Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 297-2016 to 301-2016

Saskatchewan Government Insurance

November 21, 2017

Summary: Five complaints were received at the Office of the Information and Privacy Commissioner (OIPC) related to a privacy breach matter already addressed by the Commissioner in Investigation Report 131-2015. The complaints were similar to those previously investigated and the breaches of privacy occurred during the same timeframe. Upon investigation, the Commissioner was satisfied with how SGI addressed the privacy breaches involving Lestock Agencies occurring between 2010 and 2015. Further, the preventative measures that were outlined in Investigation Report 131-2015 have all been implemented.

I BACKGROUND

[1] On December 1, 2016, my office received a package containing five complaints regarding a matter my office addressed previously in Investigation Report 131-2015. The previous investigation report dealt with the breach of 17 individuals' privacy by Lestock Agencies. The new complaints were from individuals not included in the original 17 but the breaches appear to have occurred during the same timeframe as the original investigation (2010 to 2015). The new complaints involve unauthorized access to personal information in Saskatchewan Government Insurance (SGI) accounts by Lestock Agencies. The additional five complaints would bring the total number of affected individuals, known to my office, to 22.

[2] Upon review, the complaints were similar to those received by my office in the first investigation. My observations from the five new complaints are the following:

- There were multiple unauthorized accesses to the personal information of the affected individuals between 2012 and 2015. In one instance, a female's personal information was accessed on 13 separate occasions without a legitimate business purpose. She was 17 years of age at the time;
- Some of the unauthorized accesses occurred after hours when Lestock Agencies was closed;
- The unauthorized accesses were all made by one individual at Lestock Agencies;
- The complainants allege the individual was looking up information to use for an upcoming election, including information on the town administrator at the time;
- Two of the affected individuals did not live in the Lestock area but had family living there; and
- In one instance, the banking information of one affected individual was accessed.

[3] All, but one, of the affected individuals raised privacy concerns with SGI and received responses back between July 2015 and September 2015 confirming that a breach of their privacy had occurred.

[4] On December 19, 2016, my office notified SGI that it would be undertaking an investigation into the five new complaints and requested a copy of its privacy breach investigation report. On February 2, 2017, SGI referred my office to its investigation report dated August 12, 2015 for Investigation Report 131-2015.

[5] As indicated in Investigation Report 131-2015, my office does not have jurisdiction over Lestock Agencies. In order to have jurisdiction, Lestock Agencies would have to fit the definition of a "government institution" under *The Freedom of Information and Protection of Privacy Act* (FOIP), a "local authority" under *The Local Authority Freedom of Information and Protection of Privacy Act* or a health "trustee" under *The Health Information Protection Act*. It does not fit any of these definitions. It is a commercial business under contract with SGI to provide driver licensing and vehicle registration services to Saskatchewan residents.

[6] In order to provide driver licensing and vehicle registrations, Lestock Agencies needs access to SGI's Auto Fund system which holds records of all drivers and registered vehicle owners in Saskatchewan. The contract between Lestock Agencies and SGI enables this access. The breaches of privacy in this case involve inappropriate access to personal information in SGI's Auto Fund system. As the owners of this program, SGI is responsible for ensuring appropriate access by all parties it has given access to.

II DISCUSSION OF THE ISSUES

[7] SGI is a "government institution" pursuant to subsection 2(1)(d)(ii) of FOIP.

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

[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 for Government Institutions and Local Authorities* recommends five best practice steps to 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;
4. Plan for prevention; and
5. Write an investigation report.

[9] As I had done in Investigation Report 131-2015, I will weigh the appropriateness of SGI's handling of the matter against these 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] As indicated in my Investigation Report 131-2015, upon confirming that there were unauthorized accesses to personal information without legitimate business purposes, Lestock Agencies was closed for business for two weeks. When Lestock Agencies was closed for two weeks its user access privileges were on hold. Therefore, it appears the breaches were appropriately contained at the time of discovery.

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 its investigation report, SGI indicated that given the public attention the privacy breaches received, it elected not to consume its limited resources with a review of Lestock Agencies' historical transactions to determine the scope of the breaches. In this

case, SGI provided notification to known affected individuals it was aware of as of July 13, 2015. Access requests continued to be received by SGI after this date which revealed additional affected individuals. SGI alerted my office of the privacy breaches on June 30, 2015. 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] I identified some issues with the investigation conducted by SGI in Investigation Report 131-2015. However, SGI had a plan to address those issues. Therefore, I was satisfied with how SGI investigated the breaches.

Best Practice Step 4: Plan for prevention

[17] 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.

[18] In Investigation Report 131-2015, a number of preventative measures were proposed by SGI and my office recommended SGI provide my office with a quarterly report on progress. Those preventative measures were as follows:

1. 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;

2. All Lestock Agencies staff must complete Issuer Privacy Training within the next two months;

3. 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;

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

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

[19] As recommended in Investigation Report 131-2015, SGI provided three quarterly reports to my office dated: February 18, 2016, May 30, 2016 and December 9, 2016. The following is an update on the status of each of these preventative measures as of the issuing of this report.

1. Monitoring all activity conducted by Lestock Agencies for a period of one year

[20] In the third quarterly report dated December 9, 2016, SGI indicated that all daily activity by Lestock Agencies was monitored until July 2016. SGI reports that there were no additional instances of inappropriate access.

2. All Lestock Agencies staff must complete Issuer Privacy Training within the next two months

[21] According to SGI's third quarterly report, Lestock Agencies attended the Issuer training in July 2015. SGI reported that in addition, the Lestock Agencies' staff attended the Issuer training in March 2016, which included privacy training.

3. 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

[22] In its third quarterly report on December 9, 2016, SGI also indicated the system prompt had been implemented in September 2016 with results being monitored.

[23] On October 30, 2017, my office attended SGI to see the system prompt. The prompt appears whenever someone enters and attempts to leave an account without completing a transaction. The system prompt requires the individual to put a reason for the access. All activity in the system can be audited for unusual activity such as frequent accesses without transactions which could indicate snooping.

[24] Each person with access to the system has a unique identification and password. The password has to be regularly. The system prompt is now in place for all 379 motor license issuers in the province.

4. SGI will develop an e-Learning module for license issuers

[25] In its third quarterly report, SGI indicated that its Issuer e-learning module had been in place since 2014, but was reviewed and updated in February 2016. Further, it indicated that seminars that included privacy training were delivered to issuers in March 2016.

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

[26] Having a strong auditing program cannot be overstated. Auditing is a technical safeguard. It is a manual or systematic measurable technical assessment of access to a system or application. Auditing of information systems is necessary to:

- Assess compliance with and measure effectiveness of policies, procedures and agreements;
- Assess compliance with legislative requirements;
- Assess whether appropriate measures are in place to control access; and

- Monitor accesses.

[27] An audit program includes regular monitoring of behavior to determine whether users are complying with the organizations privacy and security policies and agreements when accessing and using data. Further, it serves as a deterrent to unauthorized access, and it supports other privacy activities, including providing evidence for the investigation of privacy breaches and privacy complaints. Monitoring for compliance with policies and procedures can identify gaps in user training and awareness, and areas that need reinforcement. It can also provide information useful for modifying a role-based access control model. An audit program is one component of a comprehensive risk management program (Canada's Health Informatics Association, *Putting it into Practice*, 2013, at p. 41).

[28] On October 30, 2017, my office attended at SGI to see the audit and monitoring program in place. SGI explained eight different types of reports it runs weekly, monthly and quarterly. The reports are run by a designated SGI employee (License Issuer 2) who evaluates the results. Any areas of concern are highlighted. The reports are then passed to the Facial Recognition Analysts who review the reports in more detail to identify any further areas of concern. Each Motor License Issuer has an assigned Issuing Representative at SGI. If any irregularities appear, the Issuing Representative contacts the Motor License Issuer to address it. Any significant concerns will have further investigation and follow-up. Other SGI staff may become involved including SGI's Privacy team. A number of changes have been made to SGI's investigative process including recording interviews.

[29] SGI provided a copy of its Issuer monitoring procedure titled, *Issuer Monitoring, Auditing and Visitation*. Upon review, it is very detailed. The procedure indicates that it supports SGI's Privacy Policy and the SGI Breach Procedures which have both been provided to my office previously.

[30] I am satisfied with the auditing and monitoring program in place at SGI. In my Investigation Report 131-2015, I indicated that until the prevention plans were implemented, I could not say that I was fully satisfied that SGI had taken sufficient steps to prevent future breaches of this nature. However, it now appears that all of the preventative measures have been implemented. Therefore, I am satisfied with how SGI addressed the privacy breaches.

III FINDING

[31] I am satisfied with how SGI addressed the privacy breaches involving Lestock Agencies that occurred between 2010 and 2015.

IV RECOMMENDATION

[32] There are no recommendations at this time.

Dated at Regina, in the Province of Saskatchewan, this 21st day of November, 2017.

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