INVESTIGATION REPORT 173-2015

Saskatchewan Government Insurance

November 12, 2015

Summary: Saskatchewan Government Insurance (SGI) proactively reported to the Office of the Information and Privacy Commissioner (OIPC) that it had received a complaint alleging that an employee of an insurance broker agency in the province had inappropriately accessed the personal information of two individuals on the SGI Auto Fund database. Following its investigation, SGI determined that a privacy breach had occurred and provided a copy of its investigation report to the OIPC. The Commissioner was satisfied with the steps taken by SGI to address the privacy breach and recommended that SGI provide the OIPC with a quarterly update on its progress implementing the preventative measures. SGI agreed to this recommendation.

I BACKGROUND

[1] On September 15, 2015 Saskatchewan Government Insurance (SGI) contacted my office to proactively report a privacy breach. According to SGI, an employee of an insurance broker agency in the province may have inappropriately accessed the personal information of two individuals on the SGI Auto Fund database. SGI advised my office that it would be investigating and would provide my office with a copy of its internal investigation report once completed.

[2] On October 6, 2015, my office received a written complaint from the two affected individuals, a married couple indicating they were not satisfied with the response they received from SGI on September 16, 2015. According to the couple, they had made an access to information request to SGI in July 2015 for the access history of their Auto

Fund database accounts. They wanted to know who had accessed their personal information. SGI provided the access history for two years which indicated that on September 26, 2014 an employee of an insurance broker agency accessed the couple's personal information on the Auto Fund database with no apparent business purpose. The employee is known to the couple. On September 3, 2015, SGI received a formal complaint from the couple with a request that SGI investigate further. SGI conducted an investigation and provided its response to the couple on September 16, 2015. As the couple was not satisfied, they went on to send a written complaint to my office. The couple indicated that a number of questions were not answered by SGI.

[3] On September 16, 2015, my office provided notification to SGI advising that my office would be monitoring the matter and requested that SGI provide a copy of its internal privacy breach investigation report once completed.

[4] On October 16, 2015, my office received SGI's internal privacy breach investigation report. In it, SGI confirmed that its investigation had found that the employee of the insurance broker agency accessed the personal information of the two affected individuals on one occasion without a legitimate business purpose.

[5] It is necessary to clarify the nature of the relationship between SGI and the insurance broker agency. The insurance broker agency is a license issuer under contract with SGI to provide driver licensing and vehicle registration services to the public. The insurance broker acts as an agent for SGI. The relationship is governed by contract.

[6] For purposes of this report, the focus is on SGI as a "government institution" pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Government institutions have obligations under FOIP. The insurance broker agency is a private business in Saskatchewan that is not subject to FOIP. Therefore, my office has no jurisdiction over it. However, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) may apply to the insurance broker agency. The federal Privacy Commissioner has jurisdiction over PIDEDA and the organizations subject to it.

[7] Today, public bodies may have to, in order to carry out their mandates, contract with consultants, advisors, professionals or information technology specialists to obtain services. In that process, the contractor may collect, use or disclose personal information on behalf of the public body. That personal information in the possession or control of a contractor deserves the same protection it has in the possession of public bodies. For this reason, I made the recommendation that FOIP be amended to include a new section modeled on section 18 of *The Health Information Protection Act* (HIPA) (see OIPC *Annual Report 2014-2015* at p. 13). I also made this recommendation in my recent Investigation Report 131-2015 which dealt with a privacy breach of a similar nature involving SGI and Lestock Agencies.

II DISCUSSION OF THE ISSUES

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

[8] 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: Tips for Public Bodies/Trustees Dealing with Privacy Breaches* 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.

[9] I will weigh the appropriateness of a public body's handling of a privacy breach against these four best practice steps.

Best Practice Step 1: Contain the breach

[10] 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.

[11] According to SGI's internal privacy breach investigation report, the employee remained at home until SGI completed its investigation. Upon confirming that there was an unauthorized access to personal information without a legitimate business purpose, the employee's access to the Auto Fund database was suspended for two weeks. Therefore, it appears the breach was appropriately contained at the time.

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

[12] 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.

[13] 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.

[14] In this case, SGI provided notification to the couple on September 16, 2015. The notification included an apology for the privacy breach. In addition, it alerted my office

of the privacy breach. I am satisfied with the steps taken by SGI to notify the affected individuals.

Best Practice Step 3: Investigate the breach

[15] 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.

[16] According to SGI's internal privacy breach investigation report a number of steps were taken during its investigation. This included, running an audit log for all Auto Fund transactions conducted by the employee. SGI determined that the employee accessed the couples account on one occasion. Based on the audit, there were no other suspicious or concerning accesses conducted by the employee. SGI determined that the following personal information was accessed: customer name, customer address, birth date, customer type (i.e. individual versus company), photo, email address, date of birth, height, eye color, customer profile information (safety ratings, renewal information, special requirements etc.) and driver information (issue dates, expiry, class and endorsements etc.).

[17] SGI interviewed the owners of the insurance broker agency and was advised that the employee had signed a confidentiality and non-disclosure agreement at the time she was hired by the insurance broker agency. The employee was aware of the rules around accessing the system.

[18] SGI interviewed the employee. The employee admitted to accessing the personal information without a legitimate business purpose. There is some apparent long standing

ill will between the employee and the affected couple. The couple had stopped doing business with the insurance broker agency when the employee started working there. The employee was curious. The employee remained at home until SGI completed its investigation.

[19] I am satisfied that SGI appropriately investigated the privacy breach.

Best Practice Step 4: Plan for prevention

[20] 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.

[21] Following its investigation and determination that a privacy breach had occurred, SGI suspended the employee's access to the Auto Fund database from September 14, 2015 to September 28, 2015. However, SGI emphasized in its internal privacy breach investigation report that the magnitude of this incident was different than the Lestock Agencies matter. A review of the employee's access to the Auto Fund database showed one incident a year ago. Nothing further was found.

[22] SGI acknowledged that this is the second privacy breach of this nature in the province. As noted, I issued a report of a similar nature on September 30, 2015 (Investigation Report 131-2015). In that report, a number of preventative measures proposed by SGI were outlined. The preventative measures included:

- A system prompt for all non-transaction accesses to the Auto Fund database will be put in place for all 25 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.

[23] In its internal privacy breach investigation report for this matter, SGI confirmed that it will continue to work on the above preventative measures. SGI added that, on a go forward basis, all new hires for licence issuers in Saskatchewan will be required to take privacy training within 15 days of hiring.

[24] In the previous Investigation Report 131-2015, my office had followed up with SGI on the timelines for the above prevention plans. SGI had indicated that it was still developing these plans but wanted them implemented soon. SGI agreed, in that case, to update my office on a quarterly basis. The same request applies here. As this is the second Investigation Report dealing with inappropriate access to personal information on the SGI Auto Fund database, it is important that SGI develop and implement this plan in a timely fashion. Six months is considered reasonable unless there are compelling reasons why it should take longer. If additional privacy breaches are discovered, SGI should expedite its preventative measures.

[25] Based on what has been provided by SGI, I am satisfied with the steps taken by SGI to address this privacy breach. I note that some of the preventive steps will take time to fully implement. I rely on SGI's representation that these will occur.

[26] On October 30, 2015, my office provided SGI with the findings and recommendations outlined in this report. On November 9, 2015, SGI advised my office that it would comply with the recommendation to provide a quarterly update to my office.

IV FINDINGS

[27] I am satisfied with the steps taken by SGI to address this privacy breach.

V RECOMMENDATIONS

[28] I recommend that SGI provide my office with a quarterly update of its progress in developing and implementing its preventative measures outlined in this report.

[29] I recommend 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*.

Dated at Regina, in the Province of Saskatchewan, this 12th day of November, 2015.

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