Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 168-2025, 180-2025

Town of Radisson

November 3, 2025

Summary: The Town of Radisson (Town) sent e-notices for utility billing to 180 e-notice subscribers, in two batches of 90. In the second batch, the Town intended to attach a copy of its monthly newsletter but inadvertently attached a 180-page document with the utility billing information for all 180 Town utility accounts of individuals and businesses (utility bill spreadsheet). Two of the e-notice recipients (Complainant 1 and Complainant 2) who received the utility bill spreadsheet submitted privacy breach complaints to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). Both Complainants' personal information was included in the utility bill spreadsheet. OIPC investigated the incident under *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*) and found that a privacy breach occurred when the Town disclosed the personal information of 207 identifiable individuals without authority under *LA FOIP*.

The Commissioner found that the Town: (1) has not made all reasonable efforts it could have to contain the privacy breach; (2) provided adequate and timely notification to the affected individuals; (3) made reasonable efforts to investigate the privacy breach; (4) did not meet its "duty to protect" pursuant to section 23.1 (duty of local authority to protect) of *LA FOIP*; and (5) has taken reasonable steps to change its practices to assist in preventing a similar privacy breach in the future. The Commissioner recommended that the Town follow up with the email recipients that have not responded to ensure they have followed the instructions to destroy the errant email, not retain copies of the email and not distribute the email.

I BACKGROUND

[1] On July 3, 2025, the Town of Radisson (the Town) sent e-notices for utility billings to 180 e-notice subscribers, in two batches of 90. In the second batch, one of the recipients (Complainant 1) received an email that stated: "please find attached your utility bill for the 2025-06-01 – 2025-06-30 and newsletter attached." Attached to the email were two documents: (1) a one-page *Utility Notice* in Complainant 1's name; and (2) a 180-page document with utility billing information for all 180 Town utility accounts of individuals and businesses within the local authority's jurisdiction (utility bill spreadsheet).

[2] The next day, Complainant 1 forwarded this email, with the attachments, to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). In their email to OIPC, Complainant 1 claimed that the attachments were "sent to each Rate Payer" in the Town and expressed concerns that their personal "information is now in the full and complete public domain…". OIPC reviewed the utility bill spreadsheet and confirmed Complainant 1 to be an affected individual. OIPC opened file 168-2025 in relation to this privacy breach complaint.

[3] On July 4, 2025, OIPC contacted the Town regarding this email. The Town confirmed that the day before, the utility bill spreadsheet was emailed to 90 e-billing residents in the Town in error. The Town learned of this incident a few minutes after the e-notices were sent when a resident reported it to the Town.

[4] On July 7, 2025, the Town forwarded OIPC its internal privacy breach investigation report and a copy of the notices that would be mailed to affected individuals on the following day, July 8, 2025.

[5] On July 15, 2025, Complainant 2 contacted OIPC stating, "I am a resident of Radisson and am one of the 90 recipients of the email attachment as well as one of the 180 billings that was disclosed." OIPC responded on the same day advising that this office was in receipt of the utility bill spreadsheet in question. OIPC noted that if Complainant 2 wished to file a privacy breach complaint, they would need to provide: (1) their full name, including

middle name; and (2) address (box number of physical address) to allow confirmation that they were an affected individual. Complainant 2 provided the requested information on the same day, and confirmation was established. OIPC opened file 180-2025 in relation to this privacy breach complaint.

[6] On August 15, 2025, OIPC emailed the Town and the two Complainants notices of an investigation.

[7] On August 21, 2025, the Town provided OIPC with its completed *Privacy Breach Investigation Questionnaire* (the Questionnaire),[1] and other relevant documentation. On August 17, 2025, Complainant 1 provided OIPC with their representations regarding this incident. On September 4, 2025, Complainant 2 emailed their privacy concerns to this office.

II DISCUSSION OF THE ISSUES

1. Jurisdiction

[8] The Town qualifies as a "local authority" pursuant to section 2(1)(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (*LA FOIP*).[2] Therefore, OIPC has jurisdiction and is undertaking this investigation pursuant to section 32 of *LA FOIP*.

2. Did a privacy breach occur?

[9] A privacy breach occurs when personal information is collected, used and/or disclosed in a way that is not authorized by *LA FOIP*. The first step in determining if a privacy breach has occurred is to identify if personal information is involved in this matter. If so, then the

[1] See OIPC *Privacy Breach Investigation Questionnaire*.

[2] *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. L-27.1, as amended.

second step is to determine if the personal information was collected, used and/or disclosed in a way that was not authorized by *LA FOIP*.[3]

a. Is personal information involved in this matter?

[10] Personal information is defined by means of a long list in section 23(1) of *LA FOIP*, though the list is not exhaustive. Personal information is information that is about an identifiable individual, and that is personal in nature. Information is about an identifiable individual *if* the individual can be identified from the information; examples include a person's name or social insurance number. Further, information is personal in nature if it provides something identifiable about the individual.[4]

[11] From a review of the utility bill spreadsheet, the information at issue includes columns that contained:

- Name,
- Mailing address,
- Physical address,
- Account number,
- Current billing amount,
- Outstanding charges/credits on account, and
- Total due.

[12] Each page of the utility bill spreadsheet is devoted to a different account number with an associated utility bill. The Town stipulated there were 180 accounts and these accounts made up the list of affected individuals and that the monthly billed amount was the same for each customer.

[13] This office reviewed the utility bill spreadsheet and found several irregularities such as:

- instances where an account was associated with the name of a business without an associated name of an individual;

[3] See OIPC Investigation Report 003-2025, 035-2025 at paragraph [17].

[4] *Ibid*, at paragraph [18].

- instances where the same individual is listed for multiple accounts; and
- instances where more than one individual was listed on the account.

[14] In addition, there were 21 utility accounts that had a monthly billing amount that differed from the unified amount the Town represented all customers were billed. Based on a count by this office, there were a total of 207 identifiable individuals in this matter that had their personal information disclosed without their consent.

[15] There is no question that the information on the utility bill spreadsheet qualifies as personal information pursuant to sections 23(1)(d), (e), (j) and (k)(i) of *LA FOIP* which provides as follows:[5]

> **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:
>
> …
> (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;
>
> …
> (j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or

[5] See OIPC Investigation Report 072/2014 at paragraphs [29] and [32] where an individual's name, account number and balance owing on their account qualified as personal information pursuant to sections 24(1)(d), (j) and (k)(i) of *The Freedom of Information and Protection of Privacy Act* (*FOIP*), which is the equivalent of sections 23(1)(d), (j) and (k)(i) of *LA FOIP*; See also OIPC Review Report 137-2024 at paragraph [36] where an individual's home and/or mailing address was found to be personal information pursuant to section 24(1)(e) of *FOIP*, which is the equivalent of section 23(1)(e) of *LA FOIP*.

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

[16] While *LA FOIP* does not define the term "disclosure", this office has previously defined the term as the sharing of personal information with a separate entity, not a division or branch of the local authority in possession or control of that information.[6]

[17] In this case, the Town inadvertently selected the utility bill spreadsheet to attach to its system generated e-notices that it sent to the 90 recipients. This resulted in the Town disclosing the personal information of 207 identifiable individuals without their consent.

[18] Section 28(1) of *LA FOIP* states:

> **28**(1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.

[19] The Town, quite reasonably, immediately conceded a privacy breach upon learning that the utility bill spreadsheet was sent to a list of 90 individuals without authority. Section 28(1) of *LA FOIP* prohibits the Town from disclosing personal information, unless it has obtained consent from the subject individuals or if it has authority for the disclosure without consent. *LA FOIP* requires local authorities to determine its authority to disclose personal information prior to a disclosure.[7] The Town did not have the consent of the individuals to whom the information relates, nor did it identify its authority for disclosure prior to the disclosure. This breach was the result of an inadvertent and unintentional mistake on the part of the Town. There will be a finding that that a privacy breach occurred when the Town disclosed the personal information of the 207 identifiable individuals without authority under *LA FOIP*.

[6] See OIPC Investigation Report 065-2025 at paragraph [18].

[7] *Ibid*, footnote 6 at paragraph [33].

3. Did the Town respond to the privacy breach appropriately?

[20] The response to a privacy breach by a local authority involves a consideration of several factors. Section 6-7 of OIPC *Rules of Procedure* assists in the analysis. In this case, those considerations include:

a. Has the local authority contained the breach as soon as possible?

b. Has the local authority notified all affected individuals as soon as possible?

c. Has the local authority investigated the breach?

d. Has the local authority taken concrete steps to prevent future breaches?

a. Containment of the Breach

[21] Upon learning that a privacy breach occurred, local authorities should take immediate steps to contain the breach. Depending on the nature of the breach, this can include:[8]

- Stopping the unauthorized practice that caused the breach;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.

[22] This office applies a standard of reasonableness to a local authority's actions taken with respect to the containment of a breach. The local authority must demonstrate that it has reduced both the magnitude of the breach and the resulting risk to affected individuals. This measure serves as a reassurance to the public. A privacy breach is a very serious matter. A privacy breach always results in a loss of faith and trust on the part of the public

[8] *Supra*, footnote 3 at paragraph [34].

in the local authority, and a loss of faith and trust on the part of the citizens the local authority serves.[9]

[23] Complainant 1 provided evidence that corroborated the delivery of the utility bill spreadsheet on July 3, 2025, at 3:06 p.m. by the Town. The Town reported that between 3:11 and 3:16 p.m., a resident called and alerted the Town to the breach. The Town Administrator investigated hoping that "it was a technical error and possible an error in the script on the part of MuniSoft". The Town Administrator immediately contacted both the IT Support Team and Munisoft. The Town Administrator also posted an immediate notice on the Radisson Community Facebook page stating:

> Technical Difficulties
>
> Our IT Support Team and MuniSoft Software Team are experiencing technical difficulties and in error set up the software to send out the entire listing of all accounts in a separate pdf to all e-utility residents.
>
> Please disregard the pdf that is named July 1st and only open the one with your name on it.
>
> We are working with IT Support and MuniSoft to correct this matter immediately and apologies for it.
>
> [Emphasis added]

[24] The Town took further steps to remedy the breach. By 4:30 p.m. on July 3, 2025, it attempted, unsuccessfully, to recall the emails. To be effective, a recall attempt should be made within seconds of sending an email in error.[10]

[25] On July 4, 2025, the Town sent emails to the 90 e-notice recipients who received the utility bill spreadsheet and requested the following:[11]

[9] *Supra*, footnote 6 at paragraph [24].

[10] See OIPC Investigation Report 211-2024 at paragraph [22].

[11] The Town provided a copy of one of these emails, which was dated July 4, 2025, at 2:28 p.m.

1. DO NOT OPEN THE PDF ENTITLED JULY 1ST
2. DO NOT RETAIN A COPY
3. DO NOT FORWARD A COPY
4. DELETE ALL COPIES
5. CONFIRM THAT THE ABOVE HAS BEEN DONE BY RETURN EMAIL TO THE TOWN AT town@radisson.ca

[26] On September 12, 2025, the Town confirmed with OIPC that it received emails from 15 residents confirming that the email was destroyed.

[27] Privacy best practices state that a local authority should attempt to retrieve personal information that has "gone astray."[12] In past investigation reports where errant emails were involved, OIPC has considered what reasonable steps should be taken to contain a breach including: (1) attempting to recall an email. This should be done within seconds of sending an email in error and can only be effected with immediate knowledge of the error; (2) notifying the email recipients of the breach and instructing email recipients to destroy the errant email, instructing the recipients to not retain copies of the email and to not distribute the email; and (3) requesting the email recipients confirm, via response, that they have followed the instructions.[13]

[28] As outlined in this section of the Investigation Report, the Town has taken most of the steps recommended by this office when errant emails are involved. However, there is one troubling gap in the process. Less than 25% of the email recipients responded to the Town to confirm they followed the instructions to destroy the errant email/ not retain copies of the email and that they had warranted to not distribute the email further. Based on the information provided, the Town has not followed up with the rest of the email recipients to ensure the future dissemination of the email is prohibited.

[12] See OIPC Investigation Report 015-2025 at paragraph [48].

[13] Examples of past OIPC investigation reports include: Investigation Report 211-2024 at paragraphs [20] to [23]; Investigation Report 127-2022 at paragraphs [16] to [18]; Investigation Report 062-2022 at paragraphs [15] to [16]; Investigation Report 212-2019 at paragraph [16].

[29] Local authorities must take reasonable steps to try to reduce the magnitude of the privacy breach and the resulting risk to affected individuals. Given the limited number of responses the Town has received from the email recipients, there is no reassurance to affected individuals that their personal information has been effectively destroyed. There is a finding that the Town has not made all reasonable efforts it could have to contain the privacy breach. There will be a recommendation that the Town follow up with the email recipients that have not responded to ensure they have followed the instructions to destroy the errant email, not retain copies of the email and not distribute the email.

b. Notification to Affected Individuals

[30] Section 28.1 of *LA FOIP* requires local authorities to take all reasonable steps to notify affected individuals when it is believed the privacy breach creates a real risk of significant harm to the affected individuals:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[31] Whether there is a real risk of significant harm or not, it is still best practice for local authorities to inform affected individuals when their personal information has been involved in a privacy breach. The local authority must also identify possible risks to the affected individuals and inform them of steps they can take to protect themselves.[14]

[32] The information a local authority should include in a notice to affected individuals may include:[15]

[14] *Supra*, footnote 3 at paragraph [41]. See also OIPC resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[15] *Ibid,* at paragraph [42].

- 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 OIPC (provide OIPC's contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[33] The Town indicated it mailed letters to the affected individuals on July 8, 2025. The Town provided OIPC with a copy of these letters, which included the following elements:

- A description of how the privacy breach occurred;
- The personal information involved;
- Steps taken to contain the breach and prevent future breaches;
- An apology;
- That it does not believe there is a real risk of substantial harm, but notification was being provided to allow individuals to take any measures they believe are necessary; and
- Contact information for OIPC for individuals to direct questions or make a formal complaint.

[34] While there is not a real risk of significant harm as a result of *this* breach, offering advice to affected individuals on steps they can take to protect themselves is always important.

Complainant 1 expressed a concern that the privacy breach might result in unsolicited telephone calls or emails in the future. They provided a recent email from a licensed insolvency trustee which they found distressing. However, we note that individual telephone numbers and email addresses were not included in the utility bill spreadsheet so we cannot conclude that the insolvency communication was in any way related to the privacy breach.

[35] Institutions that have experienced major privacy breaches should always advise affected individuals to protect themselves with options that range from credit monitoring to meeting with banks and police/security authorities to protect against identity theft.[16]

[36] Complainant 2 complained to this office that the Town provided an incorrect email address for a specific OIPC employee in its notification to the affected individuals. While it is highly commendable that the Town alerted the affected individuals of their right to complain to this office, we hope first that the Town never experiences a privacy breach in the future. But if it does, we ask that the Town direct affected individuals to the general email address to facilitate the receipt and investigation of future privacy breaches. A notice should also include the contact information for a Town employee to provide informational assistance as well.

[37] There is a finding that the Town provided adequate and timely notification to the affected individuals.

c. Investigation of the Breach

[38] Once containment has been addressed and appropriate notification given, the local authority should investigate the breach. The investigation must address the incident on a systemic basis and include a root cause analysis and conclusion. The local authority must consider its duty to protect personal information as set out at section 23.1 of *LA FOIP*.

[16] See OIPC Investigation Report 208-2021 at paragraph [32].

Specifically, section 23.1 of *LA FOIP* requires that local authorities establish policies and procedures to maintain administrative, technical and physical safeguards:

> **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.

[39] In assessing the root cause of a privacy breach, the local authority must formulate safeguards that would have prevented the privacy breach from occurring. Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts), technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras).[17]

[40] Some key issues to consider in determining the proper safeguards include:

When and how did your organization learn of the privacy breach?

- Has the privacy breach been contained?
- What efforts has your organization made to contain the breach?

What occurred?

- What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.)?
- What personal information was involved in the privacy breach?

[17] *Supra*, footnote 6 at paragraph [31].

- When did the privacy breach occur? What are the timelines?
- Where did the privacy breach occur?

How did the privacy breach occur?

- Who was involved?
- What employees, if any, were involved with the privacy breach?
- What privacy training have they received?
- Who witnessed the privacy breach?
- What factors or circumstances contributed to the privacy breach?
- What is the root cause of the breach?

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?

- Were the safeguards, policies, and procedures followed?
- If no safeguards, policies, or procedures were in place, why not?
- Were the individuals involved aware of the safeguards, policies, and procedures?

Who are the affected individuals?

- How many are there?
- What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.)?
- Have affected individuals been notified of the privacy breach?

[41] The Town Administrator initially believed the breach was the result of difficulties with the new software that forwards the utility e-notices. The Town requested that its software provider investigate how this breach could have occurred. The Town Administrator conceded that a script error may have resulted in the utility bill spreadsheet being attached to the e-notices, rather than the monthly newsletter. The investigation revealed, however, that the Town Administrator must have inadvertently chosen the wrong attachment and added it to the e-notices. The software does not allow for viewing of the attachment after it is selected, and the Town Administrator could not recall if the name of the attachment was visible after the attachment was selected. The Town concluded that the root cause was multi-fold: human error, software weakness, and new computer system challenges.

[42] This office accepts that the Town correctly identified the root cause of the privacy breach to be technical difficulties and employee error.

[43] At the time this privacy breach occurred, there was also a lack of administrative controls in place to assist the Town in meeting its "duty to protect" pursuant to section 23.1 of *LA FOIP*. The Town did not have a policy, procedure or work standard guiding employees on steps to take when attaching documents to emails. The Town Administrator also indicated that training was not provided on the steps to take when attaching documents to emails.

[44] The Town provided OIPC with details of its change in practices as a result of this privacy breach and how it intends to prevent a similar privacy breach from occurring in the future. This will be discussed in the next segment where we discuss the prevention measures implemented by the Town.

[45] There is a finding that the Town made reasonable efforts to investigate the privacy breach, but that the Town did not meet its "duty to protect" pursuant to section 23.1 of *LA FOIP*.

d. Prevention of Future Breaches

[46] It is crucial to ensure the implementation of vital measures to prevent similar breaches from occurring in the future. Possible prevention measures may include adding/enhancing safeguards already in place, the provision of additional training, and the regular monitoring/auditing of systems and system users. The following considerations are relevant:[18]

- 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 current practice be stopped?

[18] *Supra*, footnote 6 at paragraph [36].

[47] As a result of this privacy breach, the Town changed its practices for the delivery of newsletters, stating "attachments will no longer be added to e-notices; the newsletters will go out as a mail flyer via Canada Post." The Town also developed a policy: *Protocols and Process for Adding an Attachment.* This policy was approved by Town Council on August 27, 2025, and outlines:

> 4.1 Attachments shall not be added to utility e-notices as it is not possible to verify the attachment prior to hitting the send button;
>
> 4.2 For any email that requires an attachment to be added, after adding the attachment to the email and prior to hitting send, the sender is to open the attachment to confirm that it is the proper one to be attached to the email.

[48] This is a commendable step for the Town. It not only addresses administrative deficiencies but it helps to prevent similar future breaches. There is a finding that the Town has taken reasonable steps to change its practices to assist in preventing a similar privacy breach in the future.

[49] The Town also indicated that it is currently working on developing a written policy for responding to a privacy breach as well as a policy for the protection of privacy.[19] We applaud the efforts of the Town and we welcome an opportunity to review and consult once the policies are developed.[20] While this office can never draft such documents, we are happy to provide any consultative assistance if requested.

III FINDINGS

[50] OIPC has jurisdiction to undertake this investigation.

[51] A privacy breach occurred when the Town disclosed the personal information of 207 individuals without authority under *LA FOIP*.

---

[19] Section 23.1 of *LA FOIP* requires a written policies and/or procedures and are crucial in the event of staff turnover. As an example, see OIPC Investigation Report 065-2025 at paragraph [40].

[20] See OIPC *Consultation Request Form*.

[52] The Town has not made all reasonable efforts it could have to contain the privacy breach.

[53] The Town provided adequate and timely notification to the affected individuals.

[54] The Town made reasonable efforts to investigate the privacy breach.

[55] The Town did not meet its "duty to protect" pursuant to section 23.1 of *LA FOIP*.

[56] The Town has taken reasonable steps to change its practices to assist in preventing a similar privacy breach in the future.

IV RECOMMENDATION

[57] I recommend that the Town follow up with the email recipients that have not responded to ensure they have followed the instructions to destroy the errant email, not retain copies of the email and not distribute the email.

Dated at Regina, in the Province of Saskatchewan, this 3rd day of November, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner