Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 208-2021

Regina Police Service

August 31, 2022

Summary: A constable at the Regina Police Service (RPS) mistakenly sent the personal information of one individual to another through email. The recipient of the email notified the affected individual (Complainant). The Complainant was not satisfied with the RPS' response to their concerns, so they submitted a complaint to the Commissioner. The Commissioner made a number of findings including that the RPS made a reasonable effort to contain the privacy breach. However, he found that the RPS' letter to the Complainant did not include key elements, including an apology. He recommended that the RPS send another letter to the Complainant that includes key elements, including an apology. He also recommended that the RPS implement procedures on how to send personal information via email and to provide training to staff on such procedures.

I BACKGROUND

[1] On July 2, 2021, a constable with the Regina Police Service (RPS) followed-up a telephone conversation with an individual (Individual A) with an email. The email indicated that there was an amendment to a Summary Offence Ticket Information (SOTI) that was issued to this individual.

[2] On July 6, 2021, Individual A sent a reply to the constable requesting that the constable send them a scanned copy of the amended ticket.

[3] On the same day, the constable responded by email. However, the constable had mistakenly attached the SOTI that contained the information of another individual (Complainant) with

a similarly spelled first name. As a result, Individual A received the following information about Individual B:

- First name, middle initial, and last name
- Date of birth
- Mailing address
- Driver's license number
- Charge details related to the Summary of Offence Ticket

[4] Soon after receiving the constable's email, Individual A informed the constable that the SOTI is not theirs, but another person's with a similarly spelled first name. Minutes later, the constable responded to Individual A by apologizing.

[5] The SOTI did not contain the Complainant's telephone number. However, on July 6, 2021, Individual A was somehow able to contact Complainant via text message to notify them of this matter.

[6] On July 7, 2021, the Complainant contacted the RPS by telephone to express their concerns over the disclosure of their personal information to another individual.

[7] In a letter dated August 9, 2021, the RPS responded to the Complainant's concerns. The letter detailed what personal information was involved in this matter, the steps the RPS has taken to contain the privacy breach, and my office's contact information.

[8] In an email dated August 12, 2021 to my office, the Complainant indicated they were dissatisfied with the RPS' response and would like to file a complaint with my office.

[9] In emails dated August 20, 2021, my office notified both the RPS and the Complainant that my office would be undertaking an investigation.

[10] On October 19, 2021, the RPS provided my office with its submission.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[11] The RPS qualifies as a "local authority" as defined by section 2(f)(viii.1) of LA FOIP. Therefore, I have jurisdiction to investigate this matter.

2. Did a privacy breach occur?

[12] A privacy breach occurs when "personal information" is collected, used, and/or disclosed without authority under LA FOIP. Therefore, in order to determine if a privacy breach occurred, I need to determine if this matter involves personal information. If so, then I need to determine if there was or was not authority under LA FOIP for the RPS to collect, use, and/or disclose the personal information.

a. Did this matter involve personal information?

[13] As summarized in the background, this matter involved the following information:

- First name, middle initial, and last name
- Date of birth
- Mailing address
- Driver's license number
- Charge details related to the Summary of Offence Ticket

[14] Section 23(1) of LA FOIP defines "personal information" as follows:

> **23**(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:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;

> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> ...
> (d) any identifying number, symbol or other particular assigned to the individual;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;
>
> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[15] The information in this matter qualifies as personal information pursuant to section 23(1)(a), (b), (d), (e), and (k)(i) of LA FOIP.

b. Was there authority under LA FOIP for the collection, use, and/or disclosure of the personal information?

[16] To "disclose" personal information means to expose personal information to a separate entity that is not a division or branch of the local authority that has possession or control of that information (Investigation Report F-2009-001 at paragraph [78]).

[17] What occurred in this case was a disclosure of personal information. Section 28 of LA FOIP provides authority for the disclosure of personal information in specific circumstances. Section 28(1) of LA FOIP authorizes the disclosure of personal information if the individual has consented to the disclosure of personal information. Section 28(2) of LA FOIP provides for circumstances in which a local authority may disclose personal information without the consent of the individual.

[18] In this case, the Complainant's personal information was erroneously sent to Individual A. As such, there was no authority under section 28 of LA FOIP for such a disclosure. I find that a privacy breach occurred.

3. Did RPS respond appropriately to the privacy breach?

[19] In my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, updated September 2021, (*Privacy Breach Guidelines*), and Part 4 of my office's *Rules of Procedure*, I recommend four steps to be taken when a local authority discovers a privacy breach. The four steps are:

1. Contained the breach (as soon as possible);
2. Notify affected individual(s) (as soon as possible);
3. Investigated the breach; and
4. Prevented future breaches.

(*Privacy Breach Guidelines*, pp. 4-7, *Rules of Procedure*, Part 4)

[20] Below is an analysis to determine if RPS responded to this privacy breach in accordance with the four best practices.

Contained the Breach (as soon as possible)

[21] An important first step in responding to a privacy breach is to work to contain the breach immediately. In other words, ensure the personal information is no longer at risk. This may involve some or all of the following steps:

- Stopping the unauthorized practice
- Recovering the records
- Shutting down the system that was breached
- Revoking access to personal information
- Correcting weaknesses in physical security

[22] In RPS' letter dated August 9, 2021 to the Complainant, the RPS indicated that it contacted Individual A to destroy the Complainant's personal information. The letter said:

> Our mitigation efforts included contacting the officer involved to determine the details surrounding the breach as well as contacting [Individual A] to ensure proper destruction of your personal information.

> At this time, we can confirm that your personal information has not been shared with anyone else.

[23] In its investigation report to my office, the RPS explained its containment efforts:

> Since the unauthorized personal information was e-mailed, we were not able to recover the record but we contacted [Individual A] and asked [them]to delete the e-mail to contain the breach and also asked that [they] not make any copies of the email or forward as the information does not belong to [them] but to another person.

[24] The Complainant expressed concerns to my office regarding RPS' containment efforts. They said:

> …
> 2) This kind of sloppy police work is unacceptable. My personal info including my address was shared with a stranger (whom [sic] knows if this person is a criminal or a dangerous person or a pedophile). The RPS never addressed my nor my family's personal safety (we have young kids) in their reaponse [sic] letter.
>
> 3) in the letter from RPS they said they felt confident my personal info wasn't shared any further. How can they guarantee that? There r no guarantees in the digital world. My identity will always be at risk for identity theft now. Also did they go to the persons [sic] house whom [sic] received All my personal information and stand before them while they deleted the emails they had been sent from RPS which had included my personal information? Did they personally witnessed [sic] the person deleting the emails with my personal information? No they did not.
> …

[25] I acknowledge the Complainant's point regarding RPS' statement that the Complainant's personal information has not been shared with anyone else. That is, the RPS cannot guarantee that Individual A had not shared the Complainant's personal information further. However, my office's expectation is that local authorities such as the RPS take reasonable steps to contain a privacy breach. In this case, contacting Individual A (who is a private individual) and requesting that they destroy the Complainant's personal information is reasonable.

[26] I find that the RPS has made reasonable efforts to contain the privacy breach.

Notified affected individual(s) (as soon as possible)

[27] Once a privacy breach is discovered, the local authority should notify affected individuals of the privacy breach so that they can determine how they have been impacted and take steps to protect themselves.

[28] 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 the IPC (provide contact information); and
- recognition of the impacts of the breach on affected individuals and, an apology.

(*Privacy Breach Guidelines*, pp. 5-6)

[29] The Complainant indicated the following concern to my office:

> 4) Another concern would be that if I hadn't made a privacy breach complaint to RPS, the officer that committed the breach would have done nothing about it.

[30] I note that the Complainant had learned of the privacy breach soon after it occurred on July 6, 2021, and contacted the RPS the day after the privacy breach occurred. Therefore, in this case, the RPS learned of the privacy breach from the Complainant instead of discovering the privacy breach and notifying the Complainant. Since this was the sequence of events

that occurred, it would be impossible to know if RPS would have notified the Complainant of the privacy breach had the Complainant not contacted the RPS first.

[31] Nevertheless, I note that the RPS did respond to the Complainant's privacy concerns in a letter dated August 9, 2021. I find that RPS's letter to the Complainant contained many elements of what makes an effective notification letter except a description of possible types of harm resulting from the privacy breach, advice on actions the individual can take to mitigate the risk, and recognition of the impacts of the privacy breach on the affected individual and an apology.

[32] In its investigation report to my office, the RPS noted that the Complainant was at risk for reputational harm and humiliation and also acknowledged that the Complainant voiced concerns about identity theft. However, RPS indicated such harm was minimized because the Individual A had agreed to not disseminate the Complainant's personal information and to also destroy the Complainant's personal information. While it may very well be true that the impacts of this privacy breach have been minimized, offering advice to the Complainant on steps they can take to protect themselves could be valuable. Therefore, including advice such as how to contact credit monitoring agencies as well as contacting their banks to let them know their personal information has been lost so the banks can take extra steps to verify their identity going forward. Further, if the individual has provided their driver's license number to any organization as a means to verify their identity (see my Investigation Report 074-2020), then the RPS can advise them to contact that organization to use a different method to verify their identity.

[33] Finally, privacy breaches have an impact on affected individuals. If nothing else, the affected individuals are inconvenienced by having to take steps to be extra vigilant in protecting their identity from being stolen. Therefore, it is important that local authorities such as the RPS recognize the impacts on affected individuals in their correspondence with affected individuals and apologize for the privacy breach.

[34] I recommend that the RPS send another letter that contains advice on how the Complainant can protect themselves from identity theft, the recognition of the impacts this privacy breach may have had on the Complainant, and an apology for the privacy breach.

Investigated the breach

[35] Once a privacy breach has been contained, the next step is to investigate the breach. Identifying the root cause is key to preventing similar privacy breaches in the future.

[36] In its investigation, the RPS noted contributing factors that led to this privacy breach were that the Individual A and the Complainant were part of the same investigation file and were provided the same Summary Offence Ticket Information (SOTI). They also had the same first name.

[37] However, the RPS noted that the root cause of this error was that neither the last name nor date of birth were verified prior to sending the email with the incorrect SOTI attached.

[38] I find that the RPS had investigated and identified a root cause of the privacy breach

Prevented future breaches

[39] Prevention is the most important part of responding to a privacy breach. A privacy breach cannot be undone, but a local authority can learn from one and improve its practices. To avoid future breaches, a trustee 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.

[40] In its investigation report, the RPS noted that this particular constable had already received privacy training and was well aware of RPS' privacy policy, which is entitled "Part 14 Chapter I: Freedom of Information and Protection of Privacy".

[41] Section 9(c) of RPS' privacy policy provides:

> c. Any RPS employee who knows of, or suspects, a privacy breach shall report it immediately to their supervisor and follow the following privacy breach protocol:
>
> ...
> d. The Access and Privacy Team shall be contacted immediately by the supervisor for guidance and management of the privacy breach response.

[42] Therefore, in its investigation report, the RPS indicated it contacted the constable to indicate that they should have contacted the RPS' Privacy Officer immediately.

[43] Regarding the actual erroneous email that led to the privacy breach, RPS indicated that "safeguards were followed as per our policy, this breach was not due to any lack of safeguarding other than double checking information." However, my office noted that RPS' privacy policy was fairly vague regarding the verification of information. It states:

> the RPS will ensure that appropriate security safeguards are in place to protect personal information. **These safeguards are intended to address such concerns as** appropriate access to information, **breach prevention**, recovery, information integrity and other potential security issues. Safeguards include physical, technical, procedural and organizational measures;
>
> [Emphasis added]

[44] I find that RPS' privacy policy is not specific as to what safeguards are in place to require RPS employees to verify or "double-check" information prior to sending personal information through e-mail.

[45] I recommend that RPS implement procedures on how to send personal information via e-mail and provide training to staff on such procedures. An example of a procedure for sending personal information via e-mail would be to password protect the document. Then, the RPS employee should contact the intended recipient by a different method (such as telephone) to provide the password. Therefore, even if the email is sent to the incorrect individual, the recipient will still not be able to gain access to the document. Of course, the sender of the document should still double-check the contact information when they send the email and when they send the password.

III FINDINGS

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

[47] I find that a privacy breach occurred.

[48] I find that the RPS has made reasonable efforts to contain the privacy breach.

[49] I find that RPS's letter to the Complainant contained many elements of what makes an effective notification letter except a description of possible types of harm resulting from the privacy breach, advice on actions the individual can take to mitigate the risk, and recognition of the impacts of the privacy breach on the affected individual and an apology.

[50] I find that the RPS had investigated and identified a root cause of the privacy breach.

[51] I find that RPS' privacy policy is not clear as to what safeguards are in place to require RPS employees to verify or "double-check" information prior to sending personal information through e-mail.

IV RECOMMENDATIONS

[52] I recommend that the RPS send another letter that contains advice on how the Complainant can protect themselves from identity theft, the recognition of the impacts this privacy breach may have had on the Complainant, and an apology for the privacy breach.

[53] I recommend that RPS implement procedures on how to send personal information via e-mail and provide training to staff on such procedures.

Dated at Regina, in the Province of Saskatchewan, this 31st day of August, 2022.

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