Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 189-2016

Saskatchewan Government Insurance

September 27, 2016

Summary: Saskatchewan Government Insurance (SGI) proactively reported a breach involving its Auto Fund Database (SAM). An employee of an Issuer, Hometown Insurance Brokers in Vonda, Saskatchewan, had been making unauthorized accesses of personal information in SAM since 1995. The Commissioner raised concerns about SGI's response to this breach, the safeguards in place to protect the personal information in SAM and its monitoring and auditing programs. He made some recommendations to address his concerns including implementing data sharing agreements.

I BACKGROUND

[1] On July 28, 2016, Saskatchewan Government Insurance (SGI) advised my office of a privacy breach as follows:

> …this is to advise that SGI has discovered a privacy concern with a licence *(license)* issuer's employee in Vonda Saskatchewan. It has come to the attention of SGI that this individual has looked up information on SGI's data base without a legitimate business reason. SGI is in the process of handling the privacy concerns and will provide your office with a copy of our breach report when this matter has been finalized.

[2] My office notified SGI of our intention to undertake a privacy breach investigation on the same day.

[3] I note that this is the third and most egregious Report I have written involving unauthorized accesses to SGI's Auto Fund database (SAM) by an Issuer in one year.

II DISCUSSION OF THE ISSUES

1. Was there personal information involved in this matter?

[4] SGI informed my office that the employee of the Hometown Insurance Brokers in Vonda had inappropriately accessed the information of 1,417 individuals through SAM between the dates of July 19, 2015 to July 19, 2016.

[5] SGI indicated that the information to which the employee had accessed included customer number, customer photograph, customer name, address, date of birth, height, eye colour and email address if provided.

[6] These data elements all qualify as personal information pursuant to subsection 24(1) of *The Freedom of Information and Protection of Privacy Act* (FOIP). The relevant portions of the definition are 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.

2. How does FOIP apply in this situation?

[7] SGI is a "government institution" as defined in subsection 2(1)(d)(ii) of FOIP.

[8] Subsection 29(1) of FOIP states:

> **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.

[9] Hometown Insurance Brokers is a private business in Saskatchewan that is not subject to FOIP. Therefore, my office has no jurisdiction over Hometown Insurance Brokers. According to SGI, Hometown Insurance Brokers is a license issuer under contract with SGI to provide driver licensing and vehicle registration services to the public. Hometown Insurance Brokers acts as an agent for SGI. The relationship is governed by contract. SGI has ultimate control over which companies it allows as agents and how SAM is used.

[10] The information in SAM is both in the possession and under the control of SGI. SGI has a responsibility to ensure protection of this personal information.

3. Did SGI follow best practices in its response to this privacy breach?

[11] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the public body has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that SGI took the privacy breach seriously and appropriately addressed it. My office's resource, *Privacy Breach Guidelines*, recommends four best practice steps be taken by public bodies when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach; and
4. Plan for prevention.

[12] I will use these steps to assess SGI's response to the breach.

Best Practice Step 1: Contain the breach

[13] Upon learning that a privacy breach has occurred, public bodies 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 privileges; or
- Correcting weaknesses in physical security.

[14] On July 11, 2016, SGI was initially made aware of a concern with the employee's access to SAM as a result of "an internally raised privacy concern". SGI discovered a suspicious access to SAM at 18:41 on June 1, 2016. On July 19, 2016, after further investigation, SGI discovered that the employee had made 58 "non-transactional" accesses to personal information in SAM between 17:38 and 18:44 on June 1, 2016. It also discovered that the employee had accessed the personal information of approximately 1,900 individuals in the six month period beginning January 1, 2016.

[15] On the same day that it discovered the magnitude of the breach, SGI notified Hometown Insurance Brokers of the situation and suspended the employee's access to SAM. The employee is now permanently suspended from SAM and cannot operate as a licence issuer. It took appropriate steps to contain the breach.

Best Practice Step 2: Notify affected individuals and/or appropriate organizations

[16] Notifying an individual that their personal information has been inappropriately accessed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate access. Unless there is a compelling reason not to, public bodies should always notify affected individuals.

[17] In addition to notifying individuals, public bodies may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[18] SGI determined that notification should be given because "Customer Numbers can be used in the commission of identity theft." However, during its investigation, the employee told SGI that she had been making unauthorized accesses of personal information in SAM since 1995. SGI only notified the individual's whose personal information was accessed from July 19, 2015 to July 19, 2016. This amounted to 1,417 individuals in this year long period. Because it determined "there was little to no risk to the customer" SGI "made a decision to only send letters to those impact[ed] only 1 year back". I recommend that SGI notify those affected for at least two years.

[19] Reminders were also sent to all Issuers about privacy best practices with respect to SAM.

Best Practice Step 3: Investigate the breach

[20] Once the breach has been contained and appropriate notification has occurred, the public body should conduct an internal investigation. The investigation is generally conducted by the public body's Privacy Officer because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the public body should have a solid grasp on what occurred.

[21] According to SGI's internal privacy breach investigation report a number of steps were taken during its investigation. This included, running an audit report to determine which individuals were affected and conducting interviews at Hometown Insurance Brokers, including the employee in question.

[22] SGI advised that the employee indicated that she had received privacy training and knew that it was wrong to snoop into the personal information of others without authorization. She had also signed a Confidentiality and Non-Disclosure Agreement. The employee indicated that she didn't think she'd get caught as she did not print, disclose or save the personal information.

[23] In its internal investigation report, SGI has demonstrated that it has taken reasonable steps to investigate this breach and ascertain all of the relevant facts.

Best Practice Step 4: Plan for prevention

[24] The final step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the public body during the investigation phase such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the public body can learn from it and improve.

[25] As noted, this is the third report I have written in the past year about unauthorized accesses to personal information in SAM by insurance issuers. My office has also issued two other reports about snooping in this database, one by a Ministry of Highways employee and one by an employee of SGI. Before I assess SGI's plan for prevention in this case, I will review past recommendations that have been made to address this issue.

- In 2013, my office recommended that SGI develop auditing and monitoring capabilities in SAM.
- I recommended that SGI find a solution that would enable it to determine with more certainty employee's accesses are for legitimate business purposes.

- I recommended that the Ministry of Justice amend FOIP to include a new section that protects personal information in the possession and/or control of contractors, consultants and information technology specialists which is modeled in part on section 18 of *The Health Information Protection Act*.

[26] SGI committed to the following solutions:

- A system prompt for all non-transaction accesses to the Auto Fund database will be put in place for all Issuer offices in Saskatchewan. The prompt will mandate users to identify the reason for their access before they can enter the database;

- SGI will develop an e-Learning module for license issuers; and

- SGI will develop a program for monitoring (auditing) issuer use of the Auto Fund database.

[27] Further, in Investigation Report 131-2015, SGI had also committed to the following:

- The Auto Fund division would monitor all activity conducted by the issuer in question for a period of one year. If any further privacy transgression is found it will result in the closing of the office;

- All staff of the issuer would have to complete Issuer Privacy Training within the next two months.

[28] SGI reported its progress to my office since the issuance of those past reports.

[29] Turning back to the current investigation, SGI outlined two preventative measures in its internal privacy breach investigation report including:

- Placing an obligation on the owners of each issuing office to monitor and report on staff access. An obligation to do so would be integrated into the Issuer Agreement.

- SGI's Chief Privacy Officer will review results of audit from each issuing office.

[30] I agree with SGI's assessment that "third party access continues to be a proven critical risk for the Company." The problem of unauthorized access to personal information by third parties is systematic. I do not believe that SGI has done enough to address this problem.

i. Auditing and Monitoring

[31] As noted, I have recommended that SGI develop an auditing and monitoring program. I also recommended that SGI update my office on its progress. SGI committed to do so.

[32] I received updates in February and May 2016. SGI reported the following:

- A system prompt had been developed to require employees of issuers to log a reason for a search. SGI indicated that these notes will be monitored, but did not give specifics such as how, when and by who.

- SGI indicated that it was investigating adding a different prompt to require users to make a note if personal information had been accessed but no transactions were completed. SGI reported that implementing this was dependant on resources and that "business requirements for a conceptual design are started". I note that the employee in question made over 1,400 accesses in the past year and this could have been a powerful deterrent.

- SGI had developed a reporting tool that would analyze percentages of accesses where transactions were made versus access where no transactions were made. While there can be reasons for an access where no transaction occurs, a high percentage of these accesses could be an indication of snooping. SGI reported that this tool would be used monthly and quarterly. It reported in May 2016, that through this tool, it investigated one suspicious individual, but found nothing improper. I asked SGI why this tool did not detect the 1,400 unauthorized accesses of the employee in question. SGI indicated that although the tool was ready in May 2016, "they were not reviewing them prior to the Vonda breach as a result of a limitation in staffing". It reported that a staff person will be starting in October on a temporary basis.

- SGI also developed the metric for investigating accesses that occur outside of usual business hours which are 7:30 to 21:00 for most issuers. Accesses made from 22:00 to 6:00 will be investigated.

[33] While SGI has made some progress on an auditing and monitoring program, it is not a complete program. SGI has not yet created a meaningful prompt that requires users to explain all accesses. Further, SGI has not provided enough detail to demonstrate that it has a consistent auditing and monitoring system in place. I would expect SGI to have policies and procedures in place to address these questions:

- Who is responsible for auditing and monitoring?
- What metrics will be audited and at what frequency?

- Will audits be random or focused?
- Who will check the checker?
- Has SGI considered other common auditing metrics such as same name look up or same address lookup?
- Who will be involved in an investigation if there is a problem?
- Do the audits include users of SAM that are both internal and external to SGI?

[34] SGI has also indicated that auditing is a costly activity. Although it has received funding for an additional employee to set up an auditing program, the term is for only one year. Instead, SGI plans to place the responsibility on the owners of the Issuers. While owners have a role to play in monitoring and auditing, I question this decision. SGI is vulnerable to unauthorized accesses by the owners. In Investigation Report H-2010-001, my office found that the owner of a pharmacy was snooping in provincial electronic medical records without a need-to-know. Many Issuers are located in close knit communities and family and friends work within the office. Although the owners have a role to play in auditing and monitoring, SGI should not trust owners to rigorously monitor and discipline employees when those employees may be a spouse, child or family member.

[35] As noted above, in response to Investigation Report 131-2015, SGI committed to monitoring all activity conducted by the Issuer in question for a period of one year. If any further privacy transgression was found it would have resulted in the closing of the office. My office asked SGI if this would be in place for Hometown Insurance Brokers. It responded as follows:

> We can also monitor for one year if ordered. However, this persons access to the system has been permanently suspended and we are now monitoring non-transactional look ups on all issuers and requiring notes be placed on the file. We were not doing this at the time of the [other] breach. I believe this should suffice as an audit function.

[36] I am not satisfied with SGI's auditing and monitoring program so far. I recommend it take immediate steps to create a consistent and effective program to mitigate this "proven

critical risk" which is not only a privacy breach, but a risk management issue that will affect its brand.

ii. Information Sharing Agreements

[37] Information sharing agreements are a privacy best practice when an organization is granting a third party access to personal information within its custody or control. "Information sharing" means the exchanging, collecting, using or disclosing of personal information by one public body with another organization for certain purposes. The sharing may be carried out using any transmission method and may take place over any time period. As SGI is allowing Issuers to have access to the personal information in SAM, a robust information sharing agreement is completely appropriate and essential for risk mitigation.

[38] An information sharing agreement is a written record of understanding between parties that outlines the terms and conditions under which personal information is shared between the parties. An adequate information sharing agreement should be in place between the parties to protect the personal information involved and to ensure compliance. An information sharing agreement should include the following:

1. Define what personal information means and what personal information is involved.
2. Describe the purpose for data sharing.
3. Reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information.
4. Establish an understanding of who has possession and control.
5. Identify the type of information that each party will share with each other.
6. Identify the uses for the information and limitations on the uses to the specified purpose.
7. Describe who will have access and under what conditions.
8. Describe how the information will be exchanged.
9. Describe the process for ensuring accuracy.
10. Describe the process for managing privacy breaches, complaints, and incidents.
11. Identify retention periods.

12. Identify secure destruction methods when retention expires.
13. Describe the security safeguards in place to protect information.
14. Describe compliance monitoring. Including an obligation on the Third Party to participate in auditing and monitoring activities.
15. Describe termination of the agreement procedures.

[39] I have reviewed the agreement between Hometown Insurance Brokers and SGI. SGI has indicated that the agreement is the same with all Issuers in the province. There are two relevant sections: Confidentiality and Access to SAM. The Confidentiality section lays out general terms for the handling of "information". It does not reference "personal information". The Access to Sam section is also vague and provides as follows:

> Access to SAM
> 23 (1) In providing the Issuer and the Issuer's personnel access to SAM, SGI shall provide eligible issuer personnel with user identification to allow that employee to access SAM and the SGI Records necessary for the performance of the Services.
>
> (2) The Issuer shall ensure that all its personnel comply with all requirements set forth in the Issuer Manual in relation to obtaining access to SGI's electronic database.
>
> (3) In addition to those requirements set out in subsection (2) above, the Issuer shall not, and shall ensure that its personnel shall not:
>
> (a) permit or direct any other person to use or have knowledge of another person's user identification;
>
> (b) use or permit someone else to use the user identification of any other person; or
>
> (c) permit any person not authorized by SGI to access SAM.
>
> (4) SAM may not be accessed on any computer or mobile device outside the Issuer's place of business.

[40] The agreement also lacks any consequences if the Issuer, or one of its employees, is responsible for a privacy breach. As noted, in this case, SGI would even not commit to increased monitoring or requiring additional privacy training as a result of the breach. However, it does want to place responsibility of the monitoring back on the Issuer.

[41] I recommend SGI update its agreements between itself and the Issuers and include robust language that would normally be found in an information sharing agreement.

III FINDINGS

[42] I find that personal information was involved in this situation.

[43] I find that FOIP applies in this situation.

[44] I find that SGI has not taken reasonable steps to respond to this breach.

[45] I find that SGI has not taken adequate steps to safeguard the personal information in SAM from unauthorized disclosures by issuers.

IV RECOMMENDATIONS

[46] I recommend that SGI notify individuals affected by the breach for at least two years back.

[47] I recommend that SGI monitor all activity conducted by the issuer in question for a period of one year. If any further privacy transgressions are found it should result in loss of access to SAM.

[48] I recommend that SGI require all staff of the Issuer to complete Issuer Privacy Training within the next two months.

[49] I recommend that SGI complete a comprehensive auditing and monitoring program for accesses to SAM, complete with policies and procedure, within six months and provide them to my office for comment.

[50] I recommend SGI update its agreements between itself and the Issuers and include robust language that would normally be found in an information sharing agreement.

[51] I recommend that SGI incorporate consequences for snoopers and the Issuers in the agreement.

[52] I recommend that, within six months, SGI implement the use of a prompt for all Issuers to explain the reason for an access whenever a transaction has not been completed.

[53] I recommend that SGI forward its investigation file to the Ministry of Justice, Public Prosecutions Divisions to determine whether an offence has occurred and whether charges should be laid under FOIP.

Dated at Regina, in the Province of Saskatchewan, this 27th day of September, 2016.

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