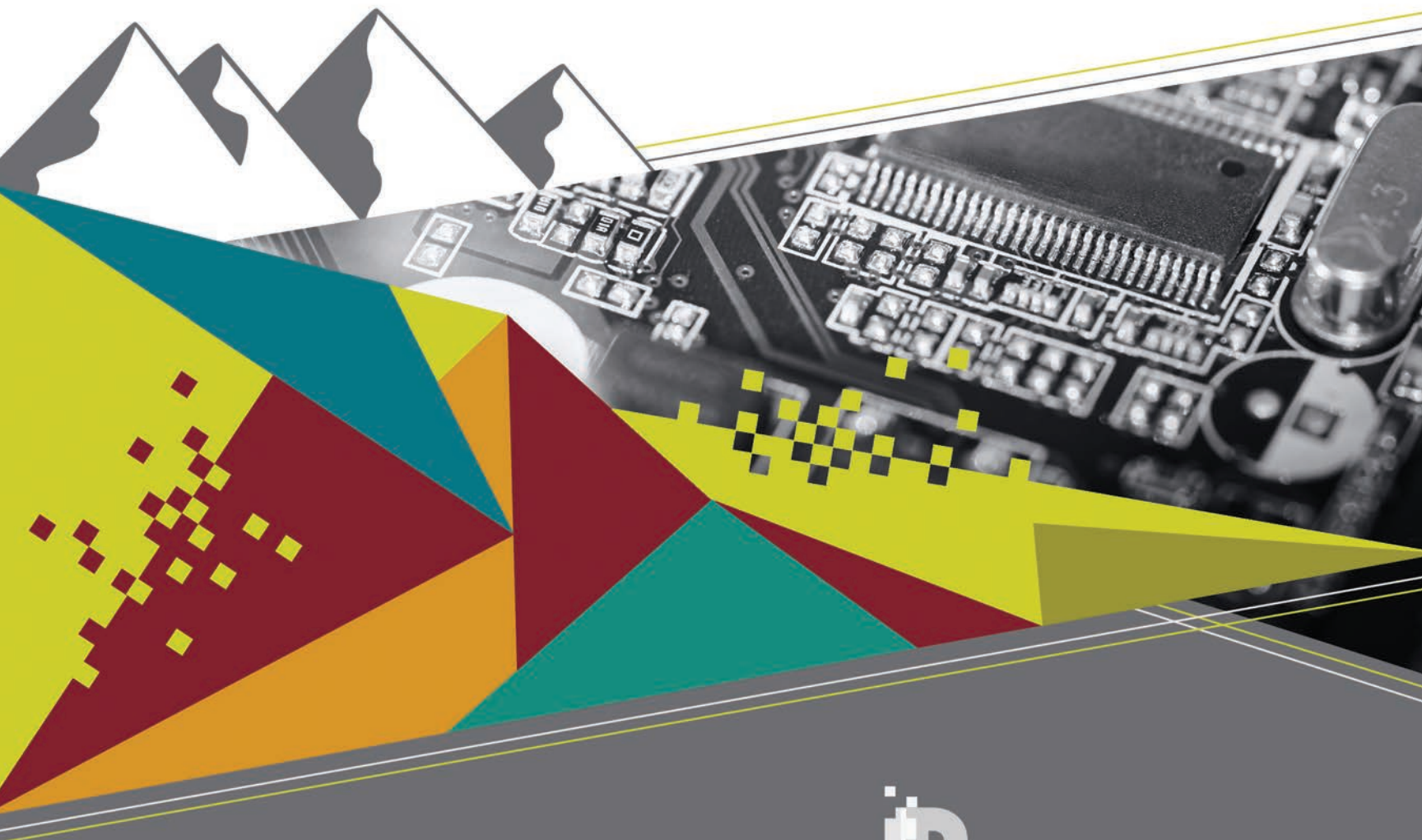


# ANNUAL REPORT 2022-23



Office of the Information and  
Privacy Commissioner of Alberta



Office of the Information and  
Privacy Commissioner of Alberta

**Office of the Information and  
Privacy Commissioner of Alberta**

410, 9925 - 109 Street, NW  
Edmonton, AB T5K 2J8

Phone: 780.422.6860  
Toll Free: 1.888.878.4044  
Fax: 780.422.5682  
Email: [generalinfo@oipc.ab.ca](mailto:generalinfo@oipc.ab.ca)  
Twitter: @ABoipc

**[www.oipc.ab.ca](http://www.oipc.ab.ca)**

NOVEMBER 2023



Office of the Information and  
Privacy Commissioner of Alberta

November 2023

Honourable Nathan Cooper  
Speaker of the Legislative Assembly  
325 Legislature Building  
10800 – 97 Avenue NW  
Edmonton, AB T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2022 to March 31, 2023.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act*, section 95(1) of the *Health Information Act*, and section 44(1) of the *Personal Information Protection Act*.

Sincerely,

Original signed by

Diane McLeod  
Information and Privacy Commissioner

# TABLE OF CONTENTS

Letter to the Speaker .....	3
Commissioner's Message .....	6
<b>ABOUT THE OFFICE .....</b>	<b>11</b>
Mandate .....	12
Commissioner's Powers, Duties and Functions.....	13
Vision.....	13
Mission .....	13
Organizational Structure .....	14
Request for Review and Complaint Process .....	15
OIPC as a Public Body .....	16
FOIP Requests to the OIPC.....	16
OIPC Privacy Matters.....	16
Proactive Travel and Expenses Disclosure.....	17
Public Sector Compensation Transparency Act .....	17
Public Interest Disclosure (Whistleblower Protection) Act.....	17
Financial Overview .....	18
Total Actual Costs Compared to Budget.....	18
Total Actual Costs Compared to Prior Year .....	18
<b>TRENDS AND ISSUES .....</b>	<b>19</b>
PIPA Review .....	20
Private Sector Privacy Breaches .....	22
<b>BY THE NUMBERS .....</b>	<b>25</b>
Graph A: Total Cases Opened.....	26
Graph B: Total Cases Closed .....	26
Table 1: Cases Opened by Case Type .....	27
Table 2: Cases Closed by Case Type .....	28
Table 3: Cases Closed by Resolution Method.....	29
Graph C: Percentage of Cases Closed by Resolution Method .....	30
Table 4: General Enquiries .....	30
Table 5: Total Cases Carried Over Into Fiscal Year 2023-24	
By Team & Case Type.....	31
<b>REGULATION AND ENFORCEMENT .....</b>	<b>35</b>

Table of Contents - Continued on the Next Page

# TABLE OF CONTENTS

Investigation Reports.....	36
Tim Hortons App Found to Collect Vast Amounts of Sensitive Location Data.....	36
PORTpass Vaccine Verification App Failed to Demonstrate Safeguards.....	38
Mediation and Investigation.....	39
Case Trends .....	39
Requests for Time Extensions by Public Bodies .....	41
Privacy Impact Assessment Reviews.....	42
HIA.....	42
FOIP .....	43
Privacy Breaches.....	44
PIPA.....	44
HIA.....	45
FOIP .....	45
Offence Investigations under HIA .....	46
Summary of Significant Decisions .....	47
Judicial Reviews and Other Court Decisions.....	49
Judicial Reviews .....	49
Other Court Decisions .....	51
<b>EDUCATION AND OUTREACH .....</b>	<b>53</b>
Speaking Engagements.....	54
Collaboration with Other Jurisdictions.....	54
New Memorandum of Understanding on Private Sector Privacy .....	54
Joint Statement on Facial Recognition .....	54
Joint Resolution on Securing Public Trust in Digital Healthcare .....	55
Media Awareness.....	56
Traditional Media .....	56
Social Media .....	56
New OIPC Website Platform.....	56
<b>FINANCIAL STATEMENTS.....</b>	<b>57</b>
<b>APPENDICES .....</b>	<b>75</b>

# COMMISSIONER'S MESSAGE



Commissioner Diane McLeod

On August 1, 2022, I was sworn in as Alberta's fourth Information and Privacy Commissioner. As a born and raised Albertan, I am honoured to have been chosen to fill this role in my home province.

For nine years prior to taking on this position, I was the Ombudsman, Information and Privacy Commissioner, and Public Interest Disclosure Commissioner in the Yukon. Prior to that, I served in the public sector, health sector and private sector for more than a decade, working with business, government and health care custodians to help them meet their obligations under access and privacy laws in Alberta and British Columbia. This wealth of experience will serve me well, as I meet the challenges to come.

While conducting research before taking on this role, I learned that Alberta has positioned itself as a leader in the use of information technology, with several institutions dedicated to this work, including the National Institute of Nanotechnology, which operates in conjunction with the University of Alberta; Alberta Innovates; InnoTech Alberta; and the Alberta Machine Intelligence Institute. In addition, Alberta has a robust information and communications technology (ICT) industry and is home to approximately 4,600 companies that employ approximately 50,000 employees, making ICT one of Alberta's key sectors.<sup>1</sup>

Alberta's 20-year Strategic Capital Plan<sup>2</sup>, published in December of 2021, sets out several themes that emphasize the importance of capital investment in information technology as a measure to improve or enhance service delivery in the public and health sectors and to manage the economy. This plan identifies the need to break down silos between sectors to achieve a more client-centred approach to service delivery. It further identifies the use of big data and technology, such as artificial intelligence (AI), as key to realizing many of the objectives identified in the plan to improve Alberta's economy.

The Alberta Technology and Innovation Strategy<sup>3</sup>, published in April of 2022, identifies a number of “research and commercialization priorities”.<sup>4</sup> Among the priorities listed are “health and disease prevention” and “emerging technologies”. Mentioned within these priorities are: increased application of digital technologies in health care and communities; advancing novel diagnostics, medical devices and therapeutics; advancing commercialization opportunities in areas of existing strength, including artificial intelligence, machine learning and quantum science; and harnessing the digital economy across sectors, including ... big and open data, to encourage digital adoption.<sup>5</sup> The Ministry of Technology and Innovation was established in October of 2022 to advance these objectives.

Innovative and entrepreneurial ideas and thought leaders are abundant in Alberta. With the right foundation established by government, it is only a matter of time before novel technologies, including AI, will be used in the public, health and private sectors. While innovative technologies can benefit citizens through improvement of services, harm to individuals and the public can also result, including harm stemming from the use of personal or

health information. In early 2023, pioneers of AI began calling for appropriate oversight of the development of AI systems and for guard rails around the development and use of this kind of technology.<sup>6</sup>

I have always been a firm believer in supporting the use of technology to innovate, including technology that involves the use of personal or health information, so long as there is a clear pathway of responsible innovation. This means there must be a proper regulatory framework in place that facilitates the use of personal or health information, where appropriate and necessary, in the development, implementation and use of the technology, which also includes measures to prevent harm, to ensure effective oversight and to provide strong deterrence against non-compliance. It also entails public trust. For there to be trust in the system designed to facilitate the development and use of this technology, the system must be robust from a privacy management perspective. This means that any organization, public body or health custodian wishing to develop or use this technology must first have in place an effective privacy management program comprised of leadership, policies and procedures, use of privacy

---

<sup>1</sup> <https://open.alberta.ca/dataset/10989a51-f3c2-4dcb-ac0f-f07ad88f9b3b/resource/e68b9292-51d5-40e8-8151-d148bda6d473/download/2016-highlights-alberta-economy-2016-07.pdf>.

<sup>2</sup> <https://open.alberta.ca/dataset/02bb977c-1478-4395-a70d-a4d36082c68c/resource/97f93890-6dc6-4811-8934-298d1ca1c5fd/download/infra-2021-20-year-strategic-capital-plan.pdf>.

<sup>3</sup> <https://open.alberta.ca/dataset/60b678e2-76d6-4231-a76b-914270ed1a3f/resource/955cd7da-a537-4c6f-a815-cb759d47d8fc/download/jei-alberta-technology-and-innovation-strategy-2022.pdf>.

<sup>4</sup> Ibid., at p. 22.

<sup>5</sup> Ibid., at p.23.

<sup>6</sup> <https://www.cbc.ca/news/world/artificial-intelligence-extinction-risk-1.6859118>.



enhancing tools such as privacy impact assessments, and measures to evaluate the program to ensure it is operating effectively.

In Alberta, we have three laws that govern privacy: the *Freedom of Information and Protection of Privacy Act* (FOIP Act), the *Health Information Act* (HIA), and the *Personal Information Protection Act* (PIPA). All three laws require review and amendment in order to create a responsible framework for technology innovation in our province.

While there are many public bodies, custodians and private sector organizations that have in place privacy management programs, there are many that do not. Much work is needed within all three sectors to establish a trusted foundation to facilitate and use innovative technologies.

It is also necessary that developers of this technology have a clear understanding of Albertans' privacy rights under our privacy laws to ensure that the technology is developed in such a way that these rights will be protected by users of the technology and that all reasonable steps are taken to minimize risks of harm.

My office has a significant amount of expertise in privacy. We have a clear understanding of what is necessary from a legal, technical and security standpoint to protect the privacy rights of Albertans in the digital age. Because of our expertise, I am of the view that my office has a role to play in supporting the digital services transition in Alberta, which is key to my vision and goals for this office.

## Commissioner's Vision and Goals

### Goal # 1: Support innovation through the use of technology.

We will achieve this goal by:

- creating alliances with industry leaders who are doing this work and working alongside them to build privacy into the design and use of these technologies;
- facilitating the adoption of privacy management programs more broadly within public, private and

health care sector organizations to establish a trusted network that will allow greater information-sharing across these sectors and position these organizations to use innovative technologies to enhance service delivery; and

- working with government to design privacy and access to information laws that will facilitate innovation, while preserving privacy and access rights, through the use of control measures that will achieve this balance.

### Goal # 2: Shift the office from working in a primarily reactive manner to adopting a service delivery model that more proactively supports compliance.

We will achieve this goal by:

- becoming known amongst public, health care and private sector organizations as a trusted resource, which will work with them to support improvements in privacy management and access to information;
- working alongside industry leaders in the advancement and use of innovative technologies by building privacy and access to information into the design of these systems; and
- working with stakeholders and government to inform amendments required to privacy and access to information laws that will facilitate innovation and preserve the access to information and privacy rights of Albertans.

## Addressing our backlog

The office has a significant backlog in conducting our casework that must be addressed. As you will see in our *By the Numbers* section of this annual report, we closed (4,013) nearly as many cases as we opened (4,289). However, we carried over 3,534 cases that were opened in 2022-23 or prior years that remained open at fiscal year end. This demonstrates that we have a significant backlog in cases that is affecting the access and privacy rights of Albertans.



In the fall of 2022, we began examining all our procedures with the goal of reducing the time it takes to process a file while still maintaining quality and value. There were two areas of focus during 2022-23, which were mediation and breach management.

We began by examining how we are managing our mediation function. Almost 80% of our complaints and requests for review (RFRs) are settled by the Mediation and Investigation (MI) team. As such, how we perform this work is key to improving our overall efficiency. As I began examining our mediation process, I learned that it was taking approximately 15 to 18 months from the date of a complaint or RFR to reach settlement. This is simply too long. We need to reduce the amount of time it takes to resolve a complaint or RFR. I began working with the MI team on its processes and we were able to find some solutions. We established a project plan in early 2023 to implement these solutions, which will reduce our timelines for settlement. We aim to roll out the new procedures in early 2024.

We also started looking at how we are managing breaches reported under PIPA and HIA. We established a project to modify our approach and we anticipate that it too will be ready to roll out in early 2024.

As part of these projects, I will establish performance benchmarks that I will report on in my 2023-24 Annual Report and thereafter during my term. Performance reporting will help us continue to evaluate our work and establish baselines for resource needs.

In 2022-23, I also restructured the office to facilitate centralized case management to improve the management of case files from open to close. In addition, to achieve my vision, I established a strategic engagement function within my office.

## About our work

In this annual report, there are stories about our work in conducting joint investigations that we undertake with other jurisdictions in Canada. These investigations generally stem from matters of public interest that require a collaborative approach to ensure that the interests of all jurisdictions in Canada are represented in the investigation. In 2022-23, we investigated Tim Hortons about its use of location data. Together with my colleagues in British Columbia, Quebec and at the federal level<sup>7</sup>, we found that Tim Hortons was offside the privacy laws in these jurisdictions in regard to the collection of this data. Tim Hortons accepted our recommendations and was in the process of implementing them by the end of 2022-23. In the same year, we launched a joint investigation of TikTok. The investigation will examine whether the organization's practices are in compliance with Canadian privacy legislation. Later in 2023 we also launched an investigation into OpenAI, the company responsible for ChatGPT. I will report on the status of these investigations in my 2023-24 Annual Report.

In terms of access to information, we have seen an increase in requests from public bodies for time extensions. These have risen steadily over the past decade to hundreds of requests. In 2022-23, there were 294 requests for time extensions. Not only is this volume of requests impacting our workload, it is creating significant delays in access to government information. We are monitoring this situation closely and will be working with public bodies to understand why they see the need for more time to process access requests.

These and many other stories about our work can be found in this annual report. I hope you find the information useful in understanding the work of my office.

**Diane McLeod**

Information and Privacy Commissioner

---

<sup>7</sup> Alberta, British Columbia and Quebec are the only provinces in Canada that have private sector privacy laws that are substantially similar to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Privacy Commissioner of Canada is responsible for oversight of PIPEDA. PIPEDA applies in every other province and the territories.





A modern office interior with glass partitions, desks, and chairs. The office is bright and airy, with large windows and a clean, minimalist design. The floor is a light teal color, and the walls are white. The ceiling has exposed ductwork and modern lighting fixtures. The office is furnished with black leather chairs, white desks, and various office equipment like computers and printers. There are also some potted plants and colorful storage bins.

# ABOUT THE OFFICE

# MANDATE

The Information and Privacy Commissioner is an Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta and is independent of the government. Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy laws.

## *Freedom of Information and Protection of Privacy Act*

The *Freedom of Information and Protection of Privacy Act* (FOIP Act) applies to public bodies, including provincial government departments, agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

FOIP provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use or disclose personal information.

## *Health Information Act*

The *Health Information Act* (HIA) applies to health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists and dental hygienists.

HIA also applies to "affiliates" who perform a service for custodians, such as employees, contractors, students

and volunteers. Custodians are responsible for the information collected, used and disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

HIA protects patients' privacy by regulating how health information may be collected, used and disclosed, and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through the provincial electronic health record information system (that is, Alberta Netcare).

## *Personal Information Protection Act*

The *Personal Information Protection Act* (PIPA) applies to provincially regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

PIPA seeks to balance the right of the individual to have their personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. The Act also gives individuals the right to access their own personal information held by organizations and to request corrections.

## COMMISSIONER'S POWERS, DUTIES AND FUNCTIONS

The Commissioner oversees and enforces the administration of the Acts to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- Providing independent review and resolution on requests for review of responses to access to information requests and privacy complaints related to the collection, use and disclosure of personal and health information
- Investigating any matters relating to the application of the Acts, whether or not a review is requested
- Conducting inquiries to decide questions of fact and law and issuing binding orders
- Reviewing privacy breach reports submitted by private sector organizations and health custodians as required under PIPA and HIA, and when voluntarily submitted by public bodies
- Reviewing and commenting on privacy impact assessments submitted to the Commissioner
- Receiving comments from the public concerning the administration of the Acts
- Educating the public about the Acts, their rights under the Acts, and access and privacy issues in general

- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the access and privacy implications of existing or proposed legislative schemes and programs
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

## VISION

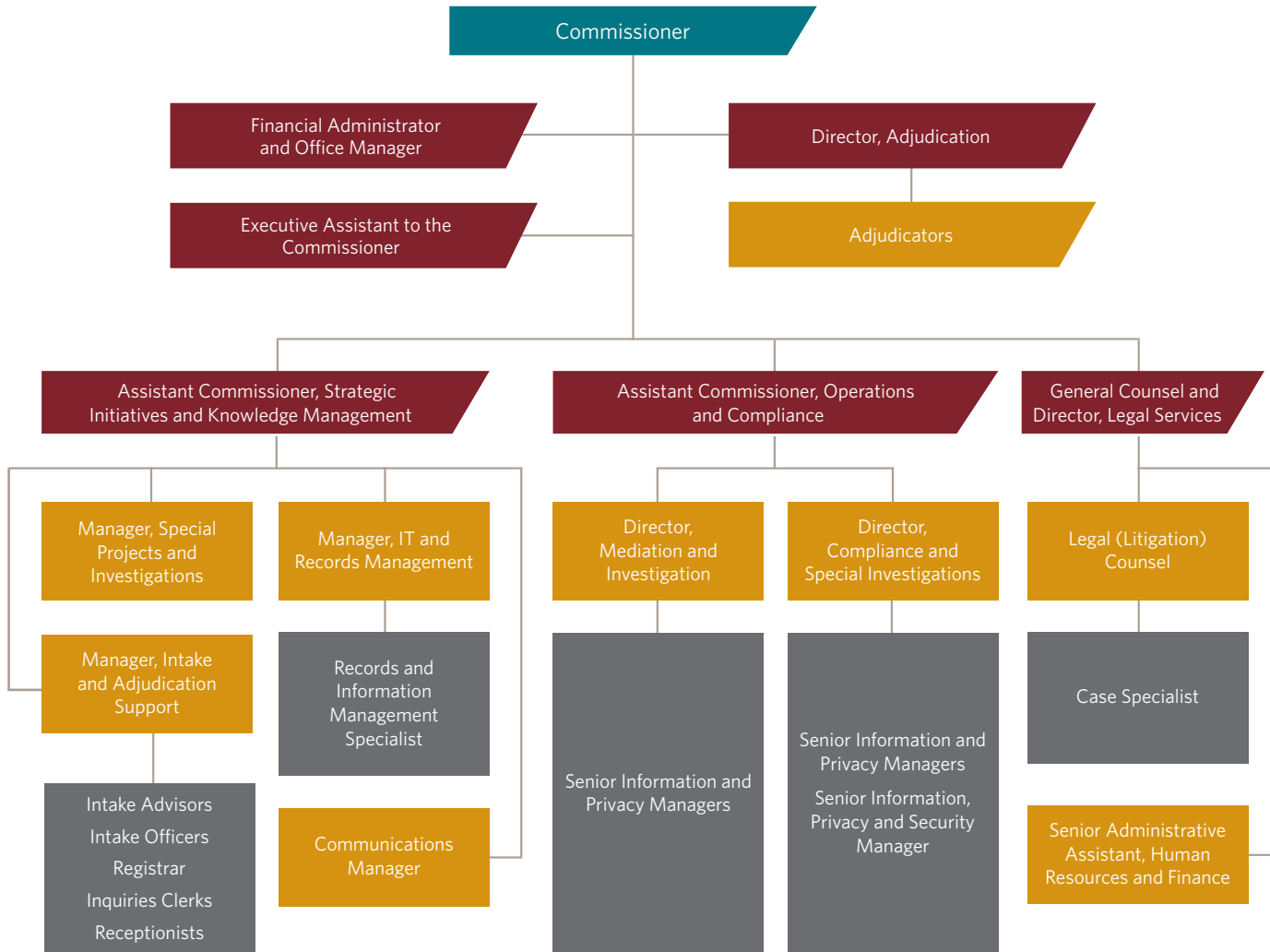
A society that values and respects access to information and personal privacy.

## MISSION

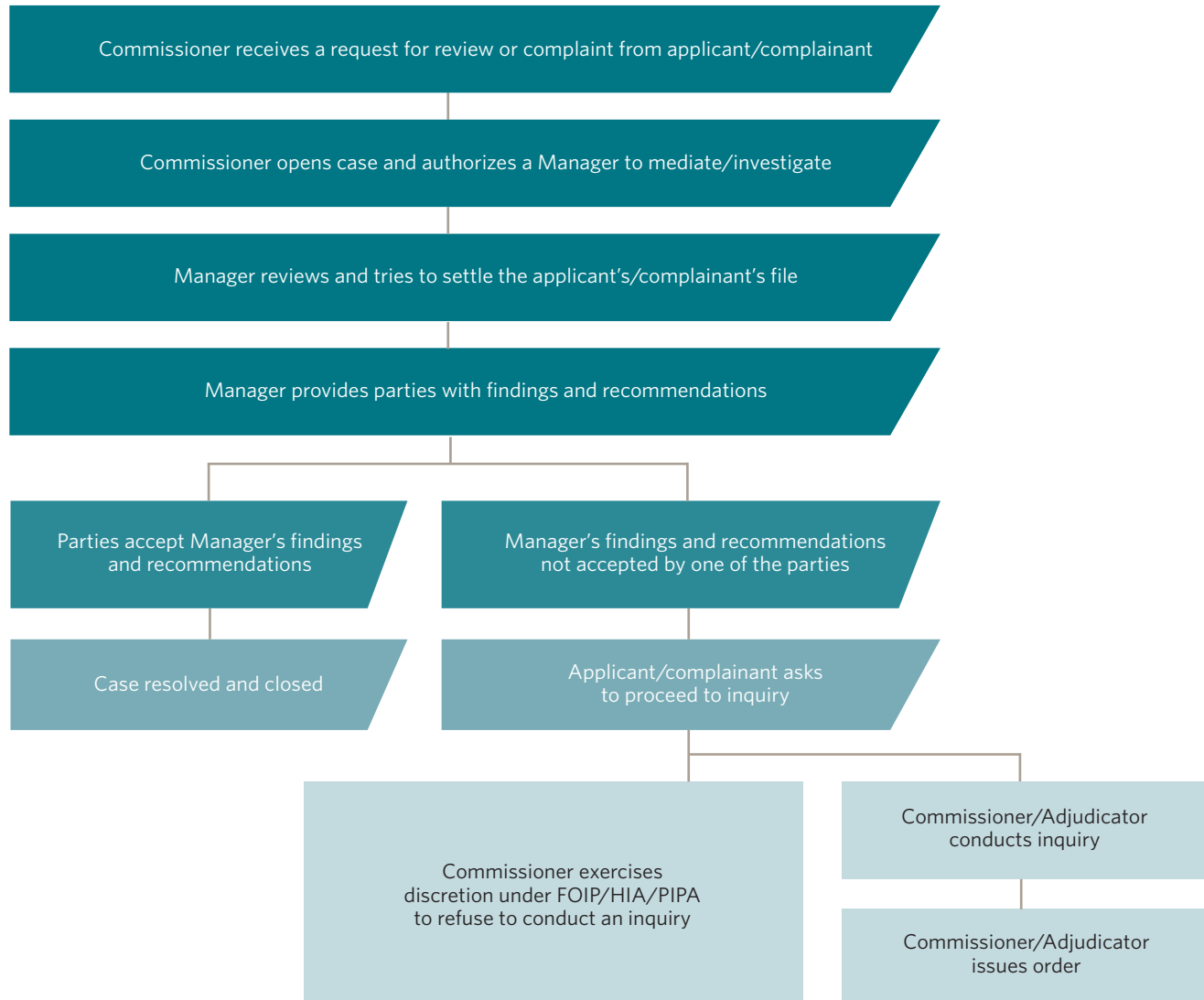
Our work toward supporting our vision includes:

- Advocating for the access and privacy rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner

# ORGANIZATIONAL STRUCTURE



# REQUEST FOR REVIEW and COMPLAINT PROCESS





# OIPC as a PUBLIC BODY

## FOIP REQUESTS TO THE OIPC

As a public body under the FOIP Act, the OIPC receives access requests on occasion. In 2022-23, the OIPC received two general information requests under the FOIP Act. The OIPC responded to both requests within 30 days.

Individuals who disagree with the access request response received from the OIPC can request a review of the OIPC's decision. An External Adjudicator is appointed by order in council to determine whether the OIPC properly responded to the access request, such as properly excluding records subject to the access request.

On October 19, 2022, an External Adjudicator heard a matter and subsequently issued Adjudication Order #14, available on the Commissioner's website at [www.oipc.ab.ca](http://www.oipc.ab.ca). The External Adjudicator decided that the Applicant had abandoned her request for review.

As of March 31, 2023, there were no longer any outstanding requests for review awaiting the appointment of an External Adjudicator.

## OIPC PRIVACY MATTERS

In 2022-23, the OIPC conducted four investigations into internal incidents involving potential privacy breaches.

### Incident 1

The OIPC sent an acknowledgement letter in error to an individual. The letter confirmed that the OIPC had received a self-reported breach. The individual who received the package in error notified the OIPC and returned the letter to the OIPC. The letter did not contain personal information. There was no real risk of significant harm and no notification was required. To prevent recurrence, we reminded staff about the importance of verifying an address supplied by another staff member before sending an acknowledgement letter.

### Incident 2

The OIPC sent a complaint acknowledgement package in error to a public body. The public body was not involved in the complaint. The privacy office of the public body notified the OIPC and returned the package to the OIPC. The package contained the personal information of the complainant and 12 other individuals. The OIPC assessed that there was no real risk of significant harm as the package was received by the privacy office which understood the need to keep personal information confidential, and the public body returned the information to the OIPC. No notification was required. To prevent recurrence, we reminded staff about the importance of a second check on work before sending acknowledgement packages.

### **Incident 3**

The applicant named the respondent as public body A on the request for review form submitted to the OIPC. However, the attachments to the form showed that the review concerned public body B. The OIPC relied on the form and sent the request for review acknowledgement package to public body A. The OIPC contacted public body A and the package was returned. There was no real risk of significant harm, and no notification was required. To prevent recurrence, we informed staff to review materials attached to forms submitted by the public to ensure there are no discrepancies.

### **Incident 4**

An Order was sent to the wrong public body. This was due to an auto-population email error. The Order did not contain personal information. Orders are ultimately published on the OIPC website. There was no real risk of significant harm and no notification was required. To prevent recurrence, we reminded staff to delete the auto population cache to avoid errors.

## **PROACTIVE TRAVEL AND EXPENSES DISCLOSURE**

The OIPC continues to disclose the vehicle, travel and hosting expenses of the Commissioner, and the travel and hosting expenses of the Assistant Commissioners and Directors every second month. The disclosures are available at [www.oipc.ab.ca](http://www.oipc.ab.ca).

## **PUBLIC SECTOR COMPENSATION TRANSPARENCY ACT**

The *Public Sector Compensation Transparency Act* requires public sector bodies, including the OIPC, to publicly disclose compensation and severance provided to an employee if it is more than \$125,000 in a calendar year, as adjusted according to the Act. For the 2021 calendar year, the threshold was adjusted to \$136,805. Other non-monetary employer-paid benefits and pension are also reported.

This disclosure is made annually by June 30 and is available at [www.oipc.ab.ca](http://www.oipc.ab.ca).

## **PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWER PROTECTION) ACT**

There were no disclosures received by the OIPC's designated officer under the *Public Interest Disclosure Act* in 2022-23.

# FINANCIAL OVERVIEW

In 2022-23, the total approved budget for the OIPC was \$7,441,000. The total cost of operating expenses and capital purchases was \$7,410,102. The OIPC returned \$30,898 to the Legislative Assembly.

## TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	\$ 7,441,000	\$ 7,410,102	\$ 30,898
Capital Purchases	-	-	-
<b>TOTAL</b>	<b>\$ 7,441,000</b>	<b>\$ 7,410,102</b>	<b>\$ 30,898</b>

\*Amortization is not included

## TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2022-2023	2021-2022	DIFFERENCE
Operating Expenses*	\$ 7,410,102	\$ 7,015,537	\$ 394,565
Capital Purchases	-	31,876	(31,876)
<b>TOTAL</b>	<b>\$ 7,410,102</b>	<b>\$ 7,047,413</b>	<b>\$ 362,689</b>

Total costs for operating expenses and capital purchases increased by \$362,689 from the previous year.



# TRENDS & ISSUES

# PIPA REVIEW

Section 63 of PIPA requires a special committee of the Legislative Assembly to begin a comprehensive review of the Act every six years after the previous special committee submits its final report.

On May 25, 2022, a government motion was passed by the Legislative Assembly that referred PIPA to the Standing Committee on Alberta's Economic Future to conduct the review, pursuant to section 63 of PIPA. The Committee must report its findings to the Legislative Assembly, including any recommended amendments (section 63(2)). The Committee commenced its review on September 27, 2022.<sup>1</sup>

To begin its work, the Committee invited representatives from the Government of Alberta and the OIPC to provide a technical briefing on the Act. On January 10, 2023, the Commissioner presented to the Committee highlighting PIPA's importance and the Commissioner's powers, as well as identifying global changes in privacy laws that must be considered to ensure PIPA remains relevant. For example, the Commissioner spoke about individual rights in other laws respecting automated decision making. If a decision is made about or for an individual by a piece of software or "bot" using artificial intelligence without human involvement then recourse becomes available to the individual. These automated decision-making rights recognize the harms that can occur to an individual through automated decision-making technology, such as decisions to deny a loan or insurance.

The Commissioner also noted in the presentation to the Committee that a trust deficit has accumulated between customers and businesses with respect to privacy. One example was the PORTpass investigation that is summarized in the Regulation and Enforcement section of this annual report. The Commissioner said that modernizing PIPA would help to rebuild trust.

While further details on possible amendments to PIPA were not provided during the technical briefing, the OIPC shared some topics for consideration with Service Alberta in November 2020 (the Ministry of Technology and Innovation is now responsible for the administration of PIPA). Those recommendations for PIPA included:

- Requiring organizations to have a privacy management program in place.

Also requiring that organizations provide written information about their privacy management program to the Commissioner and to individuals, upon request. The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control. Other aspects that could make up part of the requirement to establish a privacy

---

<sup>1</sup> Section 63(2) of PIPA also requires that the Committee report to the Legislative Assembly within 18 months from the commencement of its work. However, in anticipation of the 2023 provincial election, all Standing Committees were dissolved on May 1, 2023 and the Standing Committee on Alberta's Economic Future ceased to exist until the Legislative Assembly agrees to reestablish Committee membership. As a result, the PIPA review will recommence at a later date.

management program include mandatory Privacy Impact Assessments (PIAs) for projects meeting certain criteria and requiring certain criteria for the use of automated decision-making.

- Exploring data trusts as a potential enabler of responsible innovation.
- At minimum, permitting the use of de-identified personal information without consent for internal research and development purposes; defining “de-identified” to mean removing any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual; and making it an offence to attempt to re-identify individuals using de-identified information.
- Making PIPA apply fully to all non-profit organizations and political parties.
- Including the right to data portability, which is the ability to move personal information among or between different organizations, applications or services.

In addition, the government should explore consulting on the right to erasure and the right to de-indexing.

- Strengthening oversight and offence and penalty provisions.

For example, granting the Commissioner the power to impose administrative monetary penalties for certain violations and increasing offence fines.

Many possible ideas for amendments during the PIPA review reflect significant changes to global and national private sector privacy laws since 2016, when the last PIPA review was undertaken, including, but not limited to:

- The European Union’s *General Data Protection Regulation* (GDPR), which came into force in May 2018. GDPR introduced several enhanced provisions around the themes of consent, accountability and breach reporting, and it introduced significant penalties for non-compliance.
- Quebec’s *Act respecting the protection of personal information in the private sector*, which fully came into force in September 2022. Among the changes, businesses in Quebec must, for example, designate a “person in charge” of privacy compliance and report certain types of security incidents.
- The federal government introducing Bill C-27 in June 2022, which in part comprises the *Consumer Privacy Protection Act* (CPPA). If passed, CPPA would mostly replace the long-standing *Personal Information Protection and Electronic Documents Act*, commonly referred to as PIPEDA. It would introduce privacy requirements similar to those set out in GDPR and Quebec’s new law.
- A Special Committee to Review British Columbia’s PIPA issuing a report in December 2021 resulting in 34 recommendations to modernize the Act.



# PRIVATE SECTOR PRIVACY BREACHES

The OIPC released a report in July 2022 that analyzed nearly 2,000 breaches reported in Alberta over 11 years. The report examined PIPA breaches from 2010-11 to 2020-21.

In May 2010, requirements to report certain breaches to the OIPC and notify affected individuals came into force under PIPA. Alberta became one of the first North American jurisdictions to require organizations to notify individuals affected by breaches, and to report those incidents to a privacy regulator. Under PIPA, it is mandatory for an organization with personal information under its control to notify the Commissioner of a privacy breach where “a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure” (section 34.1).

The Commissioner was also given the power in PIPA to require organizations to notify an affected individual when the Commissioner determines there is a real risk of significant harm to the affected individual resulting from a breach (section 37.1).

Data in the report show that organizations sent millions of notifications to people affected by breaches since the requirements came into force. The leading reason for notification to an affected individual has been unauthorized access to personal information, most often caused by a compromised

electronic information system, such as the installation of malware or ransomware on work computers or within entire networks.

The report offered guidance to help organizations and law firms specializing in privacy law to decide whether there is a real risk of significant harm (RROSH) to an affected individual resulting from a breach. RROSH is the legal threshold under PIPA for reporting breaches. In particular, the executive summary of the report listed criteria used by the Commissioner to decide whether there was RROSH or No RROSH, and why there was a no jurisdiction finding in some cases.

The factors that contributed to RROSH decisions included:

- Deliberate action or malicious intent to cause the breach
- Personal information is not recovered, returned or destroyed securely
- Length of time the personal information is exposed
- Personal information is exposed and there is no auditing or ability to determine whether information was accessed
- No encryption of personal information



The factors that contributed to No RROSH decisions included:

- Accidental or inadvertent cause of the breach
- Personal information is recovered, the organization confirms it has been destroyed securely, or the organization confirms it has not been used, forwarded or retained
- Encryption of the personal information
- Breach is reported to the organization by the unintended recipient(s)
- Unintended recipient of personal information is a known or trusted party

- Fewer personal information data elements are at issue, and the personal information cannot be used to cause significant harm

Based on information submitted by organizations when reporting a breach, the report also analyzed how long it takes organizations to discover breaches, notify individuals and report to the OIPC. It also looked at whether malicious intent or deliberate action was involved in a breach, types of harm, types of personal information and reporting industries, among other data. Hypothetical scenarios in the report also compared “typical” RROSH and No RROSH breaches that occurred in 2010-11 through 2020-21 to show how the nature of breaches have changed over time.

“Organizations face constant challenges in preventing and responding to breaches, and this report shows how dynamic privacy and security management has become. The legal mechanisms have remained the same but the administrative and technical aspects require regular reviews and updates. Digital realities underscore the need for regular privacy and security training for staff in all industries and for diligence in performing security updates to IT infrastructure. Beyond digital privacy and security management, it is also important for organizations to remind staff regularly about not leaving work products in vehicles and to triple check addresses when sending mail or email containing personal information.”

- Former Commissioner Jill Clayton, July 27, 2022



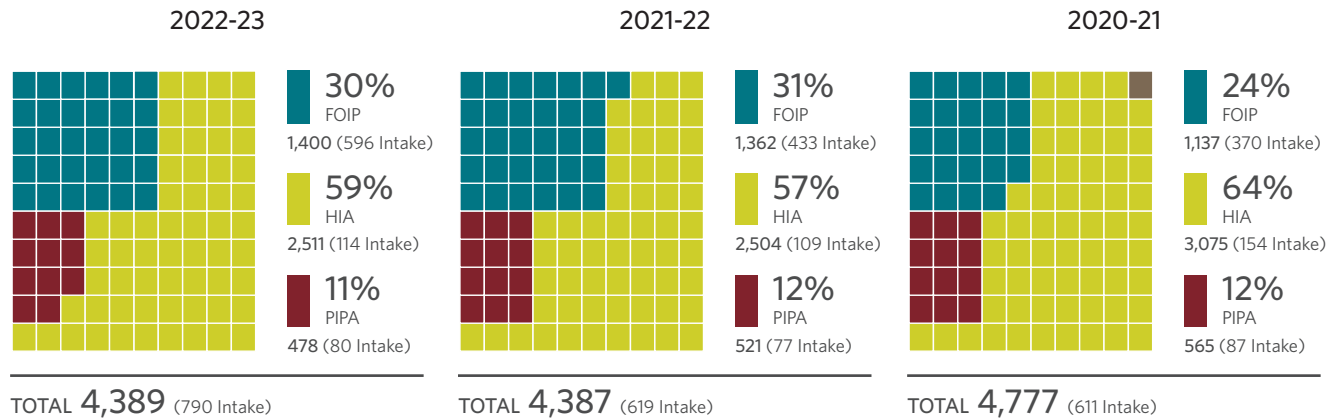




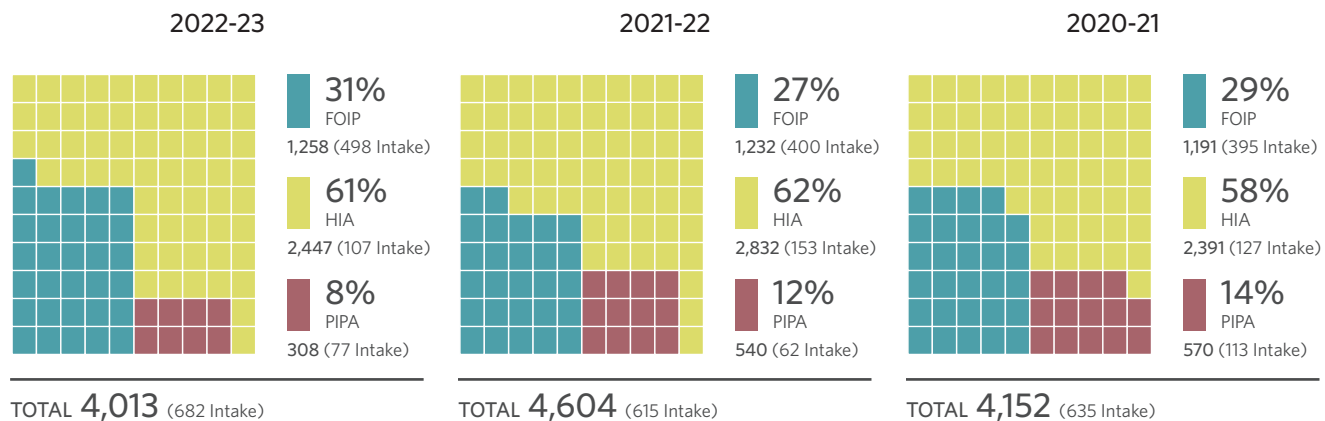
# BY THE NUMBERS

---

## GRAPH A: TOTAL CASES OPENED Three Year Comparison



## GRAPH B: TOTAL CASES CLOSED Three Year Comparison



# TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2022-2023	2021-2022	2020-2021
Advice and Direction	0	0	0
Authorization to Disregard a Request	2	4	4
Complaint	42	38	28
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	1	5	2
Investigation Generated by Commissioner	4	2	4
Notification to OIPC	2	1	7
Offence Investigation	0	0	1
Privacy Impact Assessment	7	10	14
Request Authorization to Collect Indirectly	0	0	0
Request for Information	4	14	9
Request for Review	349	343	283
Request for Review 3rd Party	46	41	40
Request Time Extension	294	398	294
Self-reported Breach	53	73	81
<b>Subtotal</b>	<b>804</b>	<b>929</b>	<b>767</b>
Intake cases	596	433	370
<b>Total</b>	<b>1,400</b>	<b>1,362</b>	<b>1,137</b>

HIA	2022-2023	2021-2022	2020-2021
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	1	0
Complaint	20	48	33
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	1
Investigation Generated by Commissioner	1	6	19
Notification to OIPC	0	0	0
Offence Investigation	5	17	11
Privacy Impact Assessment	1,856	1,730	1,888
Request for Information	16	23	19
Request for Review	24	19	19
Request Time Extension	0	0	1
Self-reported Breach	475	551	930
<b>Subtotal</b>	<b>2,397</b>	<b>2,395</b>	<b>2,921</b>
Intake cases	114	109	154
<b>Total</b>	<b>2,511</b>	<b>2,504</b>	<b>3,075</b>

PIPA	2021-2022	2020-2021	2019-2020
Advice and Direction	0	0	0
Authorization to Disregard a Request	2	0	1
Complaint	41	38	46
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	3	2	7
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	1	11	6
Request for Advanced Ruling	0	0	0
Request for Information	3	7	4
Request for Review	34	52	37
Request Time Extension	1	1	0
Self-reported Breach	313	333	377
<b>Subtotal</b>	<b>398</b>	<b>444</b>	<b>478</b>
Intake cases	80	77	87
<b>Total</b>	<b>478</b>	<b>521</b>	<b>565</b>

## Notes

- 1 See Appendix A for a complete listing of cases opened in 2022-23.
- 2 Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.
- 3 Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

## TABLE 2: CASES CLOSED BY CASE TYPE

FOIP	2022-2023	2021-2022	2020-2021
Advice and Direction	0	1	0
Authorization to Disregard a Request	7	4	1
Complaint	50	36	53
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	3	6	11
Investigation Generated by Commissioner	8	3	6
Notification to OIPC	2	1	7
Offence Investigation	0	1	3
Privacy Impact Assessment	11	13	27
Request Authorization to Collect Indirectly	0	0	0
Request for Information	5	15	14
Request for Review	286	286	241
Request for Review 3rd Party	30	31	28
Request Time Extension	293	375	303
Self-reported Breach	65	60	102
<b>Subtotal</b>	<b>760</b>	<b>832</b>	<b>796</b>
Intake cases	498	400	395
<b>Total</b>	<b>1,258</b>	<b>1,232</b>	<b>1,191</b>

HIA	2022-2023	2021-2022	2020-2021
Advice and Direction	0	0	0
Authorization to Disregard a Request	1	0	0
Complaint	34	56	42
Engage in or Commission a Study	0	0	0
Excuse Fee	0	1	0
Investigation Generated by Commissioner	19	7	2
Notification to OIPC	0	0	0
Offence Investigation	12	13	12
Privacy Impact Assessment	1,557	1,560	1,491
Request for Information	14	18	24
Request for Review	22	24	17
Request Time Extension	0	0	1
Self-reported Breach	681	1,000	675
<b>Subtotal</b>	<b>2,340</b>	<b>2,679</b>	<b>2,264</b>
Intake cases	107	153	127
<b>Total</b>	<b>2,447</b>	<b>2,832</b>	<b>2,391</b>

PIPA	2022-2023	2021-2022	2020-2021
Advice and Direction	0	0	0
Authorization to Disregard a Request	4	1	1
Complaint	55	64	66
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	6	7	7
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	7	6	4
Request for Advanced Ruling	0	0	1
Request for Information	1	7	4
Request for Review	38	52	36
Request Time Extension	1	1	0
Self-reported Breach	119	340	338
<b>Subtotal</b>	<b>231</b>	<b>478</b>	<b>457</b>
Intake cases	77	62	113
<b>Total</b>	<b>308</b>	<b>540</b>	<b>570</b>

### Notes

- 1 See Appendix B for a complete listing of cases closed in 2022-23.
- 2 A listing of all privacy impact assessments accepted in 2022-23 is available at [www.oipc.ab.ca](http://www.oipc.ab.ca).
- 3 Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.
- 4 Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

## TABLE 3: CASES CLOSED BY RESOLUTION METHOD

Under FOIP, HIA and PIPA, only certain case types can proceed to Inquiry if the matters are not resolved at Mediation/Investigation. The statistics below are for those case types that can proceed to Inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Mediation/Investigation	278	47	78	403	78%
Order or Decision	61	6	9	76	15%
Commissioner's decision to refuse to conduct an Inquiry	4	3	3	10	2%
Withdrawn during Inquiry process	15	0	1	16	3%
Discontinued during Inquiry process	11	0	2	13	2%
<b>Total</b>	<b>369</b>	<b>56</b>	<b>93</b>	<b>518</b>	<b>100%</b>

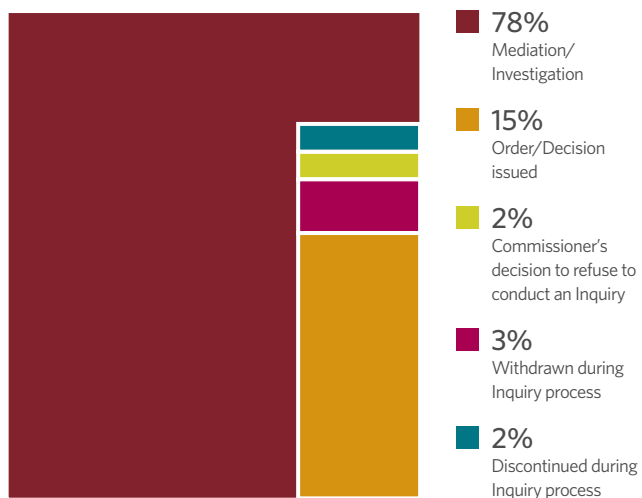
FOIP Orders: 59 (61 cases); HIA Orders: 5 (6 cases); PIPA Orders: 8 (9 cases)

### Notes

- 1 This table includes only the Orders and Decisions issued that concluded/closed the file. See Appendix C for a list of all Orders, Decisions and public Investigation Reports issued in 2022-23. Copies of Orders, Decisions and public Investigation Reports are available at [www.oipc.ab.ca](http://www.oipc.ab.ca).
- 2 Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.
- 3 An Inquiry can be discontinued due to a lack of contact with or participation of the applicant or complainant or if the issues have become moot.



**GRAPH C:  
PERCENTAGE OF CASES CLOSED  
BY RESOLUTION METHOD**



Of the **584** cases that could proceed to Inquiry:  
**3%** were resolved within 90 days  
**6%** were resolved within 180 days  
**91%** were resolved in more than 180 days

**TABLE 4: GENERAL ENQUIRIES**

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	43	16%
Individuals	221	84%
<b>Total</b>	<b>264</b>	<b>100%</b>

HIA	Number	Percentage
Custodians	228	40%
Individuals	343	60%
<b>Total</b>	<b>571</b>	<b>100%</b>

PIPA	Number	Percentage
Organizations	81	16%
Individuals	432	84%
<b>Total</b>	<b>513</b>	<b>100%</b>

NON-JURISDICTIONAL	141
--------------------	-----

EMAILS FOIP/HIA/PIPA	418
----------------------	-----

<b>Total</b>	<b>1,907</b>
--------------	--------------

**TABLE 5: TOTAL CASES CARRIED OVER INTO FISCAL YEAR 2023-24  
BY TEAM & CASE TYPE**

Mediation and Investigation (MI)				
Statistics are from the period of April 1, 2022 to March 31, 2023				
Cases Types (FOIP   HIA   PIPA)	Opened prior to 2022-23 & remains open	Opened in 2022-23	Closed in 2022-23	Total # cases carried over 2023-24
Advice and Direction				
Authorization to Disregard a Request				
Authorization to Indirectly Collect				
Complaint	129	88	102	115
Disclosure to Commissioner				
Engage in or Commission a study				
Excuse Fee	5	1	3	3
Investigation Generated by Commissioner	4	4	1	7
Notification to OIPC				
Offence Investigation				
Privacy Impact Assessment (PIA)	1	53		54
Request for Information (RFI)	2	3	4	1
Request for Review (RFR)	514	340	250	604
Request for Review 3rd Party	45	43	23	65
Request for Time Extension (RFTE)		295	294	1
Self-reported Breach				
<b>TOTAL</b>	<b>700</b>	<b>827</b>	<b>677</b>	<b>850</b>

**Note:** The bulk of the work of the MI Team is to informally resolve complaints and RFRs received by the public, which are related to the exercise of their rights under the FOIP Act, HIA and PIPA. RFRs (the majority of which are reviews of decisions of heads of public bodies concerning access to information requests) make up approximately 76% of the MI Team's case files. While this Team closed a significant number of files in 2022-23, 699 cases were carried over into this fiscal year and 796 remain open at the end. In 2022-23, there were 7.2 Senior Information and Privacy Managers (SIPMs) responsible to carry out this work. Each SIPM has 35 files that they actively work on with the remaining assigned files in the queue. During this fiscal year, each SIPM had a file load of approximately 80 cases and completes an average of six to eight files per month. As of March 31, 2023, each had a caseload of approximately 111. Files move up in the queue in the order they are received. RFTEs are requested by public bodies for more time to respond to an access request. Given that there are tight timelines associated with RFTEs, work on these cases is prioritized which is why there is little to no carry over from year to year. In 2022-23 there was one staff assigned for this work.

## Compliance Support and Investigations (CSI)

Statistics are from the period of April 1, 2022 to March 31, 2023

Cases Types (FOIP   HIA   PIPA)	Opened prior to 2022-23 & remains open	Opened in 2022-23	Closed in 2022-23	Total # cases carried over 2023-24
Advice and Direction				
Authorization to Disregard a Request				
Authorization to Indirectly Collect				
Complaint	16		8	8
Disclosure to Commissioner				
Engage in or Commission a study				
Excuse Fee				
Investigation Generated by Commissioner	10		22	-12
Notification to OIPC		2	2	
Offence Investigation	17	5	12	10
Privacy Impact Assessment	1599	1802	1569	1832
Request for Information	18	17	13	22
Request for Review				
Request for Review 3 <sup>rd</sup> Party				
Request for Time Extension				
Self-reported Breach (SRB)	605	840	865	580
<b>TOTAL</b>	<b>2,265</b>	<b>2,666</b>	<b>2,491</b>	<b>2,440</b>

**Note:** The bulk of the work for the CSI Team is reviewing PIAs, SRBs, privacy education (stakeholder engagement), and conducting investigations generated by the Commissioner, including offence investigations. There are seven SIPMs assigned to review PIAs. There were nearly as many PIAs closed as opened in 2022-23. However, there was a large carry over of files from the previous fiscal year. Some of this has to do with files being put in abeyance pending investigation. In 2022-23, there were more than 500 files in abeyance. SRBs are spread among the SIPMs with two focused on this work. The majority of the carry-over files, which are in the queue, involve SRB reports where notice of the breach was given to the affected individuals by the organization. Three SIPMs carry out offence investigation work with defined limitation periods. As such, these files are actively worked on from assignment.

<b>Special Investigations</b> <i>Statistics are from the period of April 1, 2022 to March 31, 2023</i>				
Cases Types (FOIP   HIA   PIPA)	Opened prior to 2022-23 & remains open	Opened in 2022-23	Closed in 2022-23	Total # cases carried over 2023-24
Advice and Direction				
Authorization to Disregard a Request				
Authorization to Indirectly Collect				
Complaint	9			9
Disclosure to Commissioner				
Engage in or Commission a study				
Excuse Fee				
Investigation Generated by Commissioner	21	4	5	20
Notification to OIPC				
Offence Investigation	1			1
Privacy Impact Assessment				
Request for Information (RFI)	1			1
Request for Review				
Request for Review 3 <sup>rd</sup> Party				
Request for Time Extension				
Self-reported Breach	1			1
<b>TOTAL</b>	<b>33</b>	<b>4</b>	<b>5</b>	<b>32</b>

**Note:** In 2022-23, there was one person responsible for special investigations in the OIPC. The number of files closed in 2022-23 exceeded (by one) the number of files opened during the fiscal year. However, there were 21 investigation files carried over from prior fiscal years, leaving 20 cases carried over into 2023-24. The remaining files, 12, consist of nine complaint files that were held in abeyance pending the outcome of one investigation which was not complete in 2022-23, one RFI, one offence investigation and one self-reported breach case file.

<div> Adjudication Statistics are from the period of April 1, 2022 to March 31, 2023 </div>				
Cases Types (FOIP   HIA   PIPA)	Opened prior to 2022-23 & remains open	Opened in 2022-23	Closed in 2022-23	Total # cases carried over 2023-24
Complaint	36	7	20	23
Excuse Fee				0
Request for Review	180	51	80	151
Request for Review 3 <sup>rd</sup> Party	33	10	5	38
<b>TOTAL</b>	<b>249</b>	<b>68</b>	<b>105</b>	<b>212</b>

**Note:** The work of the Adjudication Team is to issue Orders. At the end of fiscal year 2022-23, there were four adjudicators. Each is assigned approximately 50 files (though sometimes multiple files are combined in a single inquiry). Of these, at a given point in time, Notices of Inquiry have been issued for approximately 15 of the 50, and submissions have been received and adjudicators are actively writing the orders for some proportion of these files. Files not being actively worked on are in the queue waiting for Notices of Inquiry to be issued. At the end of 2022-23 there were approximately 152 files in the queue.



# REGULATION & ENFORCEMENT

---

# INVESTIGATION REPORTS

## TIM HORTONS APP FOUND TO COLLECT VAST AMOUNTS OF SENSITIVE LOCATION DATA

---

The OIPC opened a joint investigation along with the Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec and the Office of the Information and Privacy Commissioner for British Columbia into Tim Hortons (Restaurant Brands International Inc.) and its mobile app after numerous media reports raised questions and concerns among privacy authorities. The investigation reviewed whether Tim Hortons was obtaining consent to collect, use and disclose geolocation and associated data, including for the creation of detailed user profiles. The Commissioners also reviewed whether Tim Hortons' privacy practices were reasonable in the circumstances.

The investigation concluded that Tim Hortons' continual and vast collection of location information was not proportional to the benefits Tim Hortons may have hoped to gain from better targeted promotion of its coffee and other products.

The Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, and Office of the Information and Privacy Commissioner of Alberta issued their Report of Findings on June 1, 2022.

The Tim Hortons app asked for permission to access the mobile device's geolocation functions, but misled many users to believe information would only be accessed when the app was in use. In reality, the app tracked users as long as the device was on, continually collecting their location data.

The app also used location data to infer where users lived, where they worked, and whether they were travelling. It generated an "event" every time users entered or left a Tim Hortons competitor, a major sports venue, or their home or workplace.

The investigation uncovered that Tim Hortons continued to collect vast amounts of location data for a year after shelving plans to use it for targeted advertising, even though it had no legitimate need to do so.

Tim Hortons said that it only used aggregated location data in a limited way, to analyze user trends – for example, whether users switched to other coffee chains, and how users' movements changed as the pandemic took hold.

While Tim Hortons stopped continually tracking users' locations in 2020, after the investigation was launched, that decision did not eliminate the risk of surveillance. The investigation found that Tim Hortons' contract with an American third-party location services supplier contained language so vague and permissive that it would have allowed that supplier to sell "de-identified" location data for its own purposes.

There is a real risk that de-identified geolocation data could be re-identified. A research report by the Office of the Privacy Commissioner of Canada underscored how easily people can be identified by their movements.



Location data is highly sensitive because it can be used to infer where people live and work and reveal trips to medical clinics. It can be used to make deductions about religious beliefs, sexual preferences, social political affiliations and more.

Organizations must implement robust contractual safeguards to limit service providers' use and disclosure of their app users' information, including in de-identified form. Failure to do so could put those users at risk of having their data used by data aggregators in ways they never envisioned, including for detailed profiling.

The investigation also revealed that Tim Hortons lacked a robust privacy management program for the app, which would have allowed the company to identify and address many of the privacy contraventions the investigation found.

The four privacy authorities recommended that Tim Hortons:

- Delete any remaining location data and direct third-party service providers to do the same;

- Establish and maintain a privacy management program that includes privacy impact assessments for the app and any other apps it launches; creates a process to ensure information collection is necessary and proportional to the privacy impacts identified; ensures that privacy communications are consistent with and adequately explain app-related practices; and
- Report back with the details of measures it has taken to comply with the recommendations.

Tim Hortons agreed to implement the recommendations.

*Investigation Report P2022-IR-01: Joint investigation by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia into The TDL Group Corp. (the operator and franchisor of Tim Hortons in Canada)*

"This investigation is yet another example where an organization has not effectively notified customers about its practices. Tim Hortons' customers did not have adequate information to consent to the location tracking that was actually occurring. When people download and use these types of apps, it's important that they know in advance what will happen to their personal information and that organizations follow through with their commitments."

- Former Commissioner Jill Clayton, June 1, 2022

## PORTpass VACCINE VERIFICATION APP FAILED TO DEMONSTRATE SAFEGUARDS

The investigation into PORTpass' protection of personal information under PIPA was opened after an individual made a complaint to the OIPC.

PORTpass claimed, via its website and privacy policy, to protect personal information by implementing encryption and blockchain technology. Such claims were compelling, particularly at a time when organizations and individuals wanted an immediate digital solution for proving vaccination. The OIPC was not, however, able to substantiate any of PORTpass' claims about how it protected personal information.

During the investigation, PORTpass failed to demonstrate that it implemented any technical and administrative safeguards to protect personal information. The investigation found that PORTpass did not protect personal information in its custody or under its control in contravention of section 34 of PIPA.

Additional assurances from PORTpass that steps had been taken to securely destroy personal information were also unreliable. There were no responses to follow-up questions about the destruction of personal information. It was also unclear whether PORTpass took other corrective measures.

PORTpass dissolved its operations during the investigation and, as there was no longer an "organization" as defined in PIPA to whom the Commissioner could make recommendations or issue an order compelling compliance, the investigation did not result in any recommendations or an order.

*Investigation Report P2022-IR-02 Investigation into PORTpass' protection of personal information under the Personal Information Protection Act*

"Overall, this investigation serves as a reminder to customers and business clients alike. Everyone must exercise caution and, where possible, verify that organizations deliver on privacy and security promises prior to consenting to the collection, use or disclosure of personal information. When startups can disappear as suddenly as they appear, building trust with organizations can be challenging. Taking a few minutes to research an organization before deciding whether to accept the terms and conditions can go a long way.

Likewise, organizations contracting or subcontracting services ought to assess the privacy and security controls of prospective contractors – for example, by way of a privacy impact assessment – to understand and mitigate potential risks to customer privacy and organizational reputation."

*- Former Commissioner Jill Clayton, July 28, 2022*

# MEDIATION and INVESTIGATION

The Mediation and Investigation (MI) team, consisting of a Director and seven Senior Information and Privacy Managers (SIPMs), is responsible for resolving or settling privacy complaints or requests for review of responses to access requests brought by the public under all three of Alberta's privacy and information laws.

In addition, the MI team conducts investigations initiated by the Commissioner; reviews and makes recommendations to the Assistant Commissioner concerning time extension requests; reviews and comments on compliance with these laws by public bodies, custodians and other organizations; and educates and informs the public, public bodies, custodians and organizations about the Acts.

The informal case resolution function performed by this team is the first phase of the review process for the OIPC and the majority of disputes are resolved at this stage.

## **TRENDS AND CHALLENGES**

Many of the trends identified in last year's Annual Report continued to figure prominently in the reviews and complaints investigated in 2022-2023.

### **Pandemic-Related Issues**

The OIPC continued to see a notable number of requests for reviews and complaints related to COVID-19 matters in 2022-23.

Access topics included individual vaccination records, the handling of COVID-19 policy exemptions or accommodation requests,

PPE procurement, initiative costs, statistics and research, vaccine efficacy, mask mandates and pandemic planning.

Complaints were received about the collection of information about vaccine status or COVID-19 tests required for work, to attend a hearing or to maintain college housing. Individuals also complained about alleged unauthorized disclosures of personal information when handling COVID-19 accommodation requests.

### **HIA Challenges: Identifying Custodians Responsible for Compliance**

One challenge in investigating complaints or requests for review under the *Health Information Act* (HIA) has been identifying the proper respondent custodian.

For example, HIA allows applicants to make access requests for their own health information to custodians (as defined in section I(1)(f) of HIA) and custodians are responsible for responding to an access request in the manner set out in HIA. However, applicants often make access requests for their health information to a health clinic, which is not a custodian. Also, the health records sought may have been created by more than one custodian (or affiliate of a custodian). In such circumstances, it can be difficult to identify the custodian(s) responsible for HIA compliance.

Similarly, in complaints about the handling of an individual's health information under HIA, it can be difficult to determine whether a health care provider was acting as a custodian or as an affiliate to another custodian or which custodian is responsible for the activities of a particular affiliate. Affiliates, including

information managers, also have duties and obligations under HIA. At the same time, the custodians whose patients' health information was affected by an incident are ultimately responsible for any contraventions of HIA attributed to their affiliates.

The reality of current health care sector business models (and the complex relationships between health service clinics, health care providers and health information technology service providers) do not easily align with HIA, which makes custodians ultimately responsible for HIA compliance.

## **PIPA**

Under PIPA, Alberta's private sector privacy legislation, individuals have the right to request access to their own information held by organizations, ask how their own personal information has been used or disclosed, and request corrections to their own personal information. However, individuals and organizations commonly misunderstand the scope of an individual's access rights under PIPA. Personal information is limited to information "about" an individual and has a personal dimension. Individuals will often ask for information relating to the organization's business or for information related to a property, rather than (or in addition to) their own information. At the same time, many small to medium organizations remain unaware of individuals' access rights under PIPA, resulting in non-responses to access requests.

The MI team continues to provide education and guidance to individuals and organizations about their respective rights and obligations under PIPA.

## **Complaints about Political Parties**

The OIPC continued to receive privacy complaints about the handling of individuals' personal information by Alberta political parties. In these cases, the OIPC had to inform individuals that the Office does not have jurisdiction to review their complaints under PIPA (section 4(3)(m)).

In 2018, Canada's federal, provincial and territorial Information and Privacy Commissioners and Ombudspersons passed a joint resolution, urging their respective governments to pass legislation requiring political parties to comply with globally recognized privacy principles.

In 2020, (now former) Alberta Commissioner Clayton proposed various legislative amendments to PIPA, including that PIPA apply fully to political parties.

## **Over-collection of Tenants' Personal Information**

Once again, the Office investigated complaints relating to the over-collection of tenants' personal information by landlords. Examples of excessive collection included landlords requiring a copy of a tenant's will (or name of their executor), their health care numbers and, in one case, information about when tenants were away or having overnight guests.

To deal with this issue, the OIPC is preparing updated guidance along with several partners.

# REQUESTS for TIME EXTENSIONS by PUBLIC BODIES

A public body must make every reasonable effort to respond to an access request under FOIP within 30 calendar days (section 11). A public body may extend the time limit for responding by up to 30 days on its own authority in certain circumstances (section 14(1)).

An extension period longer than an additional 30 days requires the Commissioner's approval (sections 14(1) and (2)). A failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under section 14, is treated as a decision to refuse access (section 11(2)).

In 2022-23, there were 294 requests for time extensions submitted by public bodies to the OIPC, representing a 26% decrease compared with 2021-22 (398).

- 65% were made by Provincial Government
- 22% were made by Municipalities
- 2% were made by Law Enforcement
- 4% were made by Regional Health Authorities

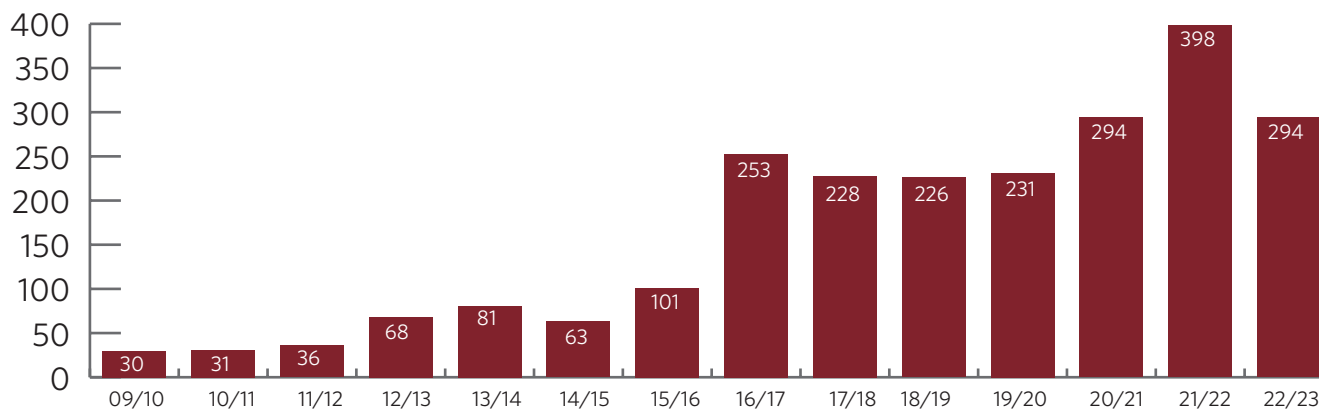
- 4% were made by School Districts, Post Secondary Institutions
- 3% were made by a Board, Commission, Other Public Bodies

Of the 294 requests received by the OIPC:

- 70% were the first request made by a public body
- 23% were second requests made by a public body
- 6% were third requests made by a public body
- 1% were four or more requests made by a public body

In total, 44% of the time extension requests were granted to the public body. The remaining 56% were partially granted or denied, or the public body withdrew its request.

While it is positive that requests for time extensions decreased in 2022-23, other than in 2021-22, a pandemic year, the trend has been a steady increase in the number of requests. Below is a graph demonstrating the increase from 2009-10 to 2022-23.



# PRIVACY IMPACT ASSESSMENT REVIEWS

A privacy impact assessment (PIA) helps to identify and address potential privacy risks that may occur in a project. A PIA is used for information systems, administrative practices and policy proposals that relate to the collection, use or disclosure of individually identifying personal or health information.

There were 1864 PIAs accepted by the OIPC in 2022-23, representing a 40% increase compared with 2021-22 (1,332). The OIPC's current practice is to either 'accept' or 'not accept' a PIA. Acceptance reflects the opinion of the person reviewing the PIA, usually a senior information and privacy manager, that the custodian, public body or organization has considered the requirements of the applicable privacy law and has made reasonable efforts to protect privacy.

Health custodians under HIA submit nearly all PIAs. Only HIA, under section 64, requires the submission of PIAs to the OIPC for review and comment. Similar PIA requirements do not exist under the FOIP Act and PIPA. As a result, public bodies and private sector organizations submit few PIAs to the OIPC.

## HIA

The complexity of information systems implemented in the health sector has increased significantly since 2001 when HIA came into force and the OIPC has experienced this evolution through the review of PIAs submitted to the office by health custodians. The need to deliver healthcare remotely during the pandemic drove an increase in the use of virtual care platforms to deliver these services, which use has continued post-pandemic.

What once were single purpose information systems have morphed into multipurpose applications that are used to not only manage and store records, but to facilitate health care delivery. Many are now cloud-based and require numerous third party private sector vendors to deliver the services and function effectively. These changes have resulted in a significant increase

in PIAs being submitted to the OIPC for review and comment that are cross-sectoral and highly complex.

Despite these drastic digital changes in healthcare delivery, a PIA remains the best way for health custodians to identify and address risks to the privacy of Albertans' health information before implementing a new system.

Two notable PIAs that the OIPC accepted under HIA are summarized below:

- A PIA was submitted by Alberta Health (AH) regarding a secure portal for the administration of Alberta Aids to Daily Living (AADL) benefits for prosthetic, orthotic and footwear



aids by Alberta Blue Cross (ABC) on behalf of AH. The ABC portal is used for requesting and adjudicating benefits, processing claims/billing and determining cost-share. Most AADL benefits include a cost-share where the client pays 25% toward the cost of the benefit up to a household maximum of \$500 per benefit year.

- A PIA was submitted by Alberta Health Services (AHS) on its implementation of a Bring Your Own Device (BYOD) program. The BYOD program authorizes employees of AHS to use their personal mobile devices for business purposes after those devices meet specific security requirements as set out by AHS. Implementing a BYOD program within an organization of AHS size (over 100,000 employees) is particularly complex, because of the sheer number of dissimilar employee-owned devices that need to be managed by AHS. The solution used in the BYOD program combines device identity and application delivery, provides self-serve capability to users, enables single sign-on to applications and continuous monitoring capabilities to ensure devices enrolled in the BYOD program continuously meet the security requirements set out by AHS. Devices enrolled in the program include iOS/iPadOS devices (iPhone, iPad, and iPod Touch, Apple Mac), Android devices and Windows 10 devices.

## FOIP

The submission of a PIA by public bodies to the OIPC under the FOIP Act remains voluntary. However, there was one notable PIA submitted under the FOIP Act, which was accepted by the OIPC in 2022-23:

- The Edmonton Police Service (EPS) submitted a PIA on its implementation of facial recognition technology to assist in the identification of perpetrators in criminal investigations. EPS' initiative connects to the Calgary Police Service (CPS) network and enables both police services to share mugshot images, which are collected pursuant to the federal *Identification of Criminals Act*. The connectivity to the CPS network increases the availability of mugshot images to both police services to over 900,000.



# PRIVACY BREACHES

The OIPC received 841 breach reports in 2022-23 under all three laws, representing a 13% decrease compared with 2021-22 (957).

HIA and PIPA require health custodians and private sector organizations, respectively, to report certain privacy breaches to the OIPC. Public bodies may report breaches voluntarily under the FOIP Act.

The OIPC closed 865 self-reported breach files in 2022-23 under all three laws, representing a 47% decrease compared with 2021-22 (1,400).

Certain breaches are prioritized for review, including files where affected individuals have not yet been notified or when a significant number of Albertans have been affected.

## PIPA

It is mandatory for an organization with personal information under its control to notify the Commissioner, without unreasonable delay, of a privacy breach where “a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure” (section 34.1). Section 37.1 of PIPA provides authority for the Commissioner to require an organization to notify individuals of a loss or unauthorized access or disclosure of personal information.

There were 313 breaches reported in 2022-23, an 8% decrease compared with 2021-22 (340).

The OIPC issued 111 breach decisions in 2022-23, representing a 67% decrease from 2021-22 (338). The following decisions were made in 2022-23:

- 90 were found to have a real risk of significant harm
- 18 were found to have no real risk of significant harm
- 3 where PIPA did not apply (that is, the Commissioner did not have jurisdiction to make a decision)

There were several notable breach decisions in 2022-23:

- The organization was subject to a ransomware attack that potentially affected the personal information of 115,175 individuals in Alberta. This incident was notable due to the large number of individuals affected and the organization's national presence. There was also a notable delay between the discovery of the incident and notification of affected individuals. The OIPC issued a decision under section 37.1 requiring the organization to notify affected individuals within 10 days of the decision.

Related to this incident, an affiliate to the organization also reported a breach. The affiliate was affected by the same ransomware incident. However, different individuals and personal information were affected.

*P2023-ND-007, Sobeys Capital Incorporated*  
*P2023-ND-008, Managed Health Care Services Inc.*

- The organization was subject to a ransomware attack affecting the personal information of 473 individuals who were current and former employees of the organization. The organization is a service provider to another organization, and the other organization was also affected by the ransomware incident. Both organizations only notified current employees, however, and the OIPC required the organizations to notify all affected former employees within 10 days of the decisions.

*P2022-ND-060, Universe Machine Corporation*  
*P2022-ND-061, Universe Machine Corporation on behalf of Saturn Machine Works Ltd.*

## HIA

It is mandatory for a custodian having individually identifying health information in its custody or control to notify the Commissioner of a privacy breach if the custodian determines “there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure” (section 60.1(2)). In addition to notifying the Commissioner of the privacy breach, the custodian is also required by section 60.1(2) of HIA to notify the Minister of Health and the individuals affected by the privacy breach.

There were 475 breaches reported by custodians to the OIPC in 2022-23, representing a 15% decrease compared with 2021-22 (551).

Continuing challenges the OIPC sees in reviewing HIA breach reports is that many custodians believe that verbal notification to affected individuals meets the requirements. However, HIA requires that affected individuals be notified about the breach of their health information in writing. Another theme from previous years is human error breaches in pharmacies where prescribed medication is given to the wrong patients. Finally, snooping into health information without a valid business purpose continues to be a common issue in breach reports, despite the training custodians provide to their employees.

## FOIP

There were 53 breaches reported voluntarily by public bodies in 2022-23, representing a 32% decrease compared with 2021-22 (73).

The FOIP Act is Alberta's only privacy law that does not require regulated entities to report privacy breaches to the Commissioner or to notify affected individuals. Modernized public sector privacy laws include mandatory breach notification for public bodies.

## OFFENCE INVESTIGATIONS UNDER HIA

There was one conviction in 2022-23 for knowingly disclosing health information in contravention of HIA. It is an offence under HIA to knowingly disclose health information in contravention of the Act (section 107(2)(a)).

On August 12, 2019, an employee at the Lamont Health Care Centre inappropriately took photos and videos of residents using her personal devices. The employee applied filters to the faces of the individuals in the photos and videos, added derogatory comments, and then shared the photos and videos with colleagues and friends through social media. The Commissioner initiated an offence investigation into the matter. Upon completing the investigation, the Commissioner referred the case to the Crown for pre-charge screening. The individual was charged, received a conditional discharge and was placed on probation with conditions for the next 12 months, including the requirement to advise any potential employer about the conviction if the prospective employment would involve accessing health information. The individual was also sentenced to 30 hours of community service.

There have been 22 convictions for offences under HIA as of March 31, 2023.

# SUMMARY of SIGNIFICANT DECISIONS

## **Alberta Health Directed to Respond to Access Request after Deciding the Request was Unclear**

The applicant made an access request to Alberta Health for:

All emails received by [names of individuals] from  
Tyler Shandro

Eliminate dup-recs, drafts, dup-emails, litigation privilege,  
third party business and third party personal [information]

From June 1, 2019 to November 8, 2020

Alberta Health informed the applicant that his access request was unclear. The applicant explained that he was looking for emails located in Microsoft Outlook.

Alberta Health informed the applicant that the added clarification that responsive records would be located in Microsoft Outlook was insufficient. Alberta Health required the applicant to provide the topic of records that would be responsive.

The applicant agreed to the topic suggested by Alberta Health; however, Alberta Health determined that the access request was still too vague to meet the requirements of section 7(2) of the FOIP Act, which deals with how an applicant makes a request. Alberta Health subsequently closed the file without responding to the applicant.

The applicant sought review by the OIPC.

At inquiry, the Adjudicator determined that the access request was clear and directed Alberta Health to search for responsive email records, and to include Microsoft Outlook in its search. In the event that Alberta Health determined that it had destroyed responsive records, the Adjudicator ordered it to determine whether any such records could reasonably be restored or recovered.

*Alberta Health, Order F2022-25*

## **City of Calgary Properly Disclosed an Applicant/Complainant's Personal Information to Search for Responsive Records**

An individual made a complaint to the OIPC regarding the City of Calgary. The complainant, who is an emergency medical technician (EMT) with Alberta Health Services (AHS), was concerned that employees of the City of Calgary's 911 call centre had accessed her schedule information for their own purposes, without authority under the FOIP Act.

In order to obtain records to substantiate this concern, the complainant made an access request to the City of Calgary for emails and messages sent by particular employees about her. The City of Calgary asked each of these employees to search through their emails and messages for the complainant's personal information.

The complainant raised concerns that her identity as an applicant under the FOIP Act was inappropriately disclosed to the employees who were asked to search through their emails and messages for her personal information. With respect to this issue, the City of Calgary's response and the Adjudicator's finding were addressed in paras. 71 to 74 in the order as follows:

[para 71] The [City of Calgary] argues that when a request includes emails of named employees, it is reasonable to have those employees conduct a search of their email accounts, including any emails that may have been printed and filed in hardcopy format.

[para 72] I agree with the [City of Calgary]. There are practical reasons for having an employee identified in an access request search their own files, whether it be an email account, a network drive assigned to them, or their own hardcopy records. Even if someone in [one of the employee's] position could search the email accounts of all 15 employees, [the employee] would not be aware of any emails that may have been printed and maintained

in hardcopy format, if the electronic email no longer existed at the time of the search. [The employee] would also not have known whether any of the 15 employees was likely to have saved any emails in another location (e.g. a network drive) before deleting them from their email account. Having the named employees conduct their own search ensures that the search is sufficiently comprehensive to fulfill the [City of Calgary's] obligations under section 10 of the Act (duty to assist applicants).

[para 73] I find that the [City of Calgary] did not use the Complainant's personal information beyond what was necessary when the 15 employees identified in the Complainant's access request were instructed to conduct a search for responsive records, and that accordingly it complied with section 39(4) of the Act.

[para 74] To the extent that the Complainant was led to believe that the employees identified in her request would not be involved in the search for responsive records, this does not negate the [City of Calgary's] authority to use her personal information to process her request as it did here. That said, the [City of Calgary] should take care to be clear with applicants on this point should a similar situation arise in the future.

The Adjudicator found that the City of Calgary had authority to use and/or disclose the complainant's personal information as it did. The Adjudicator also found that the City of Calgary made reasonable security arrangements to protect the Complainant's personal information as required by section 38 of the FOIP Act.

*City of Calgary, Order F2022-45*

### **Decision on Request regarding Emergency Response Records**

The applicant made an access request to Alberta Health Services (AHS) for a 911 call, and all audio, video and handwritten records from the initial 911 call to patient handover at the Misericordia hospital, for a specified date.

AHS provided the applicant with a recording of the 911 call and other records it located. AHS informed the applicant that although ambulances are equipped with cameras in the patient compartment, there was no functionality to record audio or video. The applicant replied, questioning AHS' response regarding the camera functionality, and asking for a written statement from the ambulance driver as to what the driver observed in the patient compartment.

AHS replied that it had received all records that responded to her access request. The applicant requested a review and subsequently an inquiry into AHS' response.

The Adjudicator found that AHS had conducted an adequate search for the 911 call and for any video-audio from the ambulance patient compartment, but had failed to conduct an adequate search for handwritten records. In making this finding, the Adjudicator considered whether the services provided by paramedics to patients in an ambulance compartment are excluded from the definition of "health services" in HIA pursuant to section 3.1(f) of the *Health Information Regulation*. The Adjudicator concluded that the services provided by paramedics to patients in an ambulance compartment are not "emergency response dispatch services" as defined in the *Health Information Regulation* and therefore are not excluded from the definition of "health services" under the *Health Information Act*. The Adjudicator ordered AHS to conduct a further search for any responsive handwritten records.

The Adjudicator further concluded that a custodian under HIA does not have a duty to create a record for an applicant under section 10(b) where there is no information in electronic form to create such a record.

*Alberta Health Services, Order F2023-10/H2023-02*



# JUDICIAL REVIEWS and OTHER COURT DECISIONS

## JUDICIAL REVIEWS

### **ABC Benefits Corporation v Alberta (Information and Privacy Commissioner), 2022 ABQB 276**

On March 28, 2011, the applicant requested a copy of the contract between Alberta Health and ABC Benefits Corporation, operating as Alberta Blue Cross (ABC). The applicant also requested how much ABC was paid to administer these plans. ABC was an affected third party. The contract, including schedules and amendments, was provided to the applicant with redactions under section 16 (information harmful to business interests of third party) and section 25 (information harmful to interests of a public body).

The applicant requested a review of the redactions. In Order F2013-47, Alberta Health was ordered to disclose the entire agreement. On judicial review of Order F2013-47, (ABC Benefits Corporation v Alberta (Information and Privacy Commissioner), 2015 ABQB 662), the matter was remitted to the OIPC for determination on sections 16(1)(b) and (c) of the FOIP Act.

Upon receipt of the judicial review decision and the OIPC's Notice of Reconsideration, Alberta Health undertook a further review of the records. Alberta Health concluded that the initial severing had not considered all relevant factors and that some records that had initially been withheld under section 16(1) should have been disclosed. As an affected third party, ABC again objected to Alberta Health's proposed disclosure. In reconsideration Order F2019-R-01, the Adjudicator ordered disclosure of the entire agreement to the applicant.

ABC requested a second judicial review, this time of Order F2019-R-01. The court held that the findings under sections 16(1)(b) and (c) of the FOIP Act were unreasonable and remitted the matter to the OIPC for reconsideration.

### **Governors of the University of Alberta v Alberta (Information and Privacy Commissioner), 2022 ABQB 316**

An applicant requested information held by the University of Alberta and also complained that her personal information had been collected, used, and disclosed in contravention of the FOIP Act. The matters were joined into one inquiry. Order F2021-12 dealt with the University's response to the access request.

Among the findings, the Adjudicator ordered the University of Alberta to disclose further information to the applicant and to reconsider whether to disclose information under other provisions of the FOIP Act. The Adjudicator also ordered the University of Alberta to consider whether any mandatory exceptions applied to information found to be improperly withheld on the basis of solicitor-client privilege.

On judicial review, the court quashed the Adjudicator's findings on section 17 (disclosure harmful to personal privacy), section 18 (disclosure harmful to individual or public safety) and section 27 (solicitor-client privilege). The matter was remitted to the OIPC.

### **Edmonton Police Service v Alberta (Information and Privacy Commissioner), 2022 ABCA 397**

In Order F2020-17, the applicant, a retired police officer, had requested access to documents provided to the Edmonton Police Service (EPS) by the RCMP in relation to personal safety concerns regarding an incident at his home. The Adjudicator held that section 21(1)(b) (disclosure harmful to intergovernmental relations) did not apply, relying on previous OIPC orders and the Supreme Court of Canada's decision in *Societe des Acadiens et Acadiennes du Nouveau-Brunswick Inc. v Canada*, 2008 SCC 15 ("*Societe des Acadiens*").

On judicial review, *Edmonton Police Service v Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304, the Court of King's Bench upheld Order F2020-17 as reasonable.

EPS appealed the judicial review decision and, on application, intervener status was granted to the Attorney General of Alberta and the Attorney General of Canada (*Edmonton Police Service v Alberta (Information and Privacy Commissioner)*, 2021 ABCA 428).

The Alberta Court of Appeal granted the appeal. In finding that Order F2020-17 was unreasonable, the Court of Appeal held that

the definition of "local government body" in section 1(i)(x) of the FOIP Act included the RCMP in this case. Under this statutory definition, the court held at para. 3 that "EPS falls within [section] 21(1)(b) and could refuse to disclose the confidential report received from the RCMP to the applicant provided the other requirements in the section are satisfied." The Court of Appeal further held at para. 31 that *Societe des Acadiens* "was decided in a different context unrelated to privacy legislation" and was therefore inapplicable. The Court of Appeal stated:

[33] Defining the RCMP as being an entity whose confidentiality may be protected by a public body cannot, on its own, transform the RCMP into an entity subject to provincial privacy legislation. As the OIPC has recently decided, where the question engages the RCMP's obligation to disclose information in its custody or control, the RCMP are more appropriately guided by federal privacy legislation: Order F2017-81.

Order F2020-17 was quashed and the matter was remitted to the OIPC to make determinations on the remaining parts of the test under section 21(1)(b) of the FOIP Act.

## OTHER COURT DECISIONS

### **Carter v Information and Privacy Commissioner, 2022 ABQB 517**

The self-represented applicant had previously been made subject to court access restrictions and had been limited in conducting activities under the FOIP Act (*Carter v Alberta (Ministry of Justice and Solicitor General)*, 2019 ABQB 491) (Carter #1). As such, the applicant was required to obtain leave of the court to initiate and continue litigation, and to conduct certain tribunal activities and processes.

The applicant sought leave from the court to make privacy-related requests under the FOIP Act.

The court held that, as a vexatious litigant, the applicant's proposed activities are presumed to be an abuse of process unless the court is satisfied otherwise. The court reviewed the applicant's materials and held that they did not comply with the conditions set out in Carter #1. The applicant had not copied his leave request to the Information and Privacy Commissioner and the materials did not attach his proposed information or privacy related request. The court held that these defects were fatal to the application and denied the applicant leave to initiate proceedings.

### **Oleynik v University of Calgary, 2023 ABKB 43**

The applicant filed for judicial review of Order F2022-18, and included an affidavit with his originating application. The University of Calgary brought an application to strike the affidavit stating that it contained new evidence that had not been before the adjudicator. The court struck and expunged the affidavit, as well as other materials on the court file containing the affidavit or references to it. The court provided additional instructions regarding scheduling and costs.







# EDUCATION & OUTREACH

53

2022/23 ANNUAL REPORT

Office of the Information and Privacy Commissioner of Alberta

# SPEAKING ENGAGEMENTS

The Commissioner and staff presented at thirteen events in 2022-23. Notably, the OIPC continued to participate in the School at the Legislature program, which provides an opportunity for the office to speak to Alberta students in Grades 6 or 9 about digital privacy, privacy rights and the office's role in protecting personal information.

## COLLABORATION with OTHER JURISDICTIONS

The OIPC works with Information and Privacy Commissioners across Canada, as well as international counterparts, on a variety of initiatives.

### NEW MEMORANDUM OF UNDERSTANDING ON PRIVATE SECTOR PRIVACY

In May 2022, a new Memorandum of Understanding (MOU) was issued promoting greater collaboration between the OIPC, Office of the Privacy Commissioner of Canada (OPC), the Office of the Information and Privacy Commissioner for British Columbia and the Commission d'accès à l'information du Québec. The MOU builds on one previously signed between the OIPC, OPC and Office of the Information and Privacy Commissioner for British Columbia.

Domestic and international enforcement cooperation in the area of privacy law is increasingly critical in a digitized world where data flows transcend borders. Cross-jurisdictional collaboration helps to ensure better protection of the rights of citizens. It can

also benefit organizations by streamlining investigative processes and promoting a greater harmonization in the application of laws. An example of this collaboration is the investigation report on the Tim Hortons app highlighted in the Regulation and Enforcement Section of this annual report.

### JOINT STATEMENT ON FACIAL RECOGNITION

Canada's federal, provincial and territorial privacy commissioners issued in May 2022 a joint statement recommending a legal framework for police agencies' use of facial recognition.

The joint statement recognized facial recognition as a tool of significant interest to police agencies across Canada. Despite its emergence, the Commissioners noted that use of facial recognition by police is not subject to a clear and comprehensive set of rules and, instead, is regulated through a patchwork of statutes that for the most part do not specifically address different uses or risks posed by the technology. The Commissioners cautioned that the current legal framework risks encouraging fragmented approaches to facial recognition use that would take years to resolve before the courts.

To help resolve these issues the Commissioners recommended the following key elements of a legal framework for regulating police use of facial recognition including:

- Clear authorization for police use of facial recognition subject to clear "no-go zones"



- Strict necessity and proportionality requirements
- Independent oversight for facial recognition initiatives
- Consideration of other privacy rights and protections

To assist with developing the joint statement, in June 2021, Canada's privacy commissioners published draft guidance intended to clarify police agencies' existing privacy obligations relating to the use of facial recognition technology. At the same time, the Commissioners launched a public consultation, seeking feedback on both the guidance as well as a future legal and policy framework to govern police use of the technology. In Alberta, municipal police services, certain academics and a privacy advocacy organization were invited by the OIPC to respond to the public consultation. In total, Canada's privacy commissioners received 29 written submissions that assisted in formulating the joint statement.

## JOINT RESOLUTION ON SECURING PUBLIC TRUST IN DIGITAL HEALTHCARE

In September 2022, Canada's privacy commissioners joined in commenting on the innovation and change in the delivery of healthcare services, including through virtual care visits and other forms of digital health communications. Despite rapid digital advancements in the health sector, the Commissioners noted breaches continue to be caused by the use of insecure communication technologies such as traditional fax machines and unencrypted emails, unauthorized access to health records by employees (often in the form of "snooping", or unauthorized access to health information without a valid business purpose), and cybersecurity attacks including ransomware.

In the resolution, the Commissioners said that privacy is not a barrier to innovation. They added that we must ensure that the shift to digital healthcare is secured by reasonable administrative, technical and physical safeguards as critical to maintaining

Canadians' trust in the health system. Furthermore, the adoption of secure digital technologies can provide relief from the administrative, financial and reputational costs associated with privacy breaches.

Considering the complexities involved in implementing secure digital healthcare technologies, the Commissioners urged various stakeholders to commit to certain actions.

For example, federal, provincial and territorial governments were asked to promote the adoption of secure digital technologies and the implementation of responsible data governance frameworks that provide reasonable protection of personal health information against unauthorized access or inadvertent disclosures. Governments were also called on to amend laws and regulations, as necessary, to further provide for meaningful penalties, including administrative penalties where appropriate, for health institutions and providers that do not take reasonable measures necessary to protect personal health information as well as for individuals who unlawfully collect, use, or disclose personal health information.

With respect to health sector institutions and providers, these stakeholders were, for example, urged by the Commissioners to seek guidance from relevant experts to understand how to evaluate new digital health solutions for modernizing means of communicating personal health information. Health sector institutions and providers were also called on to assess new innovations' compatibility with other digital assets, compliance with health information privacy laws, and how these products facilitate the rights of individuals to access their own records of personal health information.

Finally, the Commissioners committed to, for example, collaborating with governments, regulatory colleges, health sector and other relevant stakeholders to provide privacy and security guidance as the health sector transitions toward modern, secure and interoperable digital alternatives for communicating personal health information.

# MEDIA AWARENESS

## **TRADITIONAL MEDIA**

The OIPC responded to 49 media requests in 2022-23, a decrease of 22% compared with 2021-22 (63).

The following topics generated the most media requests:

- Tenant “blacklists” and discussions about “bad tenants” by landlords on social media sites
- Allegations of political staff in the Government of Alberta evading access to information requests by using instant messaging services and regularly deleting potentially responsive records
- Announcement of an investigation into the Alberta Energy Regulator (AER) concerning AER’s consideration of the public interest override, or section 32, under the FOIP Act with respect to a tailings pond leak from Imperial’s Kearl Oil Sands Project

## **SOCIAL MEDIA**

Twitter is used by the OIPC to share investigation reports, publications, announcements and news releases, and to promote events or raise awareness about access and privacy laws.

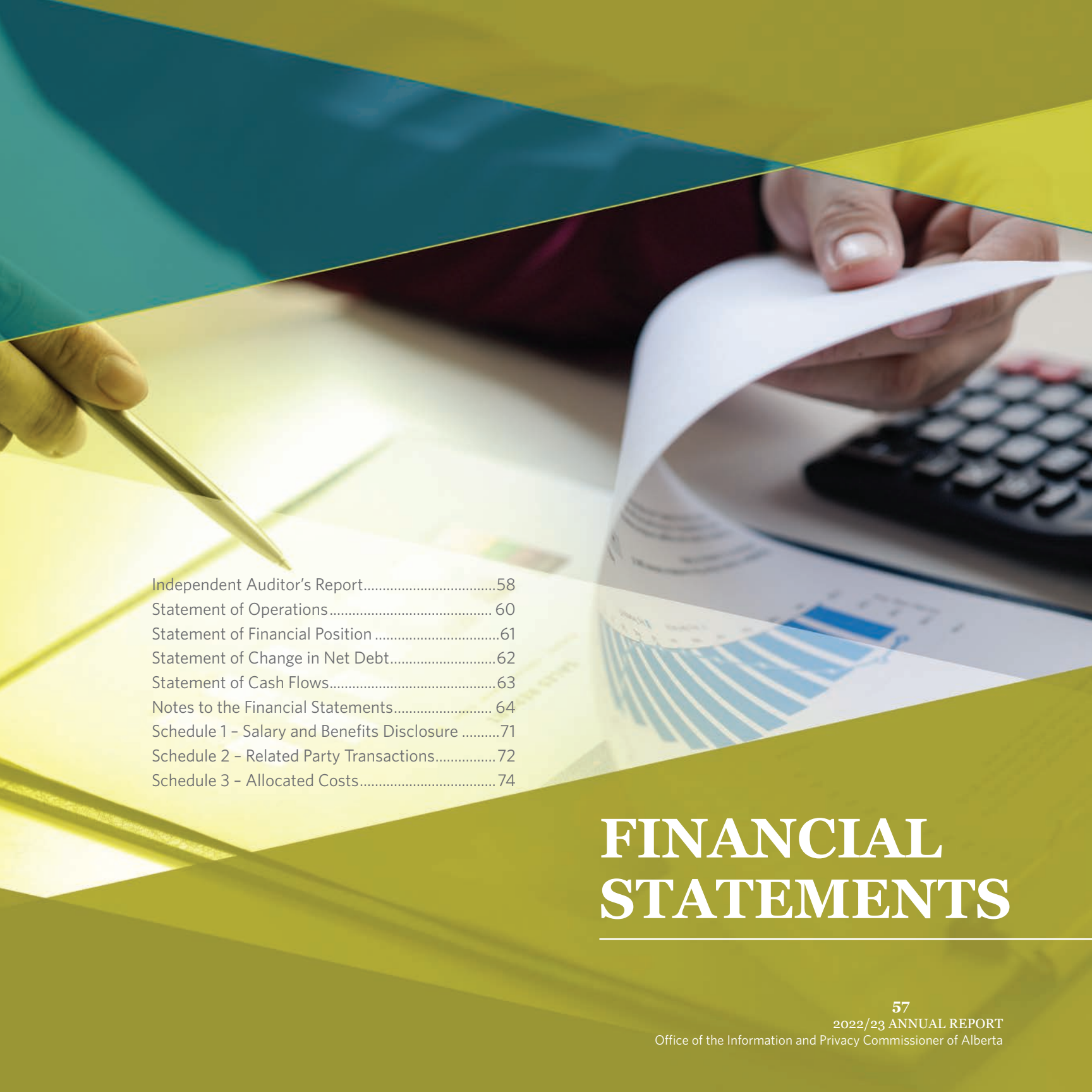
The following topics received among the most views or engagements on Twitter:

- Announcement of an investigation into AER as noted above in the section on Traditional Media
- Guidance on landlord and tenant privacy issues under PIPA
- Welcoming new Commissioner Diane McLeod

The OIPC’s Twitter account is available at [www.twitter.com/ABoipc](https://www.twitter.com/ABoipc).

## **NEW OIPC WEBSITE PLATFORM**

The OIPC updated the website in July 2022 to a new platform or content management system. While the design and content remained similar, the change allows the OIPC to provide new functionality and features in the future.



Independent Auditor's Report.....58  
Statement of Operations..... 60  
Statement of Financial Position .....61  
Statement of Change in Net Debt.....62  
Statement of Cash Flows.....63  
Notes to the Financial Statements..... 64  
Schedule 1 – Salary and Benefits Disclosure .....71  
Schedule 2 – Related Party Transactions..... 72  
Schedule 3 – Allocated Costs..... 74

# FINANCIAL STATEMENTS

## **Independent Auditor's Report**

To the Members of the Legislative Assembly

### **Report on the Financial Statements**

#### **Opinion**

I have audited the financial statements of the Office of the Information and Privacy Commissioner (the OIPC), which comprise the statement of financial position as at March 31, 2023, and the statements of operations, change in net debt, and cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In my opinion, the accompanying financial statements present fairly, in all material respects, the financial position of the OIPC as at March 31, 2023, and the results of its operations, its changes in net debt, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

#### **Basis for opinion**

I conducted my audit in accordance with Canadian generally accepted auditing standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the OIPC in accordance with the ethical requirements that are relevant to my audit of the financial statements in Canada, and I have fulfilled my other ethical responsibilities in accordance with these requirements. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

#### **Other information**

Management is responsible for the other information. The other information comprises the information included in the Annual Report, but does not include the financial statements and my auditor's report thereon. The Annual Report is expected to be made available to me after the date of this auditor's report.

My opinion on the financial statements does not cover the other information and I do not express any form of assurance conclusion thereon.

In connection with my audit of the financial statements, my responsibility is to read the other information identified above and, in doing so, consider whether the other information is materially inconsistent with the financial statements or my knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work I will perform on this other information, I conclude that there is a material misstatement of this other information, I am required to communicate the matter to those charged with governance.

#### **Responsibilities of management and those charged with governance for the financial statements**

Management is responsible for the preparation and fair presentation of the financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of the financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the OIPC's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless an intention exists to liquidate or to cease operations, or there is no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the OIPC's financial reporting process.

### **Auditor's responsibilities for the audit of the financial statements**

My objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Canadian generally accepted auditing standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Canadian generally accepted auditing standards, I exercise professional judgment and maintain professional skepticism throughout the audit. I also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the OIPC's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.

- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the OIPC's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the OIPC to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Original signed by

**W. Doug Wylie FCPA, FCMA, ICD.D**

Auditor General  
July 12, 2023  
Edmonton, Alberta

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER **STATEMENT OF OPERATIONS**

Year ended March 31, 2023

	2023		2022
	Budget	Actual	Actual
<b>Revenues</b>			
Prior Year Expenditure Refund	\$ -	\$ -	\$ 3,979
Other Revenue	-	283	135
	-	283	4,114
<b>Expenses – Directly Incurred (Note 3b)</b>			
Salaries, Wages, and Employee Benefits	\$ 6,385,000	\$ 6,096,258	\$ 5,750,518
Supplies and Services	1,056,000	1,313,844	1,265,019
Amortization of Tangible Capital Assets (Note 5)	-	51,824	45,613
<b>Total Program-Operations</b>	7,441,000	7,461,926	7,061,150
<b>Net Cost of Operations</b>	\$ (7,441,000)	\$ (7,461,643)	\$ (7,057,036)

The accompanying notes and schedules are part of these financial statements.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF FINANCIAL POSITION

As at March 31, 2023

### Financial Assets

Cash

Accounts Receivable

### Liabilities

Accounts Payable and Other Accrued Liabilities

Accrued Vacation Pay

### Net Debt

### Non-Financial Assets

Tangible Capital Assets (Note 5)

Prepaid Expenses

### Net Liabilities

Net Liabilities at Beginning of Year

Net Cost of Operations

Net Financing Provided from General Revenues

Net Liabilities at End of Year

Contractual obligations (Note 7)

	2023	2022
<b>Financial Assets</b>		
Cash	\$ 200	\$ 200
Accounts Receivable	4,721	-
	4,921	200
<b>Liabilities</b>		
Accounts Payable and Other Accrued Liabilities	169,841	319,314
Accrued Vacation Pay	726,792	621,434
	896,633	940,748
<b>Net Debt</b>	(891,712)	(940,548)
<b>Non-Financial Assets</b>		
Tangible Capital Assets (Note 5)	158,016	209,840
Prepaid Expenses	60,671	47,668
	218,687	257,508
<b>Net Liabilities</b>	\$ (673,025)	\$ (683,040)
Net Liabilities at Beginning of Year	\$ (683,040)	\$ (655,050)
Net Cost of Operations	(7,461,643)	(7,057,036)
Net Financing Provided from General Revenues	7,471,658	7,029,046
Net Liabilities at End of Year	\$ (673,025)	\$ (683,040)

The accompanying notes and schedules are part of these financial statements.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

### STATEMENT OF CHANGE IN NET DEBT

Year ended March 31, 2023

	2023		2022
	Budget	Actual	Actual
<b>Net Cost of Operations</b>	\$ (7,441,000)	\$ (7,461,643)	\$ (7,057,036)
Acquisition of Tangible Capital Assets (Note 5)		-	(31,876)
Amortization of Tangible Capital Assets (Note 5)		51,824	45,613
(Increase)/Decrease in Prepaid Expenses		(13,003)	6,070
Net Financing Provided from General Revenues		7,471,658	7,029,046
<b>Decrease/(Increase) in Net Debt</b>		48,836	(8,183)
<b>Net Debt, Beginning of Year</b>		(940,548)	(932,365)
<b>Net Debt, End of Year</b>		\$ (891,712)	\$ (940,548)

The accompanying notes and schedules are part of these financial statements.

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF CASH FLOWS

Year ended March 31, 2023

	2023	2022
<b>Operating Transactions</b>		
Net Cost of Operations	\$ (7,461,643)	\$ (7,057,036)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 5)	51,824	45,613
Valuation adjustment - Accrued Vacation Pay	105,358	85,262
	(7,304,461)	(6,926,161)
(Increase)/Decrease in Accounts Receivable	(4,721)	57,884
(Increase)/Decrease in Prepaid Expenses	(13,003)	6,070
Decrease in Accounts Payable and Other Accrued Liabilities	(149,473)	(134,963)
Cash Applied to Operating Transactions	(7,471,658)	(6,997,170)
<b>Capital Transactions</b>		
Acquisition of Tangible Capital Assets (Note 5)	-	(31,876)
<b>Financing Transactions</b>		
Net Financing Provided from General Revenues	7,471,658	7,029,046
<b>Cash, Increase</b>	-	-
<b>Cash, at Beginning of Year</b>	200	200
<b>Cash, at End of Year</b>	\$ 200	\$ 200

The accompanying notes and schedules are part of these financial statements.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

### NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

#### **Note 1 Authority**

The Office of the Information and Privacy Commissioner (the Office) operates under the authority of the *Freedom of Information and Protection of Privacy Act*. General Revenues of the Province of Alberta fund both the cost of operations of the Office and the purchase of tangible capital assets. The all-party Standing Committee on Legislative Offices reviews and approves the Office's annual operating and capital budgets.

#### **Note 2 Purpose**

The Office provides oversight on the following legislation governing access to information and protection of privacy:

*Freedom of Information and Protection of Privacy Act*  
*Health Information Act*  
*Personal Information Protection Act*

The major operational purposes of the Office are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

#### **Note 3 Summary of Significant Accounting Policies and Reporting Practices**

##### **Reporting Entity**

These financial statements are prepared in accordance with Canadian public sector accounting standards. The Office has adopted PS3450 Financial Instruments. As the Office does not have any transactions involving financial instruments that are classified in the fair value category, there is no statement of remeasurement gains and losses.

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

### **Note 3 Summary of Significant Accounting Policies and Reporting Practices (Cont'd)**

#### **Basis of Financial Reporting**

(a) Revenue

All revenues are reported on the accrual basis of accounting.

(b) Expenses

Expenses are reported on an accrual basis. The Office's expenses are either directly incurred or incurred by others:

Directly incurred

Directly incurred expenses are those costs incurred under the authority of the Office's budget as disclosed in the Office's budget documents.

Pension costs included in directly incurred expenses comprise employer contributions to multi-employer plans. The contributions are based on actuarially determined amounts that are expected to provide the plans' future benefits.

Incurred by others

Services contributed by other entities in support of the Office's operations are not recognized and are disclosed in Schedule 2.

(c) Financial assets

Financial assets are assets that could be used to discharge existing liabilities or finance future operations and are not for consumption in the normal course of operations.

Accounts Receivable

Accounts receivable are recognized at the lower of cost or net recoverable value. A valuation allowance is recognized when recovery is uncertain.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

### **Note 3 Summary of Significant Accounting Policies and Reporting Practices (Cont'd)**

(d) Liabilities

Liabilities are present obligations of the Office to external organizations and individuals arising from past transactions or events, the settlement of which is expected to result in the future sacrifice of economic benefits.

They are recognized when there is an appropriate basis of measurement and management can reasonably estimate the amounts.

(e) Non-financial assets

Non-financial assets are acquired, constructed, or developed assets that do not normally provide resources to discharge existing liabilities, but instead:

- are normally employed to deliver the Office's services;
- may be consumed in the normal course of operations; and
- are not for sale in the normal course of operations.

Non-financial assets of the Office include tangible capital assets and prepaid expenses.

Tangible capital assets

Tangible capital assets are recorded at historical cost less accumulated amortization. Amortization begins when the assets are put into service and is recorded on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is \$5,000 except new systems development is \$250,000 and major enhancements to existing systems is \$100,000.

Prepaid expenses

Prepaid expenses are recognized at cost and amortized based on the terms of the agreement.

(f) Net debt

Net debt indicates additional cash required from General Revenues to finance the Office's cost of operations to March 31, 2023.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER **NOTES TO THE FINANCIAL STATEMENTS**

March 31, 2023

### **Note 4 Future Accounting Changes**

The Public Sector Accounting Standards Board's PS 3400 Revenue and PS 3160 Public Private Partnerships are effective for fiscal years starting on or after April 1, 2023. Management has determined neither standard will impact the office's financial statements.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

### Note 5 Tangible Capital Assets

	Leasehold Improvements	Office Furniture and Equipment	Computer Hardware and Software	2023 Total	2022 Total
<b>Estimated Useful Life</b>	5 years	5 years	5 years		
<b>Historical Cost</b>					
Beginning of Year	\$ 43,142	\$ 113,759	\$ 609,849	\$ 766,750	\$ 734,874
Additions	-	-	-	-	31,876
Disposals	-	-	-	-	-
<b>Total Historical Cost</b>	\$ 43,142	\$ 113,759	\$ 609,849	\$ 766,750	\$ 766,750
<b>Accumulated Amortization</b>					
Beginning of Year	\$ 11,639	\$ 82,761	\$ 462,510	\$ 556,910	\$ 511,297
Amortization Expense	8,628	8,599	34,597	51,824	45,613
Disposals	-	-	-	-	-
<b>Total Accumulated Amortization</b>	\$ 20,267	\$ 91,360	\$ 497,107	\$ 608,734	\$ 556,910
<b>Net Book Value at March 31, 2023</b>	\$ 22,875	\$ 22,399	\$ 112,742	\$ 158,016	
<b>Net Book Value at March 31, 2022</b>	\$ 31,503	\$ 30,998	\$ 147,339		\$ 209,840

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

### **Note 6 Defined Benefit Plans**

The Office participates in the multi-employer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of \$572,253 for the year ended March 31, 2023 (2022 - \$549,125).

At December 31, 2022, the Management Employees Pension Plan reported a surplus of \$924,735,000 (2021 - surplus \$1,348,160,000) and the Public Service Pension Plan reported a surplus of \$4,258,721,000 (2021 - surplus \$4,588,479,000). At December 31, 2022 the Supplementary Retirement Plan for Public Service Managers had a deficit of \$25,117,000 (2021 - deficit \$20,982,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2023, the Management, Opted Out and Excluded Plan reported an actuarial deficit of \$1,962,000 (2022 - surplus \$7,494,000). The expense for this plan is limited to employer's annual contributions for the year.

### **Note 7 Contractual Obligations**

Contractual Obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2023	2022
Obligations under operating leases and contracts	\$ 1,562	\$ 7,808

	2023-24
Estimated payment requirements for future years are as follows:	\$ 1,562



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER NOTES TO THE FINANCIAL STATEMENTS

March 31, 2023

### **Note 8 Contingent liabilities**

The Office is named in one (2022 – one) legal matter where legal costs are being sought and the outcome of this claim is not determinable.

### **Note 9 Budget**

The budget shown on the statement of operations is based on the budgeted expenses that the all-party Standing Committee on Legislative Offices approved on March 21, 2022. The following table compares the office's actual expenditures, excluding non-voted amounts such as surplus sales and amortization, to the approved budgets:

	Voted Budget	Actual Expended	Unexpended
Operating expenditures	\$ 7,441,000	\$ 7,410,102	\$ 30,898
Capital investments	-	-	-
	\$ 7,441,000	\$ 7,410,102	\$ 30,898

(1) As per *Appropriation (Supplementary Supply) Act, 2022*, approved March 17, 2022.

### **Note 10 Approval of Financial Statements**

These financial statements were approved by the Information and Privacy Commissioner.

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER **SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE**

Year ended March 31, 2023

	2023			2022
	Base Salary <sup>(a)</sup>	Other Non-cash Benefits <sup>(b)(c)</sup>	Total	Total
<b>Senior Official</b>				
Information and Privacy Commissioner	\$ 239,251	\$ 93,504	\$ 332,755	\$ 296,760

<sup>(a)</sup> Base salary is comprised of pensionable base pay.

<sup>(b)</sup> Other non-cash benefits include the Office's share of all employee benefits and contributions or payments made on behalf of employees, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, professional memberships, and tuition fees.

<sup>(c)</sup> Other non-cash benefits for the Information and Privacy Commissioner paid by the Office include \$8,186 (2022: \$7,735) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office and a one time \$15,166 relocation expense paid to Diane McLeod hired on August 1, 2022 to replace Jill Clayton as Commissioner.



# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

### SCHEDULE 2 - RELATED PARTY TRANSACTIONS

Year ended March 31, 2023

Related parties are those entities consolidated or accounted for on the modified equity basis in the Government of Alberta's Consolidated financial statements. Related parties also include key management personnel and close family members of those individuals in the Office. The Office and its employees paid or collected certain taxes and fees set by regulations for premiums, licenses and other charges. These amounts were incurred in the normal course of business, reflect charges applicable to all users, and have been excluded from this schedule.

The Office of the Information and Privacy Commissioner had the following transactions with related parties recorded on the Statement of Operations and the Statement of Financial Position at the amount of consideration agreed upon between the related parties:

#### Expenses - Directly Incurred

Alberta Risk Management Fund  
Postage  
Information Services  
Technology Services  
Consumption  
Fleet vehicle

Other Entities			
	2023		2022
\$	4,392	\$	4,332
	10,132		11,240
	62		-
	17,500		10,500
	3,055		775
	5,108		5,412
\$	40,249	\$	32,259

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER **SCHEDULE 2 - RELATED PARTY TRANSACTIONS**

Year ended March 31, 2023

The Office of the Information and Privacy Commissioner also had the following transactions with related parties for which no consideration was exchanged. The amounts for these related party transactions are estimated based on the costs incurred by the service provider to provide the service. These amounts are not recorded in the financial statements but are disclosed in Schedule 3.

	Other Entities	
	2023	2022
<b>Expenses - Incurred by Others</b>		
Accommodation Costs	\$ 489,217	\$ 457,345
Business Services	54,000	74,000
	<b>\$ 543,217</b>	<b>\$ 531,345</b>

# FINANCIAL STATEMENTS

## OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER **SCHEDULE 3 - ALLOCATED COSTS**

Year ended March 31, 2023


Program	2023				2022
	Expenses - Incurred by Others				
	Expenses <sup>(a)</sup>	Accommodation Costs <sup>(b)</sup>	Business Services <sup>(c)</sup>	Total Expenses	Total Expenses
Operations	\$ 7,461,926	\$ 489,217	\$ 54,000	\$ 8,005,143	\$ 7,592,495

<sup>(a)</sup> Expenses - Directly Incurred as per Statement of Operations which include related party transactions as disclosed in Schedule 2.

<sup>(b)</sup> Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.

<sup>(c)</sup> Business services includes charges for shared services, finance services, technology services, 1GX, and Corporate Overhead.





Appendix A: Cases Opened under FOIP, HIA, PIPA  
by Entity Type..... 76

Appendix B: Cases Closed under FOIP, HIA, PIPA  
by Entity Type..... 78

Appendix C: Orders, Decisions and Public Investigation  
Reports Issued..... 80

# APPENDICES

## APPENDIX A: CASES OPENED UNDER FOIP BY ENTITY TYPE

Statistics are from April 1, 2022 to March 31, 2023

FOIP	Entity Type	Advice and Direction	Authorization to Disregard a Request	Authorization to Indirectly Collect	Complaint	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Office Investigation	Other	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
	Agencies																0
	Boards				2	1						14	3	4			24
	Colleges				2					1		1		1	3		7
	Commissions	1										2					2
	Committees													1			1
	Crown Corporations																0
	Federal Departments																1
	Foundations										1				1		1
	Government Ministries/Departments				14	2				4		148	19	191	9		387
	Health Quality Council of Alberta																0
	Hospital Board (Covenant Health)																0
	Independent Agency																0
	Law Enforcement Agencies				1		2			1	1	70		5	2		82
	Legislative Assembly Office																0
	Local Government Bodies											1			1		2
	Long Term Care Centres					1											0
	Municipalities	1			16						1	69	22	65	14		189
	Nursing Homes																0
	Office of the Premier/Alberta Executive Council					1						11					12
	Officers of the Legislature											3		3	1		7
	Panels																0
	Regional Health Authorities (Alberta Health Services)				1							5	2	13			21
	School Districts	1			4					2		14		2	12		35
	Tribunal																0
	Universities				2						1	10		9	4		26
	Other											1			6		7
	<b>Total</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>42</b>	<b>1</b>	<b>4</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>7</b>	<b>4</b>	<b>349</b>	<b>46</b>	<b>294</b>	<b>53</b>	<b>804</b>

Note: The statistics do not include Intake cases.

## APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2022 to March 31, 2023

Case Type	FOIP	HIA	PIPA
Intake - 3rd party RR Search	375		
Intake - Complaint	40	24	61
Intake - Info Rec'd in Error	1		
Intake - PIA		72	
Intake - Request for Access to P/C/O info	4	2	1
Intake - Request for Information			
Intake - Request for Review	75	16	18
Intake - Request for Review 3rd Party Intervention			
Intake - Request to Excuse Fees	1		
<b>Total</b>	496	114	80
<b>Total</b>	690		

## APPENDIX B: CASES CLOSED UNDER FOIP BY ENTITY TYPE

Statistics are from April 1, 2022 to March 31, 2023

FOIP	Entity Type	Advice and Direction	Authorization to Disregard a Request	Authorization to Indirectly Collect	Complaint	Disclosure to Commissioner	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Request Advance Ruling	Self-reported Breach	Total
	Agencies																	0
	Boards			3								7	1	8		1		20
	Colleges			1										1		6		8
	Commissions			1														1
	Committees													1				1
	Crown Corporations																	0
	Federal Departments																	0
	Foundations													1				1
	Government Ministries/Departments	1		7			2			3	1	108	21	187		9		339
	Health Quality Council of Alberta																	0
	Hospital Board (Covenant Health)																	0
	Law Enforcement Agencies			13		1	1	2		3	1	58		5		2		86
	Legislative Assembly Office										1							1
	Local Government Bodies											1				3		4
	Long Term Care Centres											1						1
	Municipalities	4		19		1	1				1	70	7	61		13		177
	Nursing Homes																	0
	Office of the Premier/Alberta Executive Council											4						4
	Officers of the Legislature											2		3				5
	Panels																	0
	Regional Health Authorities (Alberta Health Services)			1			1			3		13	1	14				33
	School Districts	2		4			2					5		2		23		38
	Universities										1	7		10		6		24
	Other			1		1	1			2		10				2		17
	<b>Total</b>	<b>0</b>	<b>7</b>	<b>0</b>	<b>50</b>	<b>0</b>	<b>3</b>	<b>8</b>	<b>2</b>	<b>0</b>	<b>11</b>	<b>5</b>	<b>286</b>	<b>30</b>	<b>293</b>	<b>0</b>	<b>65</b>	<b>760</b>

## APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2022 to March 31, 2023

Case Type	FOIP	HIA	PIPA
Intake - 3rd party RR Search	373		
Intake - Complaint	48	22	56
Intake - Info Rec'd in Error			
Intake - PIA		71	1
Intake - Request for Access to P/C/O info	5	2	1
Intake - Request for Information			
Intake - Request for Review	70	12	19
Intake - Request for Review 3rd Party Intervention			
Intake - Request to Excuse Fees	2		
<b>Total</b>	498	107	77
<b>Total</b>	682		

## APPENDIX C: ORDERS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from the period April 1, 2022 to March 31, 2023

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total	#files	Notes
Agriculture and Irrigation	1				1	
Alberta Health Services	2				2	Note 1
Alberta Human Rights Commission	1				1	
Alberta Pension Services Corporation	1				1	
Calgary Police Service	2				2	
Children's Services	1				1	
Chinook's Edge School Division	1				1	
City of Calgary	4				4	
City of Edmonton	3				4	
City of Lethbridge	2				2	
Edmonton Police Service	6				9	Note 2
Energy	4				4	
Environment and Parks	2				3	
Environment and Protected Areas	3				3	
Health	3				3	
Indigenous Relations	1				1	
Justice	2				2	
Justice and Solicitor General	7				7	Note 3
Public Safety and Emergency	4				4	
Public Service Commission	1				1	
Rocky View County	1				1	
Town of Beaverlodge	2				2	
Town of Penhold	1				1	
University of Alberta	2				1	Note 4
University of Calgary	1				1	
Village of Longview	1				1	
<b>Total</b>	<b>59</b>	<b>0</b>			<b>63</b>	



HIA Respondent	Orders	Decisions	Public Investigation Reports	Total	#files	Notes
Alberta Health Services	3				4	Note 5
Dr. Elizabeth Kelly	1				1	
Dr. Khaled Ateer	1				1	
<b>Total</b>	<b>5</b>	<b>0</b>			<b>6</b>	

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total	#files	Notes
Acuren Group Inc.	1				1	
Advanced Upstream Ltd.	1				1	
Alberta Teachers' Association	1				1	
Association of Professional Engineers and Geoscientists (APEGA)	1				1	
Canem Systems Ltd.	1				1	
Direct Energy Regulated Services	1				1	
Portpass Inc.			1		1	
Restaurant Brands International Inc o/a Tim Hortons			1		1	
Inner Solutions Ltd.	1				2	
Shell Canada Ltd.	1				1	
<b>Total</b>	<b>8</b>	<b>0</b>			<b>11</b>	

<b>Complete Total</b>	<b>72</b>	<b>0</b>			<b>80</b>	
-----------------------	-----------	----------	--	--	-----------	--

FOIP Orders: 59  
HIA Orders: 5  
PIPA Orders: 8  
PIPA Investigation Reports: 2

**Notes:**

Note 1: Order F2023-10/H2023-02 covers files 022152 (FOIP) and 029798 (HIA).  
Note 2: Order F2022-R-01 was a reconsideration of file F7384.  
Note 3: Order F2022-33 issued 2022/23 did not close file 011951; Order F2023-17 issued 2023/24 closed file 011951.  
Note 4: Orders F2022-22 and F2022-56 covered file 005994. Order F2022-56 closed the file.  
Note 5: Order H2022-06 covered part 1 of inquiry for files 008518 and 008527; no order issued for part 2 (refused).



## **NOTES FOR ANNUAL REPORT**

- (1) This table contains all Orders and Decisions released by the OIPC whether the issuance of the Order or Decision concluded the matter or not.
- (2) The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned. A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.
- (3) Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.
- (4) Only those Investigation Reports that are publicly released are reported.
- (5) Copies of Orders, Decisions and public Investigation Reports are available on the OIPC web site [www.oipc.ab.ca](http://www.oipc.ab.ca).

