Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 131-2015

Saskatchewan Government Insurance

September 30, 2015

Summary: Saskatchewan Government Insurance (SGI) proactively reported to the Office of the Information and Privacy Commissioner (OIPC) that a number of individual's privacy may have been breached by Lestock Agencies. SGI investigated and determined that a number of breaches had occurred when Lestock Agencies accessed the Auto Fund database without a legitimate business purpose. A number of preventative measures were proposed by SGI. The Commissioner was satisfied with a number of steps taken by SGI but determined that he could not be fully satisfied until the prevention plans proposed by SGI were fully implemented. The Commissioner 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 June 30, 2015 Saskatchewan Government Insurance (SGI) contacted my office to proactively report a privacy breach. According to SGI, a number of individuals in the Lestock area contacted SGI complaining that Lestock Agencies inappropriately accessed their personal information 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] Also on June 30, 2015, my office received the first of several complaints related to inappropriate access by Lestock Agencies. In total, 13 written complaints involving 17

affected individuals were received by my office between June 30, 2015 and August 6, 2015. All of the affected individuals indicated that they were not satisfied with the investigation conducted by SGI and that the steps taken to discipline Lestock Agencies was not commensurate with the breach. In summary, the following are recurring concerns raised in the 13 written complaints:

- There were multiple unauthorized accesses to the personal information of the affected individuals. In one instance, one affected individual's personal information was accessed on 10 separate occasions without an apparent legitimate business purpose;

- Some of the unauthorized accesses occurred after hours when Lestock Agencies was closed;

- There were two agents at the family run business (a father and daughter). Both of their names appear as having made unauthorized accesses. The affected individuals were unhappy that SGI did not address the father's unauthorized accesses;

- 11 of the affected individuals were not customers of Lestock Agencies and had not been for several years. Some do not even live in the Lestock area;

- In two instances, the banking information of two affected individuals was accessed; and

- The affected individuals estimated that 50 accesses occurred that did not have a legitimate business purpose and constituted breaches of their personal information.

[3] The affected individuals learned about the unauthorized accesses by making access to information requests to SGI requesting the access history for their accounts with SGI. Upon receiving responsive records, the affected individuals were able to see who had accessed their personal information in the SGI Auto Fund database, what dates and times access occurred and the notes associated with the access which usually indicated the purpose for the access. All of the affected individuals found that one or both of the agents at Lestock Agencies had accessed their personal information and many of the accesses were unusual and suspicious.

[4] In the package of 13 complaints received by my office, there were copies of a letter from SGI sent to each of the affected individuals. The letters were dated July 13, 2015. The letter confirmed that SGI had concluded its investigation and had found that privacy breaches had occurred. SGI provided an apology to each affected individual and outlined the steps it would take to address the breaches.

[5] On August 13, 2015, my office received SGI's internal privacy breach investigation report. In it, SGI confirmed that its investigation had found that a number of privacy breaches had occurred in the form of unauthorized accesses to the personal information of 20 individuals by Lestock Agencies. However, it did not indicate exactly how many breaches it had found. SGI determined that one of the agents at Lestock Agencies had shared her username and password with her husband to enable him to perform issuing duties. However, he also used it to look up information on the SGI Auto Fund database without a legitimate business purpose. The husband told SGI that he did not disclose the information to anyone and his wife was not aware of his actions. SGI indicated that these actions were in direct violation of the SGI License Issuer Agreement signed by Lestock Agencies. In addition, SGI's access policy does not allow for the sharing of usernames and passwords.

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

[7] 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. Lestock Agencies is a private business in Saskatchewan that is not subject to FOIP. Therefore, my office has no jurisdiction over Lestock Agencies. However, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) may apply to Lestock Agencies. The federal Privacy Commissioner has jurisdiction over PIDEDA and the organizations subject to it.

[8] 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 have 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).

II DISCUSSION OF THE ISSUES

1. Did SGI follow best practices in its response to these privacy breaches?

[9] 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.

[10] 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

[11] 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.

[12] According to SGI's internal privacy breach investigation report, upon confirming that there was unauthorized accesses to personal information without a legitimate business purpose, Lestock Agencies was closed for business for two weeks. In addition, the owner's husband was banned indefinitely from receiving user access privileges for the SGI Auto Fund database. When Lestock Agencies was closed for two weeks its user access privileges were on hold. Therefore, it appears the breach was appropriately contained.

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

[13] 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.

[14] 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.

[15] In this case, SGI provided notification to all 20 individuals. 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

[16] 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.

[17] According to SGI's internal privacy breach investigation report a number of steps were taken during its investigation. This included, running an audit log to see who accessed each individual's Auto Fund record. SGI indicated that in some cases, an Auto Fund record is accessed in order to perform a transaction, such as renewing a driver's license or vehicle registration. In these cases, the audit log activity can be reviewed and associated with a supporting transaction. In other cases, an Auto Fund record may be accessed to respond to a customer inquiry, for example, if a customer calls asking when their vehicle registration expires, or what their current safe driver rating is. In these cases, there would be no supporting transaction associated with a valid inquiry. This would be reflected the same way if an issuer was snooping. SGI concluded that if a supporting transaction was evident, there was no inappropriate access. Similarly, if there was no supporting transaction, and the record was viewed by Lestock Agencies, SGI treated this as an unauthorized access.

[18] SGI determined that the following personal information of all the affected individuals was accessed: customer name, customer address, birth date, customer type (i.e. individual versus company), photo, email address, date of birth, height and eye color. For

some of the affected individuals, additional personal information was accessed including: customer profile information (safety ratings, renewal information, special requirements etc.), driver information (issue dates, expiry, class and endorsements etc.), auto pay contracts (effective dates, status, termination dates etc.) and banking information (last four digits of branch number, bank number, last four digits of account number, bank name etc.).

[19] There is one concern with the investigation conducted by SGI. According to the internal privacy breach investigation report, the Manager of Issuer Relations interviewed one of the agents at Lestock Agencies and her husband at different times. No documentation was made of the interviews. It also does not appear that the second agent at Lestock Agencies was interviewed. SGI addressed this in the internal privacy breach investigation report noting that its interview process was too informal in this case. SGI outlined a list of new requirements that will be implemented for privacy breach investigations involving Auto Fund going forward. This included specific timelines for conducting the interviews, the SGI Privacy team being consulted regarding the content of the interviews, interviews being voice recorded and transcribed, a hold on any changes to user access privileges during investigations and the monitoring of all transactions completed by the issuer in question until the cause of the breach has been ascertained. These are positive steps for future investigations.

[20] Although SGI did not do a number of things in its investigation that would be consistent with best practice, SGI has a plan to address the deficiencies going forward. Therefore, I am satisfied.

Best Practice Step 4: Plan for prevention

[21] 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.

[22] SGI outlined a number of preventative measures in its internal privacy breach investigation report including:

- The Auto Fund division will monitor all activity conducted by Lestock Agencies for a period of one year. If any further privacy transgression is found it will result in the closing of the office;
- All Lestock Agencies staff must complete Issuer Privacy Training within the next two months;
- 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 Auto Fund will monitor the reasons and follow up on any suspicious or problematic transactions with the offending agency;
- 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 in the future.

[23] My office followed up with SGI on the timelines for the above prevention plans. SGI indicated that it was still developing these plans but wanted them implemented soon. SGI agreed to update my office as its steps and timelines were determined. However, SGI was able to clarify what its monitoring plans would entail with Lestock Agencies. SGI will be running weekly audit reports on Lestock Agencies and reviewing its accesses to the Auto Fund database.

[24] In the past, my office has recommended that public bodies run regular random audits to ensure accesses to electronic systems are only occurring for legitimate business purposes. In addition, public bodies create policy and procedure to ensure it is conducting these types of regular random audits. Finally, where an employee has been found to be snooping, public bodies should monitor those employees for a period of years instead of

months. My office is currently developing guidance for public bodies on best practices for auditing.

[25] In this instance, SGI is still developing a plan for auditing issuer use of the 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 it should take longer.

[26] My office reviewed the License Issuer Agreement signed by Lestock Agencies. The agreement stipulates what is required of Lestock Agencies in terms of accessing the database solely for business purposes. I am satisfied that the agreement is sufficiently clear.

[27] Based on what has been provided by SGI, I am satisfied, for the most part, with the steps taken by SGI to address this privacy breach. However, until the prevention plans are implemented, I cannot say that I am fully satisfied that SGI has taken sufficient steps to prevent future breaches of this nature.

[28] On September 21, 2015, my office provided SGI with the findings and recommendations outlined in this report. On September 28, 2015, SGI advised my office that it would comply with the recommendation to provide a quarterly update to my office.

IV FINDINGS

[29] I am satisfied, in part, with the steps taken by SGI to address this privacy breach.

V RECOMMENDATIONS

[30] 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.

[31] I recommend, as per my *Annual Report 2014-2015* that the Ministry of Justice amend FOIP to include a new section that protects personal information in the possession and 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 30th day of September, 2015.

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