's *Directive on Privacy Impact Assessments* (PIAs) requires that FINTRAC ensure privacy principles are taken into account when there are proposals for, and during the design, implementation and evolution of, programs and services that raise privacy issues. FINTRAC currently has core PIA reports in place for its main programs and services.

In 2022–23, FINTRAC completed no new core PIAs. However, in accordance with its *Privacy Policy*, FINTRAC routinely conducts privacy impact checklists that must be completed during the design phase of projects involving an addition or a change to a program using personal data. The Centre completed one privacy impact checklist in 2022–23. Along with these checklists, FINTRAC's Security, Information Management and ATIP experts are engaged in projects involving personal information. The ATIP Office provides regular advice and guidance to FINTRAC employees to further ensure that the Centre manages its personal information holdings effectively and in accordance with the Act.

Disclosures of Personal Information under Subsection 8(2)(m) of the Act

In accordance with subsection 8(2)(m) of the Act, a government institution may disclose personal information under its control without the consent of the individual to whom the information relates if the disclosure is in the public interest or would clearly benefit the individual.

In 2022–23, FINTRAC made 1 disclosure under subsection 8(2)(m) of the Act as it was clearly in the public interest to do so. The disclosure involved the internal sharing of information for security purposes. It was determined that the protection of FINTRAC's assets, systems and intelligence far outweighed any invasion of privacy that could have resulted from the exceptional use of the individual's personal information. Prior to disclosing, the use of information was approved by FINTRAC's Director and Chief Executive Officer and was reported to the Office of the Privacy Commissioner.

6. Training and Education

Information protection is integral to FINTRAC's mandate. As such, the Centre requires its employees (including students and contractors) to have a heightened awareness of security, privacy, information management and access to information. The FINTRAC *Code of Conduct, Values and Ethics* specifically describes employees' legal obligations to protect information under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and makes reference to the *Privacy Act*, the *Canadian Charter of Rights and Freedoms*, the *Access to Information Act*, and the Centre's privacy, security and information management policies. Adherence to the *Code of Conduct, Values and Ethics* is a condition of employment for every FINTRAC employee.

The following training and awareness activities took place during the reporting period:

- The ATIP Office published monthly information notices regarding access to information and privacy protection on FINTRAC's intranet site.
- The ATIP Office also raises awareness by providing day-to-day coaching and targeted information sessions to ATIP representatives across the Centre. In 2022–23, 3 one-on-one training sessions were delivered. This focused training fosters a spirit of collaboration and has been essential to the success of FINTRAC's broader ATIP program.
- Work is currently underway to modify FINTRAC's existing ATIP awareness training to a self-directed online learning format. While working on this modified training format, the ATIP Office delivered 1 virtual ATIP awareness session to 10 employees in 2022–23.
- Access to information and privacy protection messaging is incorporated in mandatory Information Management awareness sessions and in New Employee Orientation Training. In 2022–23:
 - Information Management awareness training was received by 143 employees. The sessions raised employee awareness about their information management responsibilities, including in relation to ATIP, and covered the obligations and best practices for managing personal information in accordance with the *Privacy Act*, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, and FINTRAC's privacy, security and information management policies.
 - The New Employee Orientation Training moved to a virtual/hybrid format and is currently being redesigned into a self-directed online learning format. The training provides information about the Centre's mandate and reinforces to employees the importance of information management and safeguarding information and privacy particularly as fundamental components of the work undertaken by the Centre. A total of 69 employees and students completed this virtual training.
- FINTRAC employees completed the following online learning courses at the Canada School of Public Service:
 - *Access to Information and Privacy Fundamentals* (6 employees)
 - *Access to Information in the Government of Canada – I701* (2 employees)
 - *Privacy in the Government of Canada – I015* (1 employee)
- FINTRAC's Legal Services unit provides privacy awareness in its training of new employees, *Legal Framework of FINTRAC*, which outlines the various provisions of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* that promote the protection of Canadians' privacy. The sessions reinforce employees' obligations with respect to receiving, collecting, using, disclosing and safeguarding personal information under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In 2022–23, 4 sessions were provided to 56 employees.
- Given the sensitive information and environment in which FINTRAC operates, a heightened understanding of information security is required of all employees. In addition

to the requirement to complete the Canada School of Public Service Security Awareness Course (A230), new and returning employees must also undertake an in-house mandatory security awareness session. In 2022–23, a total of 120 new employees received the FINTRAC security awareness presentation in digital format and were required to acknowledge and confirm that they understood their responsibilities. These sessions covered the importance of security at FINTRAC; provided an understanding of the potential security risks (e.g. cyber, personal, operational, and insider threats) in relation to FINTRAC’s environment; highlighted the roles and responsibilities of all employees; discussed classification, transmission, and storage of information; covered the need to know/need to share principle; and emphasized the consequences of unauthorized disclosure and inappropriate use of information.

- As well as mandatory security training, all FINTRAC employees are made aware of the consequences of unauthorized disclosure and inappropriate use of personal information, which is covered in FINTRAC’s Policy on Security. All new employees are required to acknowledge that they have read and understood this policy.
- In 2022, FINTRAC continued its partnership with a specialized vendor to provide additional optional security awareness training for all employees. Employees have access to videos, simulations and best practices to reinforce their security knowledge.

7. New Privacy-related Policies, Guidelines, Procedures, or Initiatives

FINTRAC’s ATIP Office established a procedure to ensure that it has adequate measures in place for verifying the identity of applicants, and authorized individuals, when processing personal information requests under the Act and the *Access to Information Act*.

8. Privacy Request Program Performance and Compliance Monitoring

FINTRAC’s automated case management system facilitates timely responses to requests, documents important actions and decisions and monitors performance. The system also includes an audit log, has extensive search capabilities to enable analysis of previously processed information, and generates progress and statistical reports. During the reporting year, FINTRAC adopted the centralized platform ATIP Online Management Tool to receive requests under the Act and communicate with applicants.

Privacy is a key consideration in all FINTRAC programs and activities. As per its *Privacy Policy* FINTRAC’s ATIP Office is engaged and assesses all new projects and programs, including contracts and agreements, that involve the use of personal information to ensure that privacy and information safeguards are at the forefront of these activities.

The ATIP Office provides updates to senior management within FINTRAC's corporate governance, as well as providing briefings on ATIP files to FINTRAC's Executive Committee on a regular basis.

9. Closing

Through its robust privacy management framework, FINTRAC continues to safeguard the personal information under its control as it focuses on protecting Canadians and the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist activity financing.