Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 370-2021

Saskatchewan Liquor and Gaming Authority

November 10, 2022

Summary: The personal information of approximately 40,000 individuals was compromised when a critical vulnerability within the content management system platform used by Saskatchewan Liquor and Gaming Authority (SLGA) was left unpatched. SLGA proactively reported the privacy breach to the Commissioner. The Commissioner found that the root causes of the privacy breach was the lack of patching of a critical vulnerability in a timely manner. The lack of detection of the attackers' activity, and SLGA's unnecessary retention of personal information. The Commissioner made a number of recommendations, including that SLGA: provide information to affected individuals on how they may request a copy of their information that was lost in the privacy breach; extend its offer of credit monitoring from two years to a minimum of five years; subscribe to receive email notifications of security bulletins from its vendor of its content management system; ensure it is sufficiently resourced to promptly act upon critical vulnerabilities; ensure it is sufficiently resourced to promptly act upon any detection of malicious activities; and implement retention policies and procedures immediately so that it is not retaining personal information unnecessarily.

I BACKGROUND

[1] On December 25, 2021, an Information Technology (IT) employee of the Saskatchewan Liquor and Gaming Authority (SLGA) attempted to perform tasks, but was unable to do so because they could not connect to the web server. Then, SLGA received a ransom demand. If the ransom was not paid, the attackers would publish data to the media and on the dark web.

[2] On December 28, 2021, SLGA issued a news release announcing it was a subject to a cyber security incident to assure its employees, customers and partners that it was working towards remediating the situation. On the same day, SLGA contacted my office to proactively report the matter.

[3] Approximately 40,000 individuals were affected by this privacy breach, including current and past employees, dependents of the employees, and regulatory clients. The attackers also followed through with their threat to disclose data to the media as well as on the dark web.

What happened

[4] SLGA uses a content management system (CMS) platform to maintain its website. A critical vulnerability existed with the software. However, SLGA was unaware of a remote code execution vulnerability that enabled attackers to enter its IT environment from the Internet. The vulnerability allowed for access to SLGA's IT environment without any authentication.

[5] Based on a forensic investigation conducted by SLGA, the attackers initially entered SLGA's IT environment in November of 2021. However, SLGA did not discover the attack until December 25, 2021 when it received the ransom demand.

[6] On December 28, 2021, SLGA proactively reported this privacy breach to my office. SLGA continued to provide status updates to my office.

[7] On April 6, 2022, my office notified SLGA that it would be undertaking an investigation into the matter.

[8] In the course of my office's investigation, several affected individuals contacted my office with concerns. For individuals whose concerns were within the scope of this investigation, my office requested that they submit a written complaint to my office to receive a copy of this Report.

[9] However, my office received a written complaint from an individual whose concerns were related, but beyond the scope of this investigation. To address the Complainant's concerns, my office opened an investigation file (096-2022). Pursuant to Part 6 of my office's *Rules of Procedure*, my office asked SLGA for a written submission on the matter, which SLGA has thus far been unable to provide. SLGA explained that it has hired a consultant to review its policies and procedures related to the collection, retention and storage of personal information. Due to recent and upcoming changes at SLGA, the consultant's work has been delayed. This delay affects my office's ability to complete its own investigation into the matter, and so my office will issue Investigation Report 096-2022 at a later date.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[10] SLGA is a "government institution" as defined by subsection 2(1)(d)(ii) of FOIP and section 3(a) and Part I of *The Freedom of Information and Protection of Privacy Regulations*. Therefore, I find that I have jurisdiction to conduct this investigation.

2. Did SLGA respond appropriately to this privacy breach?

[11] My office's *Rules of Procedure* outlines that my office will analyze whether the government institution properly managed the breach and took the following steps in responding:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Prevented future breaches

[12] I will analyze each of the four steps below.

Contained the breach (as soon as possible)

[13] Upon learning that a privacy breach has occurred, steps should be taken to immediately 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; and
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines for Government Institutions and Local Authorities*, updated August 2022, [*Privacy Breach Guidelines*], p. 4).

[14] On December 25, 2021, SLGA shut down its systems upon learning of the attack. It contacted the IT Division at the Ministry of SaskBuilds and Procurement. The following day, cyber security experts were engaged.

[15] I find that SLGA took steps to contain the privacy breach when it discovered the attack.

Notified affected individuals (as soon as possible)

[16] When an unauthorized use or disclosure of personal information occurs, section 29.1 of FOIP requires that government institutions notify affected individuals if there is a "real risk of significant harm" to the individual. Section 29.1 of FOIP provides:

> **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.

[17] My office's *Privacy Breach Guidelines* references the federal law *Personal Information Protection Electronic Documents Act* (PIPEDA) that describes "significant harm" as follows:

> **10.1(7)** For the purpose of this section, significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

[18] Further, a public body must consider if there is a "real risk" that the significant harm will occur. My office's *Privacy Breach Guidelines* references the Alberta's Office of the Information and Privacy Commissioner's (AB IPC) resource *Personal information Protection Act Mandatory Breach Reporting Tool*, which offers the following factors to consider:

- What is the nature of the information involved?
- Who obtained or could have obtained access to the information?
- How many persons was the information exposed to?
- Is there any personal or professional relationship between the affected individual and the unauthorized recipient of the information?
- Were there security measures in place to prevent unauthorized access, such as encryption?
- How long was the information exposed?
- Is there evidence of malicious intent or purpose, such as theft, hacking or malware?
- Could the information be used for criminal purposes, such as for identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved, such as youth or seniors?

[19] However, my office recommends that government institutions inform affected individuals of privacy breaches, regardless of whether there is a "real risk of significant harm". Affected individuals are in the best position to determine how a privacy breach affects them.

[20] Notification to individuals affected by the privacy breach should occur as soon as possible after key facts about the breach have been established. It is best practice to contact the affected individuals directly (*Privacy Breach Guidelines*, pp. 5-6).

[21] However, there may be circumstances where a direct notice is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements (*Privacy Breach Guidelines*, p. 6).

[22] Notifications should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to my office (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

(*Privacy Breach Guidelines*, p. 6)

[23] The first notice SLGA issued was a notice posted to its website on December 28, 2021. Since it was only three days after it discovered the breach, the notice contained minimal information. However, even if it contained minimal information, I find that notifying the public soon after the discovery, the breach was appropriate.

[24] Then, SLGA issued numerous notices, which are detailed below. Since there were different groups of affected individuals, SLGA took different approaches to notifying each group.

Current employees

[25] SLGA offered the following notices to current employees:

- In a letter dated January 17, 2022, SLGA notified current employees of the privacy breach by letter and email. The letter included a description of what happened, the personal information involved, what SLGA is doing, the offer of credit monitoring for two years, advice on to how the employee can protect themself, my office's contact information and the telephone number of a call centre that the employee may call with further questions.

- In an email, also dated January 17, 2022, SLGA informed employees that they should be receiving a letter with information regarding credit monitoring being delivered by Canada Post. The email also contained the telephone number of a call center that employees may call with further questions.

- Then, in an email dated February 2, 2022, SLGA informed employees that letters have been sent out to current employees and adult dependents regarding the privacy breach. The email also specified that the activation code for two years of credit monitoring was valid until May 31, 2022.

- A final email was sent on May 30, 2022 to employees to remind them that the activation code for the credit monitoring was valid until May 31, 2022.

Past employees

[26] SLGA sent a letter dated January 21, 2022 to past employees who were impacted by the privacy breach. This letter was similar to its January 17, 2022 letter to current employees and included a description of what happened, the personal information involved, what SLGA is doing, the offer of credit monitoring for two years, advice on to how the employee can protect themself, my office's contact information and the telephone number of a call centre that the past employee may call with further questions.

Adult dependents

[27] SLGA sent a letter dated January 24, 2022 to the adult dependents of current and past employees who were impacted by the privacy breach. Similar to its letters dated January 17, 2022 and January 21, 2022 described above, the letter included a description of what happened, the personal information involved, what SLGA is doing, the offer of credit monitoring for two years, advice on to how the employee can protect themself, my office's contact information and the telephone number of a call centre that the individual may call with further questions.

Regulatory clients

[28] Regulatory clients are liquor and cannabis permittees, gaming registrants, special occasion permittees and charitable gaming licensees.

[29] On March 22, 2022, SLGA posted a notice to its website directed at regulatory clients. The notice included a description of the information that was involved, what SLGA is doing to investigate the matter, advice on how regulatory clients can protect themselves, and the telephone number of the call centre that regulatory clients may call with further questions.

[30] On June 28, 2022, SLGA sent out letters to about 15,000 regulatory clients in Canada. There were approximately 200 regulatory clients located in the United States (US), which I will discuss below. SLGA informed the regulatory clients in Canada that some personal information (including names, contact information, criminal histories and financial information) it collected as part of liquor, gaming and cannabis regulation activities "was affected". The letter offered regulatory clients two years of credit monitoring, advice on how clients may protect themselves, my office contact information, what SLGA is doing to prevent future breaches, and the telephone number of a call center that the client may call with further questions.

[31] SLGA explained that the 15,000 regulatory clients to whom it sent direct notice of the privacy breach were clients who had been in contact with SLGA within the past five years.

For regulatory clients who had not been in contact with SLGA for five years, SLGA was unsure of the veracity of their contact information. Therefore, SLGA opted to post a notice to its website on June 28, 2022 and issued a media statement. The notice on the website contained similar information as its June 28, 2022 letter.

[32] On July 22, 2022, SLGA sent notices to about 200 of the regulatory clients located in the US. SLGA explained that there was a delay in sending out these letters since it had to research US notification requirements and arrange for credit monitoring.

[33] I find that the contents of the notices issued by SLGA contain the elements recommended by my office. However, the affected individuals who contacted my office expressed the following concerns: 1) even after contacting the call center, they did not know precisely what of their personal information was lost; and 2) the length of time it took SLGA to send direct notices to regulatory clients.

[34] First, SLGA's call centre was capable of only informing affected individuals of the types of information that were lost. It was not able to inform individual callers precisely what of their own personal information was lost. SLGA indicated it provided "information on file" to individuals who "reached out", but there was a low number of individuals who did so. SLGA indicated that it established a process where if individuals wanted to know details on their specific information, the call centre would take down their information and provide it to SLGA. Then, SLGA would follow-up. SLGA asserted it received very few of the escalated calls.

[35] Based on a review of the letters SLGA sent to affected individuals, I note that SLGA did not provide details as to how affected individuals may request their "information on file," so they could know precisely what information was lost. Unless affected individuals contacted the call centre and the call progressed to the point where the call centre would forward the individual's information to SLGA, then affected individuals would not know what the process is to get a copy of their information that was lost. As such, I recommend that SLGA post details to its website as to how affected individuals may request a copy of their information that was lost in this privacy breach. Also, I recommend that SLGA

include in its regular communications with employees and regulatory clients (such as notices to renew their licenses) details of how they may request a copy of their information that was lost in the privacy breach.

[36] Second, regarding the length of time for SLGA to send direct notice to regulatory clients, SLGA explained that the length of time was due to the following:

- At the time of its March 22, 2022 notice posted to its website for regulatory clients, SLGA had decided that an indirect notice posted to its website was the most appropriate given the number of individuals affected, SLGA's confidence in the veracity of the addresses on file, and the level of risk to the regulatory clients.

- After March 22, 2022, SLGA learned that personal information was disclosed to the dark web, which resulted in a higher risk assessment for affected individuals. Due to the higher risk, SLGA determined that direct notice was appropriate. However, it required time to verify which of its regulatory clients could confidentially be contacted by mail. Ultimately, it determined it was able to contact 15,000 regulatory clients directly by mail. SLGA asserted it took significant expense and effort to finalize the details of the direct mail out.

[37] Earlier, I noted that posting notices to its website (especially soon after the breach) is appropriate. However, if SLGA found that it was appropriate to directly notify its employees and their dependents, then efforts should have been made much sooner to contact regulatory clients directly as well. Affected regulatory clients may have been located beyond Saskatchewan, including those located internationally, reducing the likelihood of them being aware of the website notices or media statements.

[38] Later, I will discuss the retention of data and how that may have contributed to the vastness of this privacy breach. Going forward, it is my hope that SLGA does not experience a privacy breach of this magnitude. However, I recommend that SLGA develop strategies of contacting regulatory clients in a direct method in the event of a future breach. This could include sending alerts via email.

[39] Lastly, I want to comment on SLGA's offer of two years of credit monitoring to affected individuals. Given the nature of the personal information lost in this privacy breach,

affected individuals are at risk of identity theft. I find that SLGA's offer of credit monitoring to be appropriate. In the past, I have recommended that organizations offer affected individuals credit monitoring for a minimum of five years. I recommend that SLGA extend its offer of credit monitoring from two years to at least five years to individuals who request it.

Investigated the breach

[40] Investigating the privacy breach to identify root causes is key to understanding what happened. It is an important step in mitigating the risk of a future breach of a similar nature from occurring. The following are some key questions to ask during a privacy breach investigation:

- What and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

(*Privacy Breach Guidelines*, pp. 6 to 7)

[41] To investigate a privacy breach is to determine the root cause, or why the privacy breach occurred.

[42] In this investigation, I have identified three root causes of this privacy breach: 1) the lack of patching of a critical vulnerability; 2) the lack of detection of the attackers' activity; and 3) the unnecessary retention of personal information.

1. The lack of patching a critical vulnerability

[43] As described in the background, a critical vulnerability existed within the CMS platform software. SLGA reported that the "website technology vendor" did not advise SLGA of the critical vulnerability. As such, SLGA was unaware of the vulnerability that enabled attackers to enter its IT environment remotely without authentication.

[44] SLGA noted that it has a policy entitled *IT System Maintenance Policy*, which was in effect at the time of the incident. A portion of this policy provides:

> 1. Regular system maintenance and patching of information systems components shall be performed, at a minimum of every quarter or in accordance to the following patch criticality definition.
>
>   - Unmitigated Vulnerabilities: The discovery of published critical security flaw, considered to be an imminent threat to SLGA, exposed to the Internet, and/or without compensating security controls. Security update to be applied as soon as possible as an emergency change, not to exceed 30 days.
>
>   - Mitigated Vulnerabilities: The discovery of published security vulnerabilities rated as critical, high, medium and low, and are shielded by SLGA security controls. Patch will be applied within the regular system maintenance and patching process.
>
>   - Feature enhancements, bug fix and routine vendor maintenance patches applied as required.

[45] SLGA indicated it was following the policy, but that the "website technology vendor" did not advise it of the critical vulnerability.

[46] My office noted that the vendor posted a security bulletin to its website dated October 8, 2021 (updated October 13, 2021) that described the vulnerability and the solution. Soon after, security researchers published articles and blogs that publicized the vulnerability. Given the nature of the vulnerability, attackers were able to launch attacks remotely via the Internet for those who use the CMS platform but had not applied the patch.

[47] Attackers exploited the vulnerability and entered SLGA's IT environment in November of 2021. While SLGA monitored activity on its systems, the attackers' entry into the IT environment was not detected as unusual or unauthorized activity. Therefore, the attackers entry and activity went undetected. The attackers were able to copy and access multiple data areas, including the personal information of approximately 40,000 individuals, before SLGA learned of the attack on December 25, 2021.

[48] It was 78 days between the date the vendor had posted its security bulletin (October 8, 2021) and the date SLGA discovered the attack (December 25, 2021). In order to prevent a similar incident, it is important that SLGA look to reduce the window of opportunity for attackers to exploit vulnerabilities. I find that a root cause of this privacy breach is SLGA's lack of patching of the critical vulnerability in the CMS system in a timely manner.

2. The lack of detection of the attackers' activity

[49] Once the attackers gained entry into SLGA's IT environment, they were able to copy and access multiple data areas without detection. SLGA indicated that while it did have "ongoing monitoring processes" in place, the attackers' activity went undetected since the attackers used "accepted technology". I find that the lack of detection of the attackers' activity is a root cause of the privacy breach.

3. The unnecessary retention of data

[50] This privacy breach affected individuals who were past employees (and their dependents) as well as regulatory clients with whom SLGA had not been in contact with in the past five years. SLGA had cited that a challenge in directly notifying certain regulatory clients was that it could not confirm the veracity of dated information.

[51] The number of affected individuals could have been much smaller had SLGA not retained personal information indefinitely. In the course of this investigation, my office asked SLGA what records retention/disposition schedules it had in place at the time of the cyber

attack. SLGA provided my office with a copy of its policy entitled, "Records Management – Retention and Disposal Policy". I note that the policy provides as follows:

> For the purpose of archiving and disposal, SLGA operations generate two types of Records, Administrative and Operational. SLGA is no longer required to use Administrative Records Management System (ARMS) to manage its Administrative Records.
>
> *As of April 1, 2015, all of SLGA's Records (administrative and operational) will be managed by an Operational Records Schedule (ORS) which is unique to SLGA.*
>
> [Emphasis in original]

[52] However, based on the materials provided to my office, it is not evident what the retention period was for any records of the records. If there are retention periods, it is not evident that records were being disposed of in a timely manner.

[53] I find that a root cause of this privacy breach is SLGA's unnecessary retention of personal information.

Prevented future breaches

[54] The most important step in responding to a privacy breach is to implement measures to prevent future breaches from occurring. To assist, some questions a government institution can ask itself are:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

(*Privacy Breach Guidelines*, p. 7)

[55] I have identified three root causes of the privacy breach. Therefore, my focus here is if SLGA has implemented solutions to address these root causes. However, I do not want to put SLGA at risk for another attack. Therefore, I will not get into technical details of SLGA's prevention efforts.

[56] First, regarding the lack of patching a critical vulnerability, SLGA had indicated it was following its *IT System Maintenance Policy* at the time of the privacy breach; however, the vendor had not notified SLGA of the critical vulnerability. I note that the vendor offers a subscription to receive email notifications for its security bulletins. If SLGA has not already does so, I recommend that SLGA subscribe to receive the email notifications from its vendor of its content management system. Further, I recommend that SLGA ensure it is sufficiently resourced to promptly act upon critical vulnerabilities.

[57] Second, regarding the lack of detection of the attackers' activity, SLGA has informed my office that it has adopted solutions to detect and block malicious activities at the initial stage of an incident and to prevent the spread of an attack on its IT environment. I recommend that SLGA assess the effectiveness of its solutions frequently. I also recommend that SLGA ensure it's sufficiently resourced to promptly act upon any detection of malicious activities.

[58] Third, regarding the unnecessary retention of personal information, SLGA indicated to my office that it had retained third party experts regarding document management and retention policies and procedures. I recommend that SLGA implement retention policies and procedures immediately so that it is not retaining personal information unnecessarily. Policies and practices must be put into practice. Therefore, I recommend that SLGA is sufficiently resourced to implement and maintain the document management and retention policies and procedures.

III FINDINGS

[59] I find that I have jurisdiction to conduct this investigation.

[60] I find that SLGA took steps to contain the privacy breach when it discovered the attack.

[61] I find that SLGA's posting of a notice of the privacy breach to its website to notify the public of the privacy soon after it discovered the privacy breach was appropriate.

[62] I find that the contents of the notices issued by SLGA contain the elements recommended by my office.

[63] I find that a root cause of this privacy breach is the lack of patching of the critical vulnerability in the CMS system in a timely manner.

[64] I find that the lack of detection of the attackers' activity is a root cause of the privacy breach.

[65] I find that a root cause of this privacy breach is SLGA's unnecessary retention of personal information.

IV RECOMMENDATIONS

[66] I recommend that SLGA post details to its website as to how affected individuals may request a copy of their information that was lost in this privacy breach.

[67] I recommend that SLGA include in its regular communications with employees and regulatory clients (such as notices to renew their licenses) the details of how they may request a copy of their information that was lost in the privacy breach.

[68] I recommend that SLGA extend its offer of credit monitoring from two years to at least five years to individuals who request it.

[69] I recommend that SLGA subscribe to receive the email notifications of security bulletins from its vendor of its content management system.

[70] I recommend that SLGA ensure it is sufficiently resourced to promptly act upon critical vulnerabilities.

[71] I recommend that SLGA assess the effectiveness of its solutions to detect and block malicious activities frequently.

[72] I recommend that SLGA ensure its sufficiently resourced to promptly act upon any detection of malicious activities.

[73] I recommend that SLGA implement retention policies and procedures immediately so that it is not retaining personal information unnecessarily.

Dated at Regina, in the Province of Saskatchewan, this 10th day of November, 2022.

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