Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 062-2022

Rural Municipality of North Qu'Appelle No. 187

December 20, 2022

Summary: The Organized Hamlet of Pasqua Lake Board (Hamlet), within the Rural Municipality of North Qu'Appelle No. 187 (RM), sent an email to a number of individuals and did not use the blind carbon copy field for the email addresses. The Hamlet notified all recipients of the breach and requested they delete the email. The Complainant was one of the email recipients and submitted a privacy breach complaint to the RM. Once more than 30 days had passed and the Complainant had not received a response from the RM, the Complainant requested the Commissioner undertake an investigation. My office undertook an investigation into the RM's actions to respond to the privacy breach. The Commissioner found that the RM did not take appropriate action in response to the privacy breach and made a number of recommendations to the RM to ensure appropriate policy or procedures were in place, as well as implementation of appropriate safeguards to protect personal information.

I BACKGROUND

[1] On March 10, 2022, the Complainant submitted a privacy complaint to the Rural Municipality of North Qu'Appelle No. 187 (RM) as follows:

> On February 22 2022 an email was sent out by Chair [name of Chairperson] to the Organized Hamlet of Pasqua Lake (OHPL) email grouping list. There were over 200 addresses on this list.
>
> This is the Chairs apology,

> "Sorry, but forgot to bcc the previous email that I just sent out. Please delete the addresses in the email. Again my apology.
>
> [Name of Chairperson]
> OHPL Chair
>
> I have some major concerns about the integrity and responsibly of this Chair [name of Chairperson]. This is the 3rd time [the Chairperson] has personally leaked out personal email addresses of ratepayers. The last one being April 9, 2021, less than a year ago. [They] obviously did not learn from [their] mistake [sic] first two times.
>
> I have attached the letter from the Reeve dated May 3 2021 in regards to the last time over 200 email addresses were leaked out from the Chair [name of Chairperson]. In this letter [name of Chairperson] stated "that he will take the time necessary to ensure that any future communication will include the Blind Copy (Bcc) component for the recipients to ensure this situation does not re-occur." This did not work…

[2] On April 19, 2022, the Complainant requested that my office undertake an investigation. The Complainant indicated it had been 41 days since they submitted their privacy breach complaint to the RM and had not received a response.

[3] On April 28, 2022, my office followed up with the Complainant to determine if the RM had provided them with a response. The Complainant advised they had received a response from the RM dated April 20, 2022, and provided my office with a copy. However, the Complainant noted they were not satisfied with the response.

[4] On May 10, 2022, my office notified the RM and the Complainant that my office would be undertaking an investigation into this matter.

[5] On June 22, 2022, the RM provided its response to the investigation and relevant supporting documentation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] I found in my office's Investigation Report 166-2021 that the Organized Hamlet of Pasqua Lake (Hamlet), is an Organized Hamlet within the RM. The RM is a municipality, and therefore qualifies as a "local authority" pursuant to subsection 2(f)(i) of LA FOIP. Therefore, I have jurisdiction to undertake this investigation.

[7] The RM is responsible for ensuring all RM staff, members of the RM council, and members of its Organized Hamlet boards are in compliance with LA FOIP.

2. Is personal information involved and is LA FOIP engaged?

[8] In order for LA FOIP to be engaged in a privacy breach investigation, there must be personal information, as defined by subsection 23(1) of LA FOIP, involved. Subsection 23(1) of LA FOIP provides:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form…

[9] The list provided at subsection 23(1) of LA FOIP is not exhaustive; there are other types of information that may not be listed, but still considered personal information. To be personal information, I must consider if: 1) there is an identifiable individual; and 2) if the information is personal in nature. The definitions of each are as follows:

- "Identifiable" means it must be reasonable to expect that an individual may be identified if the information were disclosed.
- "Personal in nature" means that it reveals something about the individual.

[10] I previously investigated a similar privacy breach involving the same RM and Hamlet in Investigation Report 166-2021. In that matter, the Hamlet Chairperson had sent an email to a number of individuals and did not use the blind carbon copy field for the email addresses. In that report, I found that the personal email addresses qualified as personal information pursuant to subsection 23(1) of LA FOIP. I adopt that analysis for the purposes

of this Investigation Report. Therefore, I find that personal information is involved and that a privacy breach occurred.

[11] In the next section of this Investigation Report, I will consider the actions taken by the RM to respond to the privacy breach.

3. Did the RM respond appropriately to this privacy breach?

[12] As set out in my office's Rules of Procedure, when my office determines there has been a privacy breach, my office will analyze whether the government institution appropriately managed the breach. My office will consider if it:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Took appropriate steps to prevent future breaches

[13] I will use these steps to assess the RM's response to the breach.

Contained the breach (as soon as possible)

[14] Soon after a local authority learns of a privacy breach, it should contain and recover any personal information/personal health information that is involved. This will require determining how broad the privacy breach is and what type of records are involved.

[15] In this matter, the Hamlet Chairperson sent an email that included personal email addresses without using the "bcc" function. Approximately five minutes after sending the email, the Hamlet Chairperson realized their error and sent a follow-up email to the same individuals asking them to delete the first email. This was a timely step to take.

[16] As noted earlier in this Report, I had investigated a similar privacy breach in Investigation Report 166-2021, involving the same RM and Hamlet. In that matter, the Hamlet Chairperson had sent an email to a number of individuals without using the "bcc" function. I issued that report after the privacy breach that is the subject of this Investigation Report. In Investigation Report 166-2021, I had suggested the RM may want to consider what other actions it could take, including attempting to recall the email and/or requesting that recipients confirm they have deleted the email. It does not appear the Hamlet Chairperson took these steps in this matter. As the RM did not confirm these additional steps had been taken, I find the RM has not taken adequate steps to contain the privacy breach.

Notified affected individuals (as soon as possible)

[17] Notice to affected individuals should happen as soon as possible when learning of a breach. Notifying an individual that their personal information has been inappropriately accessed or disclosed 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 potential harm that may result from the inappropriate disclosure. Unless there is compelling reason not to, local authorities should always provide notification.

[18] The Hamlet Chairperson notified the recipients of the error on the same day the breach occurred. On the same day, the Hamlet Chairperson also notified the RM's Chief Administrative Officer of the privacy breach incident.

[19] The Hamlet Chairperson sent an email to all recipients advising of the error. However, there are other elements that the RM should ensure are in notifications to affected individuals. My office's *Privacy Breach Guidelines for Government Institutions and Local Authorities* (*Privacy Breach Guidelines*) on page 6 that suggests the following elements be included in notification to affected individuals:

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

[20] Public bodies should also consider proactively reporting privacy breaches to my office. This means that when a public body learns of a breach, it reports the incident to my office. While proactively reporting is not mandatory, my office does encourage public bodies to proactively report. If my office determines the breach has been responded to appropriately, there may be an opportunity to informally resolve the matter, rather than issuing a public report on the matter.

[21] Because the Hamlet Chairperson did not include the recommended elements in their follow up email, and because the RM did not ensure this occurred, I find that the RM did not provide adequate notification.

Investigated the breach

[22] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The internal investigation should also consider whether the safeguards that were in place at the time of the incident were adequate.

[23] On February 25, 2022, the RM's Reeve and Chief Administrative Officer met with the Hamlet Chairperson to investigate the incident. The Hamlet Chairperson explained they sent a group email using the Hamlet's "gmail.com" email platform and failed to use the "bcc" function. After realizing their error, the Hamlet Chairperson sent out their follow-up email to all recipients.

[24] The Reeve noted during the meeting that this was the second privacy breach of this nature. However, based on the explanation provided, the Reeve determined the cause was human error and that there was no malicious or ill-intent.

[25] As noted earlier, the investigation of the breach is an opportunity to review the safeguards that were in place at the time of the incident. Section 23.1 of LA FOIP provides the following regarding the duty to protect:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[26] My office's *Privacy Breach Guidelines* provides the following regarding administrative and technical safeguards:

> *Administrative safeguards* are controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees,

> confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules, and access restrictions.
>
> *Technical safeguards* are the technology and the policy and procedures for its use that protect personal information and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners, and audit capabilities in digital systems.

[27] In this matter, the root cause was that the Hamlet Chairperson again did not use the "bcc" line in order to protect personal information. As such, they did not adhere to administrative and technical safeguards. As the RM appears to understand this is the issue, I find it conducted an adequate investigation. I will address its response with recommendations in the next part of this Investigation Report.

Prevented future breaches

[28] Local authorities should be safeguarding personal information. Administrative, physical and technical safeguards should be reviewed regularly to determine their adequacy in protecting information, including after the discovery of a privacy breach.

[29] In this matter, the RM appears to have understood why the breach occurred. The question is what safeguards it has implemented to prevent the same, or a similar, breach from occurring in the future.

[30] The RM indicated that during its meeting on February 25, 2022 with the Hamlet Chairperson, the RM's Reeve asked that two people be present for future email communications to provide checks and balances, and to look into having an auto-bcc function included in the process. Council later passed a motion for the Hamlet Chairperson to discontinue use of email communications until the RM could implement a proven method of auto-blind copy or similar function that would effectively prevent any future privacy breaches of email addresses.

[31] When my office followed up with the RM on its motion, the RM advised that the Hamlet has since implemented the use of an alternate email platform system. The RM indicated that this was a result of the motion passed by the RM Council and my office's recommendation in Investigation Report 166-2021:

> [49] I recommend the RM should explore if its email system can be configured to ensure the bcc field is visible by default when sending an email.

[32] Based on discussions with the RM, the email service platform implemented by the Hamlet allows them to set up mass emails to default to sending an email to multiple email recipients without displaying the email addresses of others. I find that by implementing this email system, the RM has taken adequate steps to prevent the Hamlet Chairperson from breaching personal email addresses in the future. To support this, I recommend the RM ensures the email service it is using is properly safeguarded to protect personal information, and that it has a written policy on its use.

[33] I add that in Investigation Report 166-2021, my office reviewed the safeguards that were in place at the time of that breach and found that the RM did not have appropriate safeguards in place. In that report, my office made the following recommendations to the RM to implement sufficient safeguards to protect personal information:

> [30] I recommend the RM develop and implement a policy or procedure for responding to privacy breaches. This should include measures to contain a privacy breach, what parties should be notified of the privacy breach, and the elements to include in notification to affected individuals. As well, it should include what steps to take to investigate a privacy breach and consideration of preventative measures. The policy or procedures should also identify who the Privacy Officer is for the RM and direct the RM staff, members of the RM council and members of its Organized Hamlet boards to report privacy breach incidents to the Privacy Officer.
>
> [31] I recommend the RM develop and implement a privacy policy that addresses collection, use, disclosure and safeguarding of personal information to ensure it meets its obligations under LA FOIP.
>
> [32] I recommend the RM develop and implement a confidentiality agreement to be signed annually by all RM staff, members of the RM council and members of its Organized Hamlet boards.

> [33] I recommend the RM implement annual access and privacy training for all RM staff, members of the RM council and members of its Organized Hamlet boards.

[34] My office followed up with the RM to determine if the RM had implemented the safeguards noted above from that Report. On December 7, 2022, the RM advised that while there had been some discussions regarding these recommendations, at this time the RM had not developed or implemented these recommendations.

[35] As noted earlier, the RM has a duty to protect personal information in its possession or under its control by ensuring it establishes policies and procedures to maintain administrative, technical and physical safeguards. I reiterate my recommendation for the RM to implement the recommendations listed at paragraph [33] and recommend the RM implement these recommendations within six months of the issuance of this Investigation Report.

III FINDINGS

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

[37] I find that personal information is involved and that LA FOIP is engaged.

[38] I find the RM has not taken adequate steps to contain the privacy breach.

[39] I find that the RM has not provided adequate notification.

[40] I find the RM conducted an adequate investigation.

[41] I find that by implementing a new email system, the RM has taken adequate steps to prevent the Hamlet Chairperson from breaching personal email addresses in the future.

IV RECOMMENDATIONS

[42] I recommend the RM ensures the email service it is using is properly safeguarded to protect personal information, and that it has a written policy on its use.

[43] I reiterate my recommendation for the RM to implement the recommendations listed at paragraph [33] and recommend the RM implement these recommendations within six months of the issuance of this Investigation Report.

Dated at Regina, in the Province of Saskatchewan, this 20th day of December, 2022.

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