Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 007-2021

Ministry of Environment

September 30, 2021

Summary: The Ministry of Environment (Environment) proactively reported a privacy breach involving the personal information of 33,501 individuals. The privacy breach involved Environment's Hunting, Angling and Trapping License (HAL) system. A third party contracted by Environment to administer the HAL system sent emails to some HAL customers that included the name of another individual and that other individual's HAL number. The Commissioner made a number of findings including how Environment took appropriate steps to respond to this privacy breach, as well as taking appropriate steps to prevent similar privacy breaches in the future. The Commissioner recommended that the Ministry to take no further action.

I BACKGROUND

[1] The Ministry of Environment (Environment) intended to send an email to some of Saskatchewan's Hunting, Angling and Trapping License (HAL) system customers to request that they fill out a survey.

[2] On January 7, 2021, what occurred was that 33,501 individuals received an email sent by Aspira, a third party contracted by the former Ministry of Central Services (now Ministry of SaskBuilds and Procurement), to administer the HAL system. Each email contained a personalized greeting ("Dear First Name, Last Name") and the person's HAL number. Unfortunately, emails were sent to the incorrect recipients. For example, the email personalized for Person A was sent to Person B. Person B would have received Person A's HAL number.

[3] On January 8, 2021, Environment proactively reported the matter to my office.

[4] Part 4 of my office's *Rules of Procedure* provides that if a matter involves a large number of affected individuals, I may issue a report. In this case, since there is a large number of affected individuals, I thought it important to issue a Report.

II DISCUSSION OF THE ISSUES

1. Does *The Freedom of Information and Protection of Privacy Act* (FOIP) apply and do I have jurisdiction to conduct this investigation?

[5] Environment qualifies as a "government institution" pursuant to section 2(1)(d)(i) of FOIP. Therefore, I find that I have jurisdiction to investigate this matter.

[6] Aspira qualifies as a "information management service provider" pursuant to section 2(1)(e.1) of FOIP.

2. Did a privacy breach occur?

[7] A privacy breach occurs when "personal information" is collected, used, and/or disclosed without authority under FOIP. Therefore, in order to determine if a privacy breach occurred, I need to determine if: 1) this matter involves personal information and 2) there was an unauthorized collection, use, and/or disclosure of the personal information.

i. Did this matter involve personal information?

[8] First, section 24(1) of FOIP defines personal information 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:
> ...

> (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*;
> …
> (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.

[9] The emails contained a number that is to be used by the individual to log into their account. I find that such information qualifies as personal information pursuant to section 24(1)(d) of FOIP. Further, the emails contained the names of individuals who have a HAL system account. Such information qualifies as personal information as defined by sections 24(1)(k)(i) and (ii) of FOIP. I find that this matter involved personal information.

ii. Was there an unauthorized collection, use, and/or disclosure of the personal information?

[10] To *collect* personal information means to gather, obtain access to, acquire, or to receive personal information. To *use* personal information is to internally utilize personal information by a government institution and includes sharing of the personal information in such a way that the personal information remains under the control of the government institution. To *disclose* personal information means to expose personal information to a separate entity that is not a division or branch of the government institution that has possession or control of that information (IPC) Investigation Report F-2009-001 at paragraph [78]).

[11] When I consider the details described in the background of this Report, it appears as though there was a disclosure of personal information. Section 29 of FOIP provides authority for the disclosure of personal information in specific circumstances. For example, section 29(1) of FOIP authorizes the disclosure of personal information if the individual has consented to the disclosure of personal information. Section 29(2) of FOIP provides for circumstances in which a government institution may disclose personal information without the consent of the individual. However, I note that the emails were erroneously

sent to the incorrect individuals. As such, there was no authority under section 29 of FOIP for such disclosures. I find there were unauthorized disclosures of personal information. Each disclosure was a privacy breach.

3. Did Environment respond appropriately to the privacy breach?

[12] In circumstances where a government institution proactively reports a privacy breach, my office's focus is determining whether the government institution responded appropriately to the privacy breach. In order to be satisfied, my office would need to be confident that Environment took the privacy breach seriously and appropriately addressed it. In the resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* (updated September 2020) (Privacy Breach Guidelines), my office recommends four steps to be taken when a government institution discovers a privacy breach. The four steps are:

1. Contain the breach;
2. Notification;
3. Investigate the breach; and
4. Prevent future breaches.

[13] Below is an analysis to determine if Environment responded appropriately to the privacy breach.

Contain the breach

[14] To contain a breach is to ensure that personal information is no longer at risk. This may involve:

- stopping the unauthorized practice;
- recovering the records;
- shutting down the system that was breached;
- revoking access to personal information; and/or
- correcting weaknesses in physical security.

(Privacy Breach Guidelines, p. 4)

[15] When Aspira detected the error, it immediately halted the process of sending further emails. In total, 33, 501 emails were sent out; however, not all intended emails were sent as a result of Aspira halting the process. Aspira determined it was unable to recall the emails since the emails were no longer on the original server. I find that appropriate steps were taken to contain the privacy breach.

Notification

[16] Section 29.1 of FOIP requires that, if there was an unauthorized use or disclosure of personal information, the government institution must notify the affected individual(s) if the "incident creates a real risk of significant harm" (Privacy Breach Guideline, p. 4).

[17] Regardless of whether there is a "real risk of significant harm", the best practice is to notify affected individuals of the privacy breach so that they can determine how they have been impacted and take steps to protect themselves.

[18] An effective notification 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.);
- 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, how to change a health services number or driver's license number, etc.);
- 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 the my office (provide contact information); and
- recognition of the impacts of the breach on affected individuals and, an apology.

(Privacy Breach Guidelines, pp. 5 to 6)

[19] Also, depending on the circumstances, the government institution should consider notifying other individuals or organizations as soon as possible after learning of the incident, including but not limited to:

- the government institution's privacy officer;
- my office; and
- the police, if criminal activity is suspected (e.g. burglary).

(Privacy Breach Guidelines, p. 4)

[20] In this case, Aspira sent an email to the affected individuals on January 8, 2021. This email contained the original content that was intended to have been sent (e.g. Personalized content for Person A was sent to Person A). The email contained a "correction notice" that read as follows:

> Correction Notice: You may have received an email on January 7th stating incorrect information. We apologize, but this was sent in error. Please see the corrected notice below.

[21] Environment sent another email to the affected individuals on January 12, 2021 that:

- explained what happened;
- it is investigating the privacy breach and will be implementing "mitigation efforts" to prevent a similar event in the future;
- requested that the recipient delete the email that was sent in error on January 7th;
- explained that the privacy breach was a result of human error and that the system was not hacked or breached;
- explained that web accounts cannot be accessed using info contained in the erroneous email (such as HAL number) but if people wished for a new HAL number, they can request one;
- explained that individuals can also change their password to the web account through their HAL profile;
- provided the contact information of Aspira's Privacy Officer, Environment's Privacy Officer; and
- explained that affected individuals had a right to complain to my office and provided my office's contact information.

[22] Based on the above, I find that Environment has provided appropriate notification.

Investigate the breach

[23] Investigating the privacy breach to identify the root cause(s) is key to understanding what happened and to prevent similar privacy breaches in the future. Below are some key questions to ask during a privacy breach investigation:

- When 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)

[24] In this case, Environment reported that Aspira is to take the following steps when doing email mailouts:

Step 1 – Create content/imagery to be sent out; to be approved by Environment.

Step 2 – Verify proposed recipient list.

Step 3 – Add personalization fields (such as HAL number, first name, last name).

Step 4 – Create "target list" by 1) identifying any emails that should not be on mailing list (such as emails who have unsubscribed), and 2) adding the personalization fields to the mailing.

Step 5 – Configure the email system tying elements together and performing the mail merge.

Step 6 – A test communication is sent to the Aspira employee managing the email in order to review for accuracy.

Step 7 – The email is scheduled to be sent for a specific date and time within the email system. Then, the email is sent.

[25] Aspira noted that errors occurred at Step 4 when adding the personalization fields to the mailing. Then, Step 6 was skipped. Step 6 is the step to ensure accuracy. As a result, email recipients received emails that were personalized for other individuals.

[26] I find that Environment and Aspira have investigated the privacy breach and identified the root causes.

Prevent future breaches

[27] Prevention is perhaps one of the most important steps. A privacy breach cannot be undone, but a government institution can learn from one and improve its practices. To avoid future breaches, a government institution should formulate a prevention plan. Some changes that are needed may have revealed themselves during the investigation phase. For example, deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training.

[28] The following are some considerations a government institution can take when completing this step:

- 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)

[29] Environment reported to my office that Aspira updated its email handling procedure. Environment also provided my office with a copy of the updated email handling procedures. The updates include:

1) In addition to the Digital Marketing Manager reviewing email communications being sent, the Senior Marketing Manager will also review the email communications;

2) Increased the number of checks throughout the process to ensure personalized information is properly saved and matched to the correct recipient; and

3) Aspira will send a test email for every "consumer communication" and obtain written approval from Environment, prior to sending actual emails.

[30] I find that Environment and Aspira have taken appropriate steps to prevent similar privacy breaches in the future.

III FINDINGS

[31] I find that I have jurisdiction to investigate this matter.

[32] I find that this matter involved personal information.

[33] I find there were unauthorized disclosures of personal information.

[34] I find that appropriate steps were taken to contain the privacy breach.

[35] I find that Environment has provided appropriate notification.

[36] I find that Environment and Aspira have investigated the privacy breach and identified the root causes.

[37] I find that Environment and Aspira have taken appropriate steps to prevent similar privacy breaches in the future.

IV RECOMMENDATION

[38] I recommend that Environment take no further action.

Dated at Regina, in the Province of Saskatchewan, this 30th day of September, 2021.

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