Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 099-2025

Ministry of Justice and Attorney General

June 10, 2026

Summary: The Ministry of Justice and Attorney General (Justice) proactively reported a privacy breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). A privacy breach occurred when an Administrative Assistant took screenshots of an individual's criminal history from the Criminal Justice Information Management System (CJIMS) database, printed the screenshots from a computer terminal and then provided this information to a member of the public. The screenshot printout included the Complainant's young offender information and the Complainant's past record of criminal and driving convictions.

OIPC advised Justice that an investigation would occur pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act* (*FOIP*) and that an Investigation Report would be issued.

OIPC made the following findings:

(1) Personal information was involved pursuant to sections 24(1)(a), (b) and (k)(i) of *FOIP*.

(2) The disclosure in this case was not authorized.

(3) While Justice took steps to contain the breach, it has not provided evidence that it took sufficient efforts to contain this breach. Justice could have made further attempts to ensure the records were recovered and/or destroyed.

(4) Justice did not notify the Complainant that there was a real risk of significant harm in accordance with section 29.1 of *FOIP*.

(5) Justice's investigation was incomplete as it did not interview the employees serving the front desk at RPC at the time of the breach.

The Commissioner recommended that Justice commit to the speedy implementation of all four of its suggested actions outlined at paragraph [49] of this Investigation Report.

I BACKGROUND

[1] On June 7, 2024, the Complainant[1] contacted the Privacy Unit of the Ministry of Justice and Attorney General (Justice). The Complainant reported that their ex-partner was in possession of two Criminal Justice Information Management System (CJIMS) screenshots containing their personal information. The screenshots in question included a summary of the Complainant's involvement with the criminal justice system, including young offender history. The ex-partner received the screenshots from a family member (the Recipient), who obtained the screenshots from a Court Administrative Assistant (Administrative Assistant) at the Regina Provincial Court House (RPC). At the material time, the Administrative Assistant was an employee of Justice. [2]

[2] CJIMS is an online database owned and operated by the Saskatchewan Ministries of Community Safety and Justice. This database contains current and historical information with respect to accused people and convicted offenders involved in the criminal justice system in Saskatchewan and can include access to records of prior criminal involvement, charges that have been laid by the police, court dates, fine payment history and other information of this nature.

[3] On May 6, 2025, Justice proactively reported this breach to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

[4] By letter dated May 7, 2025, Justice provided the Complainant with a summary of the incident and findings. Justice acknowledged that a privacy breach occurred when the

[1] The Complainant filed a complaint with Justice but not with this office.

[2] Section 2(1)(b.1) of *FOIP* defines an "employee of a government institution" as an individual employed by the government institution including those retained under contract to provide services to the government institution.

Administrative Assistant took screenshots of the Complainant's criminal history information from the CJIMS database and downloaded it onto a courthouse computer terminal and then printed it out. The printed screenshots were provided to the Recipient. The printed screenshots contained the Complainant's "name, date of birth, and previous involvement with the criminal justice system." Justice conceded the privacy breach and advised the Complainant of the statutory right to contact this office to register a complaint.

[5] On June 16, 2025, OIPC notified Justice that an investigation would be commenced pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act* (*FOIP*).[3]

[6] On July 2, 2025, Justice provided OIPC with a copy of its internal investigation report.

[7] On January 27, 2026, OIPC notified Justice that an Investigation Report would be issued.

[8] Between March 24th and March 26th 2026, there were ongoing discussions between this office and Justice as to the nature and scope of this privacy breach and whether or not the Administrative Assistant should be named. Justice requested the opportunity to file supplemental submissions. This office granted Justice that opportunity and on May 7, 2026, Justice filed further submissions with this office.

[9] Justice submitted that the Administrative Assistant did not wilfully violate government privacy policy, training and guidelines because in the course of its investigation, Justice discovered an unwarranted practice in effect at the RPC which has now been corrected. While this privacy breach is indeed grave, we have accepted Justice's submissions and we commend Justice for its quick intervention and commitment to the privacy of the people of Saskatchewan.

[3] *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01, as amended.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

[10] Justice qualifies as a "government institution" pursuant to section 2(1)(d)(i) of *FOIP*. Therefore, OIPC has jurisdiction to undertake this investigation pursuant to PART VII of *FOIP*.

2. Did a privacy breach occur?

[11] The first determination in assessing a breach is to decide whether personal information is at issue. Section 24(1) of *FOIP* provides a non-exhaustive list of the type of information that qualifies as personal information. Personal information is information that is about an identifiable individual, and that is personal in nature. Information is about an *identifiable individual* if the individual can be identified from the information itself. Information is *personal in nature* if the information reveals something personal about the identifiable individual.[4]

[12] Justice explained that the Administrative Assistant created screenshots of the Complainant's file information in CJIMS and then downloaded the screenshots onto a courthouse computer terminal and printed from that terminal. This occurred because the CJIMS terminals do not allow for direct printing.[5] This alone must serve as a red flag that the information on CJIMS is not to be widely disseminated.

[13] Having downloaded the screenshots and after printing this information, the Administrative Assistant handed the screenshot printouts directly to the Recipient. The screenshots contained the Complainant's full name, date of birth, charge status, information on offence,

[4] OIPC Review Report 005-2025 at paragraph [33].

[5] Justice explained it with these words: "CJIMS functionality does not allow direct printing from the system".

information number, number of counts, *Criminal Code*[6] offence provisions, CJIMS result code, location of proceedings and docket date/time.[7] These data elements all qualify as the Complainant's personal information pursuant to sections 24(1)(a), (b) and (k)(i) of *FOIP*:

> **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;
>
> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[14] A *FOIP* privacy breach involves the unauthorized collection, use or disclosure of an individual's personal information that is in the possession of, or under the control of, a government institution.[8]

[15] *FOIP* does not define "disclosure", but OIPC has defined it as the sharing of personal information with a separate entity that is not a division or branch of the government institution.[9] In this matter, the Administrative Assistant gave the printed copies of the

[6] *Criminal Code*, RSC 1985, c. C-46, as amended.

[7] OIPC Investigation Report 088-2022 discussed at paragraphs [6] and [7] that date of birth and information about criminal history qualify as personal information under sections 23(1)(a), (b) and (k)(i) of *FOIP*.

[8] *Possession* means having physical possession over a record plus a measure of control over it. *Control* means having the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. OIPC Investigation Report 017-2019 at paragraph [8].

[9] OIPC Investigation Report 041-2021 at paragraph [15].

CJIMS screenshots to the Recipient who was external to Justice. Because the impugned disclosure was made to an individual external to Justice, it qualifies as a disclosure of the Complainant's personal information.

[16] Section 29(1) of *FOIP* states that a government institution cannot disclose personal information in its possession or under its control without the authorization or consent of the individual concerned:

> **29**(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30

[17] Justice provided this office with a copy of the 2024 Courts of Saskatchewan resource entitled *Public Access to Court Records in Saskatchewan: Guidelines for the Media and Public* (*Guidelines*).[10] The *Guidelines* inform Court Services staff (courthouse employees including the Administrative Assistant in this case), how to respond to requests for access to information from members of the public. The purpose of the *Guidelines* is to enhance consistency and to honour the "principle of court openness", while at the same time providing strict instructions on how to guard private information. The *Guidelines* apply to the three levels of court in Saskatchewan: the Court of Appeal, the Court of King's Bench and the Provincial Court. A "court record" is defined in the *Guidelines* as:

> …a document, information or other thing that is collected, received or maintained by a court in connection with a judicial proceeding. Records relating to case management or records generated for other internal court purposes are not considered court records.

[18] According to section 2(2)(c) of *FOIP,* Saskatchewan courts are not "government institutions". However, the printed screenshots were taken from CJIMS. Since Justice is a joint owner and manager of CJIMS, and since Justice is a government institution subject to *FOIP*, the information that formed the basis of the screenshots was in the possession and control of Justice.

[10] *Public Access to Court Records in Saskatchewan: Guidelines for the Media and the Public*.

[19] The *Guidelines* explain that the entire purpose of CJIMS is to serve as a tracking system. The *Guidelines* warn that CJIMS may contain errors and omissions and cannot be relied upon as a source of valid information. A further caution is given to the effect that the information on the CJIMS database may be subject to a court ordered publication ban but this may not be reflected in the records on CJIMS. A court official using CJIMS should always confirm the CJIMS information with the actual court file. The following are the cautions provided when searching for records or information on CJIMS:[11]

> Q: Can CJIMS be used to search for information or records in order to respond to an access request?
>
> A: While CJIMS may be used to assist the court official in locating a file, it is not a court record but rather a tracking system. As a result, it may contain errors and omissions and should not be relied on as the source of information. It may be used to locate a file but the court official must confirm the information with the court file. In some instances, an Information may be entered electronically before the document is filed in Court. *No information shall be provided from the database in these situations, until the necessary documents have been filed with the Court.* In addition, caution should be used with CJIMS searches as the existence of a publication ban may not be readily evident. Printouts from CJIMS shall not be distributed outside the court offices.
>
> [Emphasis added]

[20] The screenshots that constitute the unauthorized disclosure in this matter included, among other things, a list of the Complainant's offences under *The Traffic Safety Act.*[12] A commercial driver abstract reveals all collisions, convictions and commercial vehicle safety inspections with respect to a driver in Saskatchewan and is maintained by Saskatchewan Government Insurance (SGI). Driver's abstracts are not publicly available in Saskatchewan. SGI requires proper authorization from a Saskatchewan driver prior to the release of these records.[13] There was no authorization for release of these records in this matter.

---

[11] *Ibid,* Appendix A, at p. 38 (F. Process – Using CJIMS to Search for Records or Information).

[12] *The Traffic Safety Act,* SS 2004, c. T-18.1, as amended.

[13] SGI website: *Driver records and abstracts*.

[21] The screenshot disclosures also included information with respect to the Complainant's young offender record. Part VI of the *Youth Criminal Justice Act* (*YCJA*) [14] strictly forbids the publication of the identity of a young person. The legislative scheme provides a monitored and controlled regime for the protection of the privacy and identity of young persons and outlines very limited circumstances for the dissemination of records. Section 118 of the *YCJA* mandates that, except as authorized or required by the Act, no person shall be given access to a record kept pursuant to the Act and no information contained within a record may be given to any person where to do so would identify the young person to whom the record relates. Section 138 of the *YCJA* outlines substantial penalties for disclosure without authorization in contravention of Part VI. This includes the risk of incarceration if the offence is proceeded with by indictment.

[22] The Complainant in this matter was charged pursuant to the now repealed *Young Offenders Act.* [15] Nonetheless, the disclosure provisions of the current legislation apply retroactively to the earlier legislation by virtue of section 163 of the current *YCJA*. [16]

[23] In conclusion, CJIMS contains the criminal history information of individuals, and information from many other sources such as the *YCJA* and driving history as in this case. The information on CJIMS is in the possession and control of Justice. The Administrative Assistant did not have authority under *FOIP* to disclose the Complainant's personal information. This office agrees with Justice's conclusion that a privacy breach occurred.

3. Justice's response to the privacy breach

[24] The following determinants measure how effectively a government institution managed a privacy breach: [17]

[14] *Youth Criminal Justice Act*, SC 2002, c 1, as amended.

[15] *Young Offenders Act,* RSC 1985, c. Y-1. Repealed by SC 2002, c. 1, s.199.

[16] OIPC Review Report 055-2025 at paragraph [12].

[17] OIPC Investigation Report 155-2025 at paragraph [38].

(a) Containment of the breach as soon as possible;

(b) Notification of affected individuals;

(c) Investigation of the breach; and

(d) The adoption of preventative measures.

a. Containment of the Breach

[25] To contain a breach means to reduce its magnitude, thereby reducing the risk to the affected party. This office applies a standard of reasonableness to assess containment efforts. Privacy breaches are serious matters that result in a loss of faith and trust on the part of the public in the government institution.[18] Relevant steps to contain a breach include stopping the unauthorized practice, recovering the records and revoking/suspending access privileges pending the outcome of an investigation.[19]

[26] On August 15, 2024, Justice retrieved the CJIMS printed screenshots from the Recipient. This was two months after the breach was reported by the Complainant. The Recipient should have been contacted immediately and asked to return the printed screenshots upon notification of the breach.

[27] The ex-partner of the Complainant admitted that the printout was shared with others. Justice confirms that the extent of the disclosure is unknown. This presents a disturbing and real possibility of further dissemination. This set of facts called for strict measures to ensure the destruction and/or the return of the impugned information at the moment of notification. Containment in a matter like this is difficult, but Justice has not provided evidence that it took sufficient efforts to contain this breach.

[18] OIPC Investigation Report 033-2025 at paragraph [23]. "Reasonable" means fair, proper or moderate under the circumstances or sensible (OIPC Review Report 152-2021 at paragraph [55]).

[19] *Supra* footnote 16 at paragraph [41].

b. Notification of Affected Individuals

[28] A government institution should notify an affected individual of a privacy breach as soon as possible after the breach. In this case, it was the Complainant who discovered the breach and complained to Justice on June 7, 2024. On May 7, 2025, Justice provided the Complainant with a letter that included a summary of the incident and Justice's conclusory findings from the internal investigation. The letter offered the Complainant an apology and explained the prevention plan that had been put in place at RPC. Justice correctly provided the contact information for this office and advised the Complainant of the right to file a complaint. These are the elements of a proper notice, but there was one important omission.

[29] In its written submissions, Justice identified a "real risk of significant harm" resulting from this disclosure of the Complainant's personal information. Justice further acknowledged that there was a "potential for reputational, emotional, and legal harm to the Complainant", and assessed the risk as "high". These concessions were made to OIPC but not to the Complainant. The Complainant should have been advised of future possible harms and advised of any risk-mitigating steps that could be taken.[20] Full disclosure and notice is required by section 29.1 of *FOIP*:

> **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.

[30] Justice fell short of its required statutory notification duties because it did not include this information in the letter to the Complainant when it reported on the conclusions of its internal investigation.

[20] *Supra,* footnote 16 at paragraph [47]. See also OIPC Investigation Report 168-2025 at paragraph [31].

c. Investigation of the Breach

[31] An investigation must assess a privacy breach on a systemic basis and should include a root cause analysis and conclusion. Identifying the root and contributing cause of a breach will assist a government institution to take future, preventative measures over the current measures that have fallen short. A government institution's "duty to protect" under section 24.1 of *FOIP* requires that policies and procedures are in place to maintain administrative, technical and physical safeguards:[21]

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[32] We will only consider administrative and technical safeguards as physical safeguards are irrelevant to the assessment of this breach.

[33] The *Guidelines* were referenced earlier this Investigation Report. They are the primary source of guidance for Court Services staff when they handle a request for court records.

[21] OIPC Investigation Report 009-2025 at paragraphs [45] to [47]. Examples of administrative safeguards include policies, procedures, confidentiality statements. Technical safeguards include measures like access controls (e.g., passwords or access to a system). Physical safeguard are measures like locked cabinets or drawers.

The *Guidelines* outline the types of information or records to which access is limited, denied or allowed.

[34] The *Guidelines* describe the various ways an access request to the public may be facilitated. They outline in detail the legal limitations on access to information for civil law matters, criminal law matters, youth criminal proceedings and family law matters. The *Guidelines* explain various practical considerations but the following warning against the unilateral provision of court records to the public is clear:[22]

> **Role of local court staff**
> On a day-to-day basis, there are practical considerations that will affect how quickly court officials can provide access to information on court files. The primary responsibility of court officials is to ensure that court operations run smoothly and the administration of justice is carried out. The secondary responsibility is to perform related tasks, such as providing information pursuant to these guidelines. The primary service delivered by a court is the resolution of disputes. Responding to public access requests must not unduly impact the ability of court officials to provide the services necessary to maintain court operations.
>
> As well, it is important to note that there are limitations on the assistance that court officials can provide in relation to an access request. Specifically, court officials:
>
> - will not interpret or analyze information about court proceedings;
> - will not recount the submissions made in court for anyone who did not attend court personally;
> - *will not search files to locate specific items on anyone's behalf*; and
> - cannot ensure that the information provided relates to a particular person in the community (the responsibility for determining the accuracy of connections or relationships drawn between individuals in the community and individuals named in court documents lies with the person obtaining and using information obtained from court).
>
> [Emphasis added]

[22] *Supra,* footnote 9 at page 9.

[35] The interviews conducted by Justice in this matter revealed that the impugned information was obtained as the result of a request made to a Court Services staff member at the "front desk of the courthouse".

[36] Justice submitted that the *Guidelines* serve to provide procedural direction to courthouse staff and that employees must "ensure compliance with any legal restrictions, including publication bans, and adhere to them "when accessing or using court records." Justice added that it is through training that employees are further warned to be cautious about the type of information released to the public, and to be "vigilant with youth information."

[37] The *Guidelines* provide a five-step process for a proper response to an access request – all of which were ignored by the Administrative Assistant in this case:[23]

> 1. Does a court order exist in the case? If so, the terms of the order supersede these guidelines to the extent that the order and the guidelines conflict. What is the scope of the order? If there is any uncertainty, consult the judge who issued the order.
>
> 2. Is there any restriction in the Rules of Court, applicable legislation, or a Practice Directive, which relates to access that is being requested? If so, what is the scope of the restriction? Is there a separate process set out in that enactment for access to the record being sought?
>
> 3. Do these guidelines provide any specific direction as to how to handle the situation?
>
> 4. Do any of the circumstances exist which would require an application to court to resolve the issue?
>
> 5. If access can be granted, what is the manner (phone, fax, personal pick up) and time frame within which access can be provided, keeping in mind the other court responsibilities that must be carried out, the workload of the particular court office and the amount of material requested?

[38] In addition to the *Guidelines*, Justice provided our office with copies of relevant portions from three documents: *CJIMS Authorized Use and Restrictions Policy*; *CJIMS User*

[23] *Ibid,* Appendix A, at p. 40 (G. Step-by-Step Process for Responding to Requests).

Agreement as well as the Administrative Assistant Job Description – all of which were not followed in this matter:

> **CJIMS Authorized Access, Use and Restrictions Policy and User Agreement** (*CJIMS Policy*)
>
> - *Governance:* The Policy establishes clear rules for accessing and using the system. It defines appropriate purposes and limits disclosure.
>
> - *Access Control*: The Policy limits access to authorized users, requiring all actions to be job-related and restricted to individuals to whom the electronic file relates.
>
> **CJIMS User Agreement**
>
> - *Acknowledgment of Responsibilities*: Employees are required to read and sign the Agreement before accessing the system. The Agreement reinforces the CJIMS Policy and requires users to confirm their understanding of the restrictions on accessing, using, and disclosing information.
>
> **Court Administrative Assistant Job Description**
>
> - The employee's responsibilities are defined, such as referencing the official court record and making decisions within the scope of established Guidelines.

[39] Justice employees who gain access to CJIMS must sign the *CJIMS User Agreement* (agreement). The agreement stipulates that a user's access is in accordance with the *CJIMS Policy.* That policy provides in clear language unauthorized use of CJIMS "may result in an investigation and disciplinary action up to and including dismissal."

[40] In the course of its investigation, Justice discovered a "former" practice at RPC that it warranted has now been rectified. The real culprit in this privacy breach is the fact that somehow over time, CJIMS became a matter of convenience for busy court staff:

> [12] At RPC, members of the public can come to the front desk and request a wide variety of information about individuals who are facing charges. Often such requests relate to next court dates, fine payment, or specific charges laid. These requests are often made by individuals other than the accused person (family members, representatives or agents, counsel), as happened in this case.

> While there are procedures for verifying the identity of individuals and their purposes at the front counter, much of the information is requested informally with individuals requesting the information claiming some relation to, or agent-role on behalf of, an accused. Some of the information is available to the general public.
>
> [13] Much of the information requested is readily found in CJIMS, and less readily within the physical court files. These physical files are sometimes difficult to access in a timely fashion because they are being actively used by provincial court Judges (meaning the files may be inaccessible to Courthouse staff for hours or days at a time). The practice at RPC was to access the relevant page from CJIMS, use the print-screen key, and then print out the pertinent information. Depending on what is printed, and who the information is released to, privacy breaches can occur because of this practice. It is worth noting that this conduct will not inevitably result in a privacy breach.
>
> [14] However, because the print-screening can capture personal information, such as names and CJIMS numbers, this practice has since been amended as described at para 32, below.
>
> [15] It was this course of action which led to this breach. That is to say, it was the process, not individual action, which is the ultimate culprit…

[41] It was acknowledged by Justice that this former practice at RPC was not "in accordance with privacy best practices". The creation of a screen print off CJIMS led to a general assumption amongst staff that information could "be disclosed without lawful authorization." Because of this, Justice claimed that the real cause of this breach was a failure to provide adequate privacy training to employees and that employees were perhaps not "given the tools to recognize when there may be a practice that conflicts with privacy."

[42] Justice conducted three interviews in connection with its investigation of this matter. Justice interviewed the Recipient, the Complainant and a third party who was a family member of the Recipient. Justice concluded that interviews of the staff serving the courthouse front desk at the time of this privacy breach would have added no value to the investigation because they determined that this breach was caused by a general non-privacy compliant practice. Finally, Justice explained that an audit of this incident did not result in conclusive evidence identifying the exact employee at fault for the privacy breach. Therefore, Justice submitted that staff interviews would have been worthless.

[43] This office is of the opinion that a thorough investigation would have surely involved interviews of the staff serving at the court front desk at the time of the privacy breach. Simply alleging that the privacy breach was the result of a bad overall practice that had evolved amongst the Court Services staff is a surface conclusion. Further detail and insight could have been gained from staff interviews. We see the investigation as being severely lacking in this respect.

d. Preventative Measures Going Forward

[44] A government institution must be proactive in the prevention of privacy breaches – especially an office that deals with highly sensitive information. Preventative measures can include the addition or enhancement of safeguards, the provision of additional staff training, and the monitoring or auditing of data systems on a regular basis.[24]

[45] Nothing is more destructive to public trust as a privacy breach involving someone's criminal and youth court record. On the other hand, the adoption of meaningful preventative measures aways assists in the restoration of trust.

[46] Justice has taken this matter seriously going forward. While the Justice investigation did not lead to a conclusion that the practice of screenshotting and printing from CJIMS was a province-wide issue, it has held meetings with all Justice staff at provincial courthouses to reinforce the proper process of information dissemination to the public. RPC and the other court houses have been instructed to never take screenshots and print from CJIMS except for one instance: when an individual requests their own personal information with respect to traffic violations. In all other instances, staff must follow the procedure as outlined in the *Guidelines*.

[47] These changes may pose a roadblock for the public and may slow public access to court information, but the changes were necessary to ensure privacy.

[24] *Supra,* footnote 16 at paragraphs [70] and [71].

[48] Justice conceded that the audit in this matter was unhelpful. Justice is committed to refining the auditing capabilities of CJIMS going forward. This is a very important goal and we hope that the auditing function is improved not only to assist in identifying future wrongdoers but perhaps to also serve as an warning that violations will no longer remain anonymous.

[49] Justice also committed to the following preventative measures going forward as the result of this privacy breach. Justice will:

1. **Reinforce CJIMS Usage Policies: Court Services employees should be reminded of their responsibilities under the CJIMS Policy, CJIMS User Agreement, and Access to Court Records Guidelines.**

   This reminder must emphasize the following:

   - Employees are strictly prohibited from providing information from CJIMS to the public in any form, including screenshots or copied content, to fulfill court record requests.

   - CJIMS should only be used to locate court records, not to disseminate information to the public. Employees may, however, use CJIMS to provide individuals with their own court documentation.

2. **Develop a Comprehensive Training Module: Court Services should collaborate with the Privacy Unit to create a training module tailored to employees working in court buildings.**

   This module should cover:

   - CJIMS Policy, User Agreement, and Access to Court Records Guidelines;

   - FOIP; and

   - Proper handling of sensitive information, including Youth Criminal Justice Act (YCJA)- protected information.

3. **Implement Interim Annual Training: While the comprehensive training module is under development, Court Services should provide annual training sessions for JAG employees working in courthouses.**

   These sessions should include:

- FOIP;
- CJIMS Policy, User Agreement, and Access to Court Records Guidelines;
- How to handle sensitive information, including YCJA-protected content; and
- The Privacy Refresher Training course.

4. **Introduce Technical Safeguards in CJIMS: Consider implementing technical measures within CJIMS that require users in Court Services to input a reason code when accessing various screens.**

   This measure would:

   - Enhance accountability by ensuring users specify the purpose of access.
   - Require the development of additional codes to cover all permissible access scenarios under the CJIMS framework.

[50] The technical measure discussed in Justice's fourth proposal above is truly imperative to address the breach in this case. All CJIMS users should be required to enter a reason for the access of CJIMS. Such a measure will require users to stop and think about the reason for the access. This is a feature that can be easily implemented into any case management system.[25] Systemically, a measure that requires a stated reason for access will clearly assist in all allegations of an unwarranted privacy breach. Such a measure will also assist with the planned proactive audits of the CJIMS system.

[51] We commend Justice for the measures it has taken to date and for those it commits to in the future. These corrective measures are reasonable and will address the breach that occurred and prevent a similar breach in the future.

IV FINDINGS

[52] OIPC has jurisdiction to conduct this investigation under PART VII of *FOIP*.

[25] OIPC Investigation Report 123-2025 at paragraphs [50] to [53].

[53] Personal information was involved pursuant to sections 24(1)(a), (b) and (k)(i) of *FOIP*.

[54] The disclosure in this case was not authorized.

[55] While Justice took steps to contain the breach, it has not provided evidence that it took sufficient efforts to contain the breach. Justice could have made further attempts to ensure the records were recovered and/or destroyed.

[56] Justice did not notify the Complainant that there was a real risk of significant harm in accordance with section 29.1 of *FOIP*.

[57] Justice's investigation was incomplete because it did not interview the employees who were serving at the front desk at RPC at the time of the breach.

V RECOMMENDATION

[58] I recommend that Justice commit to the speedy implementation of all four of its suggested actions outlined at paragraph [49] of this Investigation Report.

Dated at Regina, in the Province of Saskatchewan, this 10th day of June, 2026.

Grace Hession David
Saskatchewan Information and Privacy Commissioner