Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 211-2024

Rural Municipality of Meota No. 468

February 7, 2025

Summary: The Complainant was concerned that a member of the Hamlet of Lakeview board, which is part of the Rural Municipality of Meota No. 468 (RM) breached their privacy by including their personal email address (as well as those of others) in conducting hamlet business. The Complainant raised further concerns, including continued breaches by the same board member as well as by other RM officials. The Complainant asked the A/Commissioner to investigate. The A/Commissioner found that breaches had occurred, and that while the RM did make efforts at containment, notification, investigation, and prevention for some of the breaches, the A/Commissioner found the RM could do more overall to meet its obligations to protect personal information pursuant to *The Local Authority Freedom of Information and Protection of Privacy Act*. As such, the A/Commissioner made several recommendations to the RM, which are outlined in this Investigation Report.

I BACKGROUND

[1] On July 11, 2023, a board member (board member A) for the Organized Hamlet of Lakeview (Hamlet) within the Rural Municipality of Meota No. 468 (RM) sent a mass email to property owners without using the blind carbon copy (bcc) line to mask personal email addresses. The email was in relation to "Beach weed pick up," and so was related to Hamlet business. According to the RM, board member A sent the email to 138 recipients. The Complainant was one of the individuals who had received the email, and so was affected.

[2] By email on July 15, 2023, the Complainant advised the RM of the breach. The Complainant raised their various concerns and asked the RM why it had not taken steps to contain it.

[3] By email on July 16, 2023, board member A apologized to the Complainant, stating it was not their intention to commit a breach. The same day, the Chief Administrative Officer (CAO) sent an email to those who received board member A's email (of July 11, 2023) to advise that a breach had occurred. The CAO explained that the email had not followed the RM's protocol to use the bcc line and apologized for not taking action to contain the breach. The CAO asked recipients to delete the July 11, 2023, email and to confirm deletion with the RM. The CAO added that the RM would further investigate and advised recipients that they could make a complaint to my office.

[4] On May 30, 2024, the following occurred:

- At 5:09 p.m. board member A sent another mass email to property owners without using the bcc line.
- At 5:13 p.m., a member of the Jackfish Lake Water Board (board member B) replied all to board member A's email; they did not use the bcc line.
- At 5:53 p.m., the CAO sent an email to all property owners (without apparently using the bcc line) advising that board member A's email of 5:09 p.m. violated the hamlet's email policy when they did not use the bcc line. Again, the CAO asked recipients to delete the email and advise the RM when they had done so. The CAO also advised recipients could make a complaint to my office.
- At 5:59 p.m., board member A sent another mass email (without using the bcc line) asking recipients to delete the email "sent at 5:06pm" [the email from 5:09 p.m.] and that a "new email will be sent asap."

[5] On June 15, 2024, the Complainant made a complaint to my office, citing numerous concerns with the continued breaches, including that the email distribution list being used was not current (or that the email was copied to individuals unrelated to the hamlet). In their submission, which the Complainant provided to my office on September 2, 2024, they added the following further concerns:

- Board member A had sent an email to property owners without using the bcc line on May 31, 2023 (or previous to their July 11, 2023 email).

- Various RM officials had, as outlined in the previous paragraph, committed repeated breaches, and the RM had not addressed all of them.

- In May 2024, board member A began using what appears to be their personal work "credentials", which the Applicant felt could have led to further, unidentified breaches.

- In June 2024, board member A sent an email to property owners regarding a vote and used an incorrect return address for the individual votes. The concern was that prior to board member A sending out a correction, property owners may have sent their responses to a "random email address", and their responses would have included their name, signature and personal email address.

[6] On October 24, 2024, the RM provided my office with a completed copy of my office's "Privacy Breach Investigation Questionnaire for Public Bodies" and supporting documentation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] As noted, this investigation involves a matter where a board member of the Hamlet sent out a mass email to property owners without using the bcc line. Subsection 2(1)(f)(i) of *The Local Authority Freed of Information and Protection of Privacy Act* (LA FOIP) states that a municipality qualifies as a local authority.

[8] In my office's, Investigation Report 166-2021, concerning the Rural Municipality of North Qu'Appelle No. 187, I considered the following at paragraphs [5] to [7] regarding organized hamlets:

> [5] Section 2(f)(i) of LA FOIP provides that a municipality qualifies as a local authority. *The Municipalities Act* defines a municipality at section 2(1)(w) as "a town, village, resort village, rural municipality or restructure municipality." Section 2(1)(rr) of *The Municipalities Act* provides that rural municipality "means a rural municipality incorporated or continued pursuant to this Act." Organized Hamlet is defined at section

> 2(1)(x) of *The Municipalities Act* as "an area declared to be an organized hamlet by order of the minister pursuant to this Act or any former Act providing for the establishment of organized hamlets."

[6] Further, sections 49(3) and 51(1) of *The Municipalities Act* provides:

> **49**(3) Notwithstanding any other provision of this Act, at the request of a hamlet board, the minister may designate an organized hamlet with a population in excess of 100 as a separate division within the rural municipality in which the organized hamlet is located, to be represented by its own councillor.
> …
>
> **51**(1) Subject to subsections (2) and (3), the persons within an organized hamlet may apply to the minister, in accordance with the procedures set out in Division 2 for the incorporation of the organized hamlet as a resort village or village.

[7] The Government of Saskatchewan's website provides the following regarding organized hamlets:

> Organized hamlets (OH) are designated by Minister's order, have a legal boundary and are also governed by a RM. The residents of an OH elect a three-person advisory board to represent the community to the RM council. The RM is the legal governing body…

[9] The Hamlet is within the RM. As the RM is a local authority, I find that there is a local authority involved pursuant to subsection 2(1)(f)(i) of LA FOIP.

[10] I therefore, have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

[11] A privacy breach occurs when there is an unauthorized collection, use and/or disclosure of personal information (*Guide to LA FOIP*, Chapter 6: "Protection of Privacy", updated February 27, 2023 [*Guide to LA FOIP*, Ch. 6], p. 234). There must be personal information involved, it must be in the possession or control of the RM, and the RM must have not had authority to disclose it.

[12] The list provided for at subsection 23(1) of LA FOIP is not exhaustive; to be personal information, the information: 1) must be about an identifiable individual; and 2) must be personal in nature. In this matter, I am dealing with email addresses of property owners. In many cases, the emails in question contain the recipient's first or last name, or some combination thereof. In my office's Investigation Report 166-2021 and Investigation Report 212-2019, I considered that someone's personal, non-business-related email address that contains either a "partial" or "full" name is personal information as it is capable of identifying someone, and is personal to them; thus it is personal information. It appears that this is the case for the Complainant. I am satisfied that there is personal information involved in this matter.

[13] Even though I note there is personal information involved, I also acknowledge that some of the email addresses would not qualify as personal information. In past reports, I have stated that email addresses used for business purposes (e.g., board members who may use their personal email addresses for board purposes) are not personal in nature, and so do not qualify as personal information. This includes email addresses individuals use in relation to a business or their work. Upon review, several of the email addresses in question appear to fall into this category, and so a use or disclosure without consent would not result in a privacy breach. For more information on use of email addresses in this context, see my office's Review Report 138-2021, 185-2021 and Review Report 320-2023.

[14] Where there are email addresses that qualify as personal information, to have possession of a record means to have physical possession plus a measure of control. To have control of a record means to have authority for how a record is managed, including how it is restricted, regulated, administered, disclosed, and/or disposed. As the RM apparently collected the email addresses from property owners to use for purposes such as circulating documents, the email addresses are in the RM's possession. The RM also has control over factors such as how it restricts access to the email addresses.

[15] Regarding its ability to disclose the email addresses in question amongst property owners, the RM did not state whether it had the consent(s) of the property owners to do so. The RM also did not state whether it had authority to disclose the email addresses without consent

pursuant to subsection 28(2) of LA FOIP. Rather, the RM does not dispute that a privacy breach occurred regarding the email that board member A sent July 11, 2023. I agree that this was a privacy breach. For the purposes of this investigation and for the same reasons, I also consider that the additional unauthorized disclosures of personal email addresses cited in the background of this Investigation Report also constitute privacy breaches.

[16] Based on this information, I find that privacy breaches occurred.

3. Did the RM respond appropriately to the privacy breaches?

[17] After determining that a privacy breach occurred, I shift to determining if the local authority undertook an appropriate response by addressing the following steps:

- Contain the breach (as soon as possible);
- Notify affected individuals (as soon as possible);
- Investigate the breach; and
- Prevent future breaches.

(*Guide to LA FOIP*, Ch. 6, p. 236)

[18] I will separately assess each step.

Contain the breach (as soon as possible)

[19] It is important to take steps to contain a privacy breach as soon as possible to limit the risk that disclosure of personal information poses for affected individuals. The *Guide to LA FOIP*, Ch. 6 at page 236, suggests containment efforts may involve some or all the following:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.

- Revoking access to personal information.
- Correcting weaknesses in physical security.

[20] As noted, several breaches of personal information occurred when different RM officials did not use the bcc line when sending or responding to mass emails. The Complainant states that the RM addressed only one of the breaches. In the background to this Investigation Report, I outlined that the CAO addressed the breach committed by board member A on July 11, 2023, by emailing all recipients on July 16, 2023. The CAO's email advised recipients of the breach and instructed them to delete the email and send confirmation to the CAO. In an "Administrative Report" provided by the RM dated July 27, 2023 (which was to have been presented to council on August 2, 2023), it was stated that 32 recipients complied with the confirmation request, and one recipient asked to be removed from the RM's distribution list.

[21] Based on the information before me, I note that the CAO also sent a follow up email to property owners with the breach that board member A committed on May 30, 2024. It does not appear that the RM took the same step after each breach occurred. What the CAO advised in the emails, however, was appropriate in the circumstances - there just should have been a similar email sent in all breaches.

[22] Prior to taking the above step, another practice that local authorities should undertake when an email is sent in error is to first attempt to recall it if such a function is available through its email system. Recalling an email allows you to delete or replace it if you sent it in error. Recall does not always work depending on the email system, but it can support containment efforts. To be effective, a recall attempt should be made immediately after an email is sent in error. In its submission, the RM states that it did ask board member A to attempt a recall of their July 11, 2023 email, but it appears it would have occurred a few days after the breach occurred. Recalling an email a few days later may have not helped containment efforts that much but is nonetheless a step the RM should have taken.

[23] Based on what is outlined above, I find the RM didn't make reasonable attempts to contain every breach.

[24] As far as a recommendation, the RM provided my office with a copy of its "HAMLET E-MAIL" policy (email policy), which states that when a privacy breach occurs, the hamlet board is to follow the recommendations as set out in my office's Investigation Report 166-2021. That investigation report, concerning the Rural Municipality of North Qu'Appelle No. 187, laid out several recommendations related to the use of the bcc function when sending an email. I will reserve my recommendations for the RM to update its email policy at the end of this Investigation Report when I review the RM's plan for prevention.

Notify affected individuals (as soon as possible)

[25] Local authorities should notify individuals affected by a privacy breach as soon as possible after key facts about the breach have been established. My office's *Guide to LA FOIP*, Ch. 6 at pages 237-238, outlines that notices to affected individuals 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 the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and 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 the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[26] As stated, after board member A committed a breach on July 11, 2023, the CAO sent a follow up email to affected individuals on July 16, 2023, or five days later. The CAO included the following, in part, in their email:

> The RM received a complaint on Saturday July 15, 2023 at 11:28 a.m. of a privacy breach by a Hamlet board member for disclosing personal emails on a correspondence issued on Tuesday July 11, 2023 at 8:47 a.m. The subject line of the email is "Beach weed pick up". The correspondence did not follow protocol for use of the BCC function and as a result everyone on the email could view all email addresses. The complaint noted that the CAO (myself) was included in the email and that noting has been done to date to contain the breech. I offer my sincere apology for not recognizing and taking action to contain the breech.
>
> The RM was copied in the hamlet board member response to the complainant on Sunday July 16, 2023 at 7:44 a.m. The hamlet board member expressed appreciation for bringing the matter to their attention and indicated that they had not realized what had occurred and that it was not intentional.
>
> …
> I will be conducting further investigation into this incident and requesting Council include this matter on the Hamlet Agenda at the August 2, 2023 Council meeting. Hamlet agenda items are considered at 10:00 am. Should you wish to attend the Council meeting you may do so in person at RM office located at 300-1st Street East in Meota, SK…
>
> ….
> You can protect your personal information by making request to the hamlet board to be removed from their email list…You have the right to make a complaint to the Privacy Commissioner, the form is attached…

[27] The CAO sent a similar notice when board member A again committed a breach on May 30, 2024. Based on what is outlined above, the RM's notice contained elements appropriate to a breach of this nature. The RM should have provided notice in this breach sooner, and it also should have provided such notice after every breach occurred. While the detail the RM provided in its notice to affected recipients was adequate in the circumstances, I find that it did not provide notice for every breach.

Investigate the breach

[28] Once a breach has been contained, the next step is to investigate it. This step includes identifying the root cause of the privacy breach (*Guide to LA FOIP*, Ch. 6, pp. 238-240). The root cause can be thought of what enabled someone to make an error, such as sending an email without using the bcc function.

[29] In its submission, the RM spoke to the breach that occurred on July 11, 2023 committed by board member A. As mentioned, the RM stated that 138 property owners were affected by this breach. The RM did not speak to what safeguards were in place prior to that breach occurring but did discuss training it provided to hamlet board members in November 2023 on its newly implemented hamlet email policy (dated October 4, 2023); as stated previously, I will speak to this policy in the prevention part of this Investigation Report.

[30] It is obvious that each of the breaches occurred because all the individuals who committed them did not use the bcc function. There are various reasons why they may have done so, including carelessness, not knowing how to use the bcc function, or lack of training. The root cause of such breaches, however, can indicate a lack of administrative and technical safeguards that prevent the breaches from occurring in the first place. A local authority is required to have both administrative and technical safeguards in place to protect personal information. These obligations are outlined at subsection 23.1 of LA FOIP as follows:

> **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.

[31] An administrative safeguard includes controls that focus on a local authority's policies, procedures and maintenance of security measures that protect personal information. Examples are written policies and procedures, annual training, confidentiality agreements, auditing programs, etc. A technical safeguard includes policies and procedures for using technology, such as having separate user identification, firewalls, virus scanners, etc.

[32] It is not clear that the RM had (or has) sufficient technical and administrative safeguards to prevent any of the breaches that have occurred. The RM also did not state what steps it took to determine why any of the breaches occurred, even after it implemented its email policy. As such, I find that the RM has not adequately investigated the root cause of the privacy breaches.

Prevent future breaches

[33] The most important part of responding to a privacy breach is to implement measures to prevent breaches of the same type from repeating (*Guide to LA FOIP*, Ch. 6, p. 243). In this case, it would be to ensure there is proper and effective use of the bcc function, but local authorities also need to be aware of an overall need to protect personal information that is in its possession or control.

[34] As outlined in the background to this Investigation Report, the Complainant raised several additional concerns with how the RM manages personal information. These include not using a current distribution list (or emailing individuals who are unrelated to the hamlet), using incorrect return addresses for voting, and using personal credentials to conduct public business.

[35] Regarding prevention, the RM stated that it held board member training for the email policy on November 2, 2023, during which it discussed the complaint made by the Complainant and the new hamlet email policy (which was developed/implemented in October 2023).

[36] The fact that board member A (and board member B and the CAO) continued to not use the bcc function even after a policy was implemented, is a clear indicator that more should

be done to ensure a change in practice. There also needs to be procedures or guidelines, training, and other measures such as technical ones that help prevent privacy breaches. The RM stated it could consider using a third-party email system, which may be an option, but the use of information management service providers (IMSP) can create other privacy issues, such as breaches that may occur on those platforms. When a local authority uses an IMSP, it remains responsible pursuant to LA FOIP for what agreement it has in place with the IMSP that meets the requirements to protect personal information set out in LA FOIP (use of an IMSP is set out in section 23.2 of LA FOIP and section 8.2 of *The Local Authority Freedom of Information and Protection of Privacy Regulations*). My office has often said that public bodies cannot contract out of their responsibilities under the province's privacy laws (e.g., Investigation Report F-2013-001). Any local authority considering third-party email management, then, needs to be aware of its continued responsibilities under LA FOIP.

[37] The RM also provided my office with a copy of its "LOCAL AUTHORITY FREEDOM OF INFORMATION & PROTECTION OF PRIVACY ACT" dated "February 16, 2019." The policy itself has only a statement indicating that the CAO is appointed the head pursuant to LA FOIP. If the RM has any policies and procedures regarding its overall obligations regarding the collection, use, disclosure and disposition of personal information, or its administrative and technical safeguards, they do not appear to be part of this policy.

[38] Considering what has been outlined in this Investigation Report including other concerns the Complainant raised, this brings me to my finding and recommendations.

[39] Because the RM has continued to make the same error of not using the bcc function when sending a mass email to property owners, I find its plan to prevent the same breach from reoccurring is not sufficient. The RM also appears to lack proper policies and procedures intended to help board members understand their roles and responsibilities according to LA FOIP; outside of my finding on the email breaches, I also make recommendations to help the RM address this.

[40] I recommend that the RM undertake the following to address privacy breaches by email and to ensure its overall compliance with its obligations pursuant to LA FOIP:

1. That the RM explore ways its email system can default to using the bcc line when it sends emails containing personal email addresses, or that it simply implements a rule where RM officials cannot send an email containing personal email addresses unless it has been reviewed by another RM official. These should be outlined in the RM's LA FOIP policies and procedures.

2. That the RM amend its "HAMLET E-MAIL" policy to clearly state what steps the RM will take when a breach utilizing email occurs. The policy and procedures should clearly outline that the person who sent the email in error will immediately attempt to recall it. As a second step, a designated person should send a follow up email to recipients (using the bcc function) referring to the email sent in error. The email should ask recipients to not forward, disseminate or save the email, to delete it from their inbox and deleted items folders, and then to confirm with the designated person that they have done all this. The policy and procedures should clearly state that this process will be followed anytime a privacy breach occurs by email.

3. That the RM develop policies and procedures that address the collection, use, disclosure and disposition of personal information (including personal email addresses) and how it will safeguard personal information, including through the use of technologies. This includes considerations for if it decides to use an IMSP to manage emails containing personal information.

4. That the RM train board members on access and privacy policies and procedures annually and the obligation to protect personal information pursuant to LA FOIP. These individuals should also annually sign an oath of confidentiality.

5. That the RM assign RM email addresses to board members and require that they only use those to conduct official RM business.

[41] As a reminder, my office does not do the work for any public body or trustee; my office is however, available to comment on any draft policies and procedures the RM plans to implement. Through a consultation, my office can provide feedback on proposed policies and procedures and help identify areas where the RM may wish to focus attention (see my office's Consultation Request Form).

IV FINDINGS

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

[43] I find that privacy breaches occurred.

[44] I find the RM did not make reasonable attempts to contain every privacy breach.

[45] I find that the RM did not provide notice for every breach.

[46] I find that the RM has not adequately investigated the root cause of the privacy breaches.

[47] I find the RM's plan to prevent the same breaches from reoccurring is not sufficient.

V RECOMMENDATIONS

[48] I recommend that the RM explore ways its email system can default to using the bcc line when it sends emails containing personal email addresses, or that it simply implements a rule where RM officials cannot send an email containing personal email addresses unless it has been reviewed by another RM official. These should be outlined in the RM's LA FOIP policies and procedures.

[49] I recommend that the RM amend its "HAMLET E-MAIL" policy to clearly state what steps the RM will take when a breach utilizing email occurs. The policy and procedures should clearly outline that the person who sent the email in error will immediately attempt to recall it. As a second step, a designated person should send a follow up email to recipients (using the bcc function) referring to the email sent in error. The email should ask recipients to not forward, disseminate or save the email, to delete it from their inbox and deleted items folders, and then to confirm with the designated person that they have done all this. The policy and procedures should clearly state that this process will be followed anytime a privacy breach occurs by email.

[50] I recommend that the RM develop policies and procedures that address the collection, use, disclosure and disposition of personal information (including personal email addresses) and how it will safeguard personal information, including through the use of technologies.

This includes considerations for if it decides to use an IMSP to manage emails containing personal information.

[51] I recommend that the RM train board members on access and privacy policies and procedures annually and the obligation to protect personal information pursuant to LA FOIP. These individuals should also annually sign an oath of confidentiality.

[52] I recommend that the RM assign RM email addresses to board members and require that they only use those to conduct official RM business.

Dated at Regina, in the Province of Saskatchewan, this 7th day of February, 2025.

Ronald J. Kruzeniski, KC
A/Saskatchewan Information and Privacy Commissioner