Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 032-2023

Ministry of Immigration and Career Training

May 31, 2023

Summary: The Ministry of Immigration and Career Training (Immigration) proactively reported a breach of privacy to the Commissioner's office. The report stated that an Immigration employee had inappropriately accessed the personal information of individuals contrary to *The Freedom of Information and Protection of Privacy Act* (FOIP). The Commissioner investigated the incidents. He found that Immigration's notice to the affected parties and steps taken to contain the breach were not adequate. He also found that its plan to prevent further breaches should include a plan to implement mandatory, annual privacy training. The Commissioner recommended that Immigration ensure that its notifications to affected parties include information about identity theft and offer credit monitoring where that is a risk. He also recommended that Immigration complete its investigation and proposed technical changes to its systems. If it had not already done so, the Commissioner recommended that Immigration refer this matter to the Ministry of Justice and Attorney General to consider a prosecution under FOIP.

I BACKGROUND

[1] On February 8, 2023, the Ministry of Immigration and Career Training (Immigration) proactively reported a privacy breach to my office. In its report, it indicated that an employee of its Immigration Services Branch had inappropriately accessed the personal information of 23 clients relating to their immigration applications. Immigration stated that the employee's actions were contrary to *The Freedom of Information and Protection of Privacy Act* (FOIP). Immigration subsequently explained that the access was discovered during an investigation into allegations of wrongdoing by the employee.

[2] Immigration suspected that the employee was accessing its clients' personal information and sharing it with a third party outside the ministry as part of an illegal immigration scheme. Immigration explained that it received a complaint from one of its clients alleging that the third party sought money in exchange for the approval of their immigration application.

[3] In the course of the investigation that followed this complaint, Immigration discovered that the employee had inappropriately accessed information of other clients. Immigration stated that initially it identified 23 affected individuals and notified them of the privacy breach on February 7, 2023. Five additional affected individuals were later identified and were notified on February 21, 2023. It also stated that if additional affected individuals are identified in its ongoing investigation, they will be notified as quickly as possible.

[4] On February 17, 2023, my office notified Immigration that it would be investigating the matter and requested further information about the privacy breach. On March 27, 2023, Immigration provided my office with a completed *Privacy Breach Investigation Questionnaire* and additional documentation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[5] Immigration qualifies as a "government institution" pursuant to subsection 2(1)(d)(i) of FOIP.

[6] The privacy rules in FOIP only apply to personal information. Therefore, I must determine if the information at issue qualifies as personal information (*Guide to FOIP*, Chapter 6: "Protection of Privacy", updated: February 27, 2023, [*Guide to FOIP*, Ch. 6], at page 31).

[7] Immigration stated that data inappropriately accessed by the employee varied with each of the affected individuals. In some cases, only individuals' contact information was accessed.

In other cases, affected individuals' entire file was accessed. Some of the files included information about the individuals' passports, employment, finances, and family members.

[8] Individuals' names and personal contact details would qualify as personal information pursuant to subsection 24(1)(e) of FOIP. Individuals' passport information would qualify as personal information pursuant to subsection 24(1)(d) and (k) of FOIP. Employment and financial information would qualify as personal information under subsection 24(1)(b) of FOIP. Information about the individuals' family members would qualify as personal information pursuant to subsection 24(1)(a) of FOIP. These subsections provide as follows:

> **24**(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[9] Therefore, as Immigration is a government institution and personal information is involved in this breach, I find that I have jurisdiction to investigate this matter under FOIP.

2. Did Immigration respond appropriately to this privacy breach?

[10] In circumstances where there is no dispute that a privacy breach has occurred, my office's investigation focuses on whether the government institution has appropriately handled the breach.

[11] As set out in section 4-4 of my office's *Rules of Procedure* and my office's *Guide to FOIP*, Ch. 6, p. 267, my analysis of Immigration's response to the privacy breaches involves a consideration of the following:

1. Containment of the breach
2. Notification of affected individuals
3. Investigation of the breach
4. Steps taken to prevent future breaches.

[12] I turn to consider how Immigration followed each of these steps.

Containment of the breach

[13] Upon learning that a privacy breach has occurred, government institutions should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice
- Recovering the records
- Shutting down the system that has been breached
- Revoking access to personal information or personal health information
- Correcting weakness in physical security

(*Guide to FOIP*, Ch. 6, p. 273)

[14] In my office's Investigation Report 197-2022, 215-2022, I stated that in assessing an institution's steps to contain the breach, my office applies a reasonableness standard. We want to have some reassurance that the institution has reduced the magnitude of the breach and the risk to affected individuals.

[15] The circumstances of this breach are as follows. On April 26, 2022, a client complained to Immigration's Information Communications and Technology Unit (ICT) that an Immigration employee had inappropriately accessed their Saskatchewan Immigrant Nominee Program (SINP) file and shared their information with another individual who was not an employee of Immigration (the recipient). SINP files are located in Immigration's Online Application System for Immigrating to Saskatchewan (OASIS). The client also alleged that the recipient contacted them and asked for money for approval of their SINP application. Given the serious nature of the allegations, Immigration informed the Canada Border Services Agency of the allegations.

[16] On April 28, 2022, Immigration received an audit report of the OASIS system. According to Immigration's "Privacy Breach Incident Report", the audit report revealed "unusual activity" by the employee.

[17] As a result of the allegation, Immigration notified senior staff within Immigration and further investigations were undertaken. On June 28, 2022, Immigration received another complaint about the employee. This complaint was made by an organization outside Immigration also alleging inappropriate conduct by the employee. Immigration decided to retain the services of a third party to conduct an investigation into the employee's activities. It did not initially treat the allegations in the two complaints as potential privacy breaches. Immigration asserted:

> By June of 2022, it became clear that a more in-depth investigation was warranted. At the time, ISB decided to contract with a third party […] to conduct an employee investigation, complete with interviews with the management team, [the employee] and one immigration representative. The decision was made to not pursue this as a privacy breach investigation, as it was unclear if a breach had occurred. It was clear that there was suspicious activity; however, a choice was made to pursue this as a Human Resource (HR) matter first and thus the employee investigation with […] began on July 6, 2022.

[18] According to Immigration's "Privacy Breach Incident Report" a "special vendor report" of the employee's access to OASIS on July 11, 2022, revealed that the employee had accessed client files on that day. As the employee was on vacation leave on July 11, 2022, they were not authorized to access OASIS files.

[19] On July 26, 2022, the employee's access rights to OASIS were terminated.

[20] On August 22, 2022, the third-party's investigation report concluded that the employee had not complied with FOIP.

[21] Between August 22, 2022 and November 21, 2022, Immigration's reviews of the employee's activities on OASIS continued. On November 21, 2022, the Executive Director of the Immigration Services Branch notified Immigration's privacy office of the incidents. This was approximately seven months after Immigration staff had been made aware of the allegation involving the use and disclosure of personal information.

[22] With respect to the delay in notifying Immigration's privacy office, Immigration asserted:

> This breach, the multiple investigations, and the involvement of outside agencies has resulted in a very complex and challenging situation. The complexity of a human resource investigation coupled with the potential of a criminal investigation with the Canada Border Services Agency has made this situation much more difficult to maneuver through. It was not known if the affected individuals were associates of [the employee]. In order to avoid negatively impacting an active criminal investigation, the decision was made not to inform the affected individuals immediately, and to not inform the [Director/Chief Privacy and Access Officer] until now.

[23] I note that Appendix E to Immigration's "Privacy Framework" dated April 2020 requires that staff notify Immigration's Chief Privacy and Access Officer (CPAO) "as quickly as possible" after becoming aware of a "potential privacy breach". It states that the CPAO "can provide advice and must be involved in the resulting assessments and reports." In this case, it appears that Immigration staff did not comply with the "Privacy Framework" in that they failed to notify the CPAO "as quickly as possible" after becoming aware of a potential breach.

[24] While I accept that this incident raised some complex issues that involved multiple outside parties, multiple investigations and the potential for a criminal investigation, Immigration staff should not have delayed involving the CPAO. The CPAO could have worked with staff to develop an appropriate and timely response to the breach. For example, while the allegation of inappropriate access was made in April 2022, it was not until July 2022 that the employee's access rights to OASIS were terminated. During that period of time, it appears that additional unauthorized accesses occurred, thus continuing the breaches. This might have been avoided if the CPAO had been involved earlier.

[25] Because of this, I find that Immigration did not take appropriate and timely action to contain the breach. I recommend that, in the future, Immigration should notify its privacy staff as soon as possible after becoming aware of a potential breach of privacy.

Notification of affected individuals

[26] Section 29.1 of FOIP requires that, where there is an unauthorized use or disclosure of personal information, government institutions must notify the affected individual(s) if the "incident creates a real risk of significant harm" (*Guide to FOIP*, Ch. 6, p. 268).

[27] Section 29.1 of FOIP states:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[28] Even where section 29.1 of FOIP does not apply, unless there is a compelling reason not to, government institutions should always notify affected individuals of a privacy breach.

[29] Immigration stated that the 23 affected parties it initially identified were notified on February 7, 2023. Five additional affected parties were notified on February 21, 2023. In its submission, Immigration undertook to advise my office if additional affected parties are discovered during its ongoing investigation. It also undertook to notify these affected parties. It added that the Immigration Services Branch will provide the CPAO with any

updates on the affected parties on a monthly basis. As of the date of this Investigation Report, an additional 12 affected parties have been discovered and Immigration is in the process of notifying these additional affected parties.

[30] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. Government institutions may also want to notify organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[31] A notice to affected individual(s) should include:

- A description of the breach (a general description of what happened)
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.)
- A description of possible types of harm that may come to the affected individual because of the privacy breach
- Steps taken and planned to mitigate the harm and prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies)
- Contact information of an individual within the organization who can answer questions and provide information
- A notice that individuals have a right to complain to the IPC (provide contact information)
- Recognition of the impacts of the breach on affected individuals and, an apology

(*Guide to FOIP*, Ch 6, pp. 274-275)

[32] Immigration provided my office with a copy of its notification letter. It did not include a warning about the risk of identity theft. This warning should have been included given that Immigration's own "Internal Privacy Breach Incident Report" stated that the personal information involved included "more than enough information to assume someone's identity." In these circumstances, the notice to the affected parties who are at risk of identity

theft should have informed them that this was a risk and set out the actions they could take to address it.

[33] In the previous reports where identity theft has been a risk, such as my office's Investigation Report 370-2021, I have found government institutions should also offer affected parties credit monitoring for a minimum of five years.

[34] As noted above, the notification to affected parties was sent in February 2023. This was approximately nine months after receiving a complaint about a potential breach and over five months following the completion of the internal investigation report which concluded that there had been a breach of privacy. Immigration states that it was concerned about how notification of the CPAO and the affected parties might impact a potential criminal investigation. Even if that were the case, it is not clear why the notification was not sent after the CPAO became involved in the investigation in November. The delays in notifying the affected parties in this case are not reasonable.

[35] For the reasons set out above, I find that Immigration's notice to the affected parties was not adequate.

[36] I recommend that in the future, Immigration ensure that it notifies affected parties at the earliest opportunity following discovery of a breach. I recommend that in the future, Immigration ensure that its notification letters address the risk of identity theft where the nature of the personal information involved, and other circumstances raise such a risk. I also recommend that, within 30 days, Immigration offer five years of credit monitoring to those affected parties who may be at risk of identity theft.

Investigation of the breach

[37] After containing the breach and notifying affected parties, government institutions should conduct an internal investigation. An internal investigation is a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents. The purpose is to conduct a root cause analysis, which is a useful process for

understanding and solving a problem, and to identify measures necessary to prevent further similar breaches. It seeks to identify the origin of a problem by using a specific set of steps and tools to:

- determine what happened
- determined why it happened
- figure out what to do to reduce the likelihood that it will happen again.

(*Guide to FOIP*, Ch. 6, pp. 269-271)

[38] Immigration's investigation into this matter determined that in 2020, allegations of inappropriate access to Immigration's systems were made against the employee. According to Immigration's submission, the 2020 allegations were not substantiated, but the employee was reminded about the access rules at that time. Immigration asserted:

> [They] had been warned not to [access files without authority] to do so, as there had been allegations against [them] in 2020. The 2020 investigation did not meet the test to show that [they] had accessed these files improperly at that time, but the message was delivered that this was not an allowable action.

[39] Following is a timeline of key events in Immigration's second investigation involving this employee:

> January 2021 – Immigration's internal investigation into the employee's workplace activities commenced. The circumstances of this investigation were not provided to this office.
>
> April 26, 2022 – Immigration's client made a complaint about the employee's use and sharing of personal information with the recipient.
>
> April 29, 2022 – Immigration ordered an audit report on the employee's access to the OASIS system which revealed "unusual activity" by the employee.
>
> June 15, 2022 – employee went on vacation leave.
>
> June 22, 2022 – independent investigator was retained given the serious nature of the allegations made on April 26, 2022.
>
> June 28, 2022 – Immigration received another complaint from an outside organization alleging that the employee was involved in an immigration scheme.

> July 11, 2022 – Immigration ordered another audit report described as a "special vendor report" for the employee's activities on July 11, 2022. The report revealed inappropriate access to the OASIS system.
>
> July 12, 2022 – employee returned to work and was assigned to a special project that would not require access to client files. However, the employee's access rights to OASIS were not terminated.
>
> July 26, 2022 – employee's access rights to the OASIS system were terminated.
>
> August 8, 2022 – employee resigned.
>
> August 22, 2022 – independent investigator released their report. The report found that the employee had inappropriately accessed personal information.
>
> August 22, 2022 to November 21, 2022 – Immigration reviewed the report and audit reports and identified 28 files for further investigation – 17 of which were not assigned to the employee and 11 were. It concluded that the employee had accessed client files when they were not authorized to be working such as after working hours and when on vacation.

[40] During its investigation, Immigration also determined that the employee had received the following training that involved privacy:

- Ministry of Social Services Practical Privacy Training – August 3, 2017
- Ministry of Social Services Code of Conduct Training – June 1, 2018
- Access & Privacy (Ministry of Justice and Attorney General module) – October 30, 2018
- *The Freedom of Information and Protection of Privacy Act* – May 13, 2020

[41] As to the root cause of the breach, Immigration asserted:

> The root cause of the breach is challenging to determine. We have our suspicions that the employee or a known associate may have had criminal intent, but as that investigation is ongoing at this time, we cannot state that with sense of certainty.
>
> The employee was aware that their use of OASIS could be tracked […], and yet still chose to access the system and the files without a business-related reason.

> The reasons given during the fact-finding meetings for [their] accessing these files did not make sense, especially given that [they] had been investigated in 2020 and [were] advised at that time that [they were] not to review files that were not assigned to [them].
>
> …
> Hubris is the only root cause that can be determined at this time, as [they] did not believe [they] would be caught.

[42] It is apparent that the employee was aware that the relevant accesses to OASIS were not authorized. Therefore, the root cause of this privacy breach was the failure of the employee to comply with existing policy. The other circumstances suggest that the employee may have been motivated by criminal intent and the desire for financial gain.

[43] Regarding the factors that contributed to the breach, Immigration asserted:

> Pandemic protocols – many protocols that were instituted during COVID still exist. For example, staff take their computers home with them each evening and on weekends, just in case they are ill the next day and have to work from home rather than coming to the office and getting others sick. This is a protocol that is in place in most government offices and will likely continue, as it protects the health of employees and ensures business continuity. Many of the accesses that were covered in the employee investigation (Appendix C) happened after hours or while the employee was on vacation.
>
> Lack of proactive audits – up until recently, the branch did not have the ability to run audit reports themselves. In order to have an audit run, they had to get the vendor to run a special report at a cost to the ministry. Proactive audits would have been cost prohibitive. Now that the management team in the branch has the ability to run these reports themselves, this is no longer an issue.

[44] I agree with Immigration's conclusion that the lack of proactive auditing by Immigration may have contributed to the breach. I will discuss that in more detail below. As I said in my office's Investigation Report 197-2022, 215-2022:

> Proactive random audits are an important measure to protect privacy of personal information and personal health information. Managed properly random audits can be effective in detecting and deterring privacy breaches.

[45] It appears that Immigration did a thorough investigation and understood the relevant factors. I add that its failure to involve the CPAO in the investigation process at the earliest opportunity was a breach of its own policy and best practices for breach response. If

Immigration had involved the CPAO as soon as possible, measures to contain the breach and notify affected parties may have been taken sooner. While I cannot conclude that involving the CPAO would have impacted the decisions made about containment and notification and the outcome of Immigration's investigation, as a best practice, Immigration staff should notify the CPAO of all potential breaches at the earliest opportunity.

[46] I find that Immigration's investigation did not comply with its own policy and best practices because it did not involve the CPAO at the earliest opportunity. To address this, I have already recommended above that Immigration take steps to help ensure that its staff are informed of the obligation to report all potential privacy breaches to the CPAO as soon as possible.

[47] I understand that Immigration's investigation into this incident is ongoing. I recommend that Immigration complete the investigation.

[48] I now turn to consider if Immigration has taken appropriate steps to prevent further breaches of this nature.

Take appropriate steps to prevent future breaches

[49] Once government institutions contain a breach and identify a root cause, they should consider and implement solutions that help prevent the same type of breach from occurring again. Prevention is one of the most important steps. A privacy breach cannot be undone but a government institution can learn from one and take steps to help ensure that it does not happen in the future. To avoid future breaches, government institutions should make a prevention plan.

[50] As noted above, Immigration identified a number of steps it would take to prevent future breaches.

[51] First, it identified the need for further privacy training. It provided additional privacy training to all staff in January and February 2023. It also begun updating all training manuals to include privacy notices at the beginning of each module. Immigration's CPAO has also identified a need for specific training regarding snooping for all staff who have access to personal information. This training will be delivered in the fall of 2023 and will be made available for all new staff. The CPAO has recommended that the snooping training be offered annually and be made mandatory.

[52] Privacy training and privacy awareness raising activities are important administrative safeguards. They are particularly important in cases where employees have access to vast amounts of personal information through electronic information management systems. Training and awareness raising programs should inform employees that inappropriate uses and disclosures of personal information will not be tolerated. They should also inform employees about the disciplinary actions that will be taken to address breaches involving these activities.

[53] This is consistent with my office's *Privacy Breach Guidelines* which states that annual privacy training that addresses duties under FOIP, existing safeguards, the need-to-know principle and the consequences for violating FOIP is a best practice. I recommend that, within 30 days, Immigration implement a policy requiring that privacy training, and the proposed training on snooping, be provided as soon as possible after a new employee is hired and is refreshed annually thereafter. I also recommend that Immigration's privacy training include information about the disciplinary actions that it will take when snooping is discovered.

[54] With respect to its technical safeguards, Immigration has developed a "Risk Management Action Plan" which includes system changes to help ensure that staff only have access to the information they require for their work. This is often described as role-based access controls.

[55] Management staff are currently conducting proactive audits on an ad hoc basis. Immigration is developing a formal audit plan that will be implemented as soon as it is

approved. The details of the plan were not provided to our office except that audit reports will track staff changes in OASIS and when staff view a record.

[56] Immigration added that many of the service requests that have been made with its information management service provider, will take time to implement in part because they can only be implemented when the system is offline. The reason for this is to ensure the integrity of the system and that client services are not interrupted.

[57] In its submission, Immigration asserted:

> Finally, all new systems created for ICT that have personal information or personal health information will have an automatic recommendation for mandatory, random, proactive audits to be completed on a regular basis, and that views of client records will be records as part of the audits. Existing systems that do not have this capability will also receive the same recommendation to be implemented when upgrades are required, if it is possible.

[58] The proposed steps to be taken by Immigration to prevent future breaches are appropriate. Auditing of electronic information systems is particularly important in ensuring that the privacy of individuals and the confidentiality of personal information are protected. Audits are essential technical safeguards for electronic information systems. They can be used to deter and detect unauthorized collections, uses and disclosures of personal information.

[59] As I said in my office's Investigation Report 088-2022:

> Auditing is a technical safeguard and is necessary to assess compliance with policies, procedures, and legislation. With respect to random audits, my office's *Auditing and Monitoring Guidelines for Trustees*, which also apply to government institutions, states:
>
> > Random audits should be used by the trustee to ensure user compliance with provincial and federal legislation, joint services and access policies (JSAP) and with the trustee's internal privacy and security policies. It is the trustee's responsibility to establish a process for conducting random audits of user activity.

[60] This is not the first time that Immigration's OASIS system has experienced a breach involving snooping. In Investigation Report 216-2018, 218-2018, my office investigated a complaint about snooping and the OASIS system. While the circumstances of that breach

were different, Immigration needs to take steps to ensure that snooping does not become a systemic problem.

[61] In developing its auditing program, Immigration should ensure that the program is transparent. It should advise staff about the program and the fact that it will occur without notice to employees.

[62] I recommend that, within 30 days of the issuance of this Investigation Report, Immigration confirm to my office its intention to complete and implement the proposed technical changes described in paragraphs [58] to [61] above.

[63] Finally, in its submission, Immigration stated that it is considering referring this case to Public Prosecutions to determine if pursuing charges under FOIP would be appropriate. Given the nature of the allegations made against the employee in this matter, if it has not already done so, I recommend that Immigration forward its investigation file, including the internal investigation, to the Ministry of Justice and Attorney General, Public Prosecutions Division. This would allow prosecutors to consider whether an offence under FOIP has occurred and if charges should be laid under that act or any other statute.

III FINDINGS

[64] I find that I have jurisdiction to investigate this matter under FOIP.

[65] I find that Immigration did not take appropriate and timely action to contain the breach.

[66] I find that Immigration's notice to the affected parties was not adequate.

[67] I find that Immigration's investigation was not adequate.

[68] I find that Immigration has appropriately identified steps to be taken to prevent further breaches of this nature.

IV RECOMMENDATIONS

[69] I recommend that, in the future, Immigration should notify its privacy staff as soon as possible after becoming aware of a potential breach of privacy.

[70] I recommend that, in the future, Immigration ensure that it notifies affected parties at the earliest opportunity following discovery of a breach.

[71] I recommend that in the future, Immigration ensure that its notification letters address the risk of identity theft where the nature of the personal information involved, and other circumstances raise such a risk.

[72] I recommend that, within 30 days of issuance of this Investigation Report, Immigration offer five years of credit monitoring to those affected parties who may be at risk of identity theft.

[73] I recommend that, within 30 days of the issuance of this Investigation Report, Immigration confirm to my office its plan to complete the investigation in this privacy breach in a timely fashion.

[74] I recommend that, within 30 days of issuance of this Investigation Report, Immigration implement a policy requiring that privacy training, and the proposed training on snooping, be provided as soon as possible after a new employee is hired and is refreshed annually thereafter.

[75] I recommend that Immigration's privacy training include information about the disciplinary actions that it will take when snooping is discovered.

[76] I recommend that, within 30 days of issuance of this Investigation Report, Immigration confirm to my office its intention to complete and implement the proposed technical changes described in paragraphs [58] to [61] above.

[77] I recommend that, within 30 days of issuance of this Investigation Report, Immigration forward its investigation file, including the internal investigation, to the Ministry of Justice and Attorney General, Public Prosecutions Division, if it has not already done so.

Dated at Regina, in the Province of Saskatchewan, this 31st day of May, 2023.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner