Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 065-2025

Town of Unity

August 18, 2025

Summary: The Complainant is the landlord of a property in the Town of Unity (Town). The Town issued a utility bill days after the tenants moved out of the property. A month later, the Town emailed the Complainant and identified the tenants by name as well as the outstanding balance of their utility account. Eventually, the Town transferred the outstanding balance to the Complainant's property tax roll. Then, by letter, the Town informed the Complainant that it had transferred the outstanding balance to the Complainant's property tax roll. When the tenants electronically transferred payment to the Town, the Town applied the payment to the Complainant's property tax roll. The Town issued two receipts to the tenants. One of the receipts contained the Complainant's property tax roll number and civic address. The Complainant accessed both receipts from the Town's customer portal. The Complainant emailed a privacy complaint to the Town. When the Town did not respond, the Complainant requested that the Office of the Saskatchewan Information and Privacy Commissioner undertake an investigation.

The Commissioner made several findings, including that: 1) a privacy breach occurred when the Town disclosed the Complainant's personal information to the tenants; 2) the Town took steps to establish a procedure that prevents similar privacy breaches in the future; and 3) the Town's Policy 2.13 does not sufficiently address the root cause of the privacy breach.

The Commissioner recommended several actions that the Town undertake within 60 days of the issuance of this Review Report, including that: 1) the Town document in a written policy and/or procedure its process for issuing receipts when the payee is not the account holder; and 2) the Town amend its Policy 2.13 so that it provides guidance to employees on when they are authorized to use and disclose personal information.

I BACKGROUND

[1] The Complainant is the landlord of a property in the Town of Unity (Town). There were two separate tenants and each rented the property and had a utility account in each of their names. The tenants moved out of the property on August 31, 2024, and their final utility bill, dated September 3, 2024, registered an outstanding balance of $419.39. The Town indicated it intended to transfer that amount to the Complainant's property tax roll if it remained unpaid.

[2] On October 1, 2024, the Town introduced The Utility Management Bylaw. This bylaw provided that going forward, utility accounts must be registered in the property owner's name, not that of the renter. However, there was a grandfather clause that provided current utility accounts in a renter's name would remain in the renter's name until the tenant vacated the property.

[3] On October 10, 2024, the Town emailed the Complainant to inform that the tenants' outstanding balance of $419.39 would be transferred to the Complainant's property tax roll as of November 10, 2024.

[4] On October 23, 2024, the Complainant objected that the Town expected him to pay for the unpaid portion of a tenant's utility bill. The Complainant was also upset at the violation of his privacy and that of the tenants. The Complainant relayed his concerns to the Town in an email:

> The personal and private account of the former tenants [names of tenants] is confidential. We have had many conversations with [Name of Town employee A] and [Name of Town employee B] about how we can't under the privacy act share any information. We have no right or want any financial information on my tenants in the park, or any obligation to collect your outstanding amounts, you don't have the right to put this on our tax account.

[5] On December 3, 2024, the Complainant called the Town to inquire about a charge on their tax bill for $465.94 that included a $423.58 charge with $42.36 added as interest. On the

same day, the Town forwarded its email from October 10, 2024 in an effort to explain the charges.

[6] The Town wrote a letter to the Complainant on January 8, 2025. In that letter the Town noted that the tenants had still not paid the outstanding balance of their utility account and as such, the outstanding balance would be transferred to the Complainant's property tax roll as of February 8, 2025. Enclosed with the letter was a copy of the tenants' final utility bill, which included:

- The tenants' names;
- The tenants' new mailing address;
- The tenants' account number with the utility at the material time; and
- The outstanding balance.

[7] Subsequent to the January 8, 2025 letter, the tenants e-transferred $465.94 in full payment to the Town. The tenants then received two receipts from the Town – a "general receipt" and a "tax receipt" both dated January 20, 2025. Both receipts were addressed to the tenants, and both receipts contained the tenants' names and new mailing address. The tax receipt also provided the Complainant's property tax roll number and the Complainant's civic address. The tenants forwarded both receipts to the Complainant. The Complainant also accessed both receipts via the Town's customer portal.

[8] On January 29, 2025, the Complainant sent an email to the Town detailing their privacy concerns with respect to the Town's dissemination of both his and the tenants' personal information in the receipts.

[9] On March 20, 2025, the Complainant contacted the Office of the Saskatchewan Information and Privacy Commissioner (OIPC). The Complainant indicated that the Town remained non-responsive to their concern. The Complainant requested this office conduct an investigation.

[10] On April 14, 2025 the Town sent the Complainant an email with the following three attachments:

- **First attachment:** Letter from the Town dated April 14, 2025, to the Complainant. The Town conceded it had improperly disseminated the Complainant's account number[1] with the tenants. The Town apologized to the Complainant for the privacy breach and suggested a solution that included contacting the tenants to ensure they destroyed their copy of the tax receipt.

- **Second attachment:** A copy of a revised tax receipt that the Town was issuing to the tenants, with the Complainant's account information removed.

- **Third attachment:** A copy of a letter dated April 14, 2025, by the Town to the tenants. In this letter, the Town requested that the tenants delete/destroy the tax receipt.

[11] On May 13, 2025, OIPC notified the Town and the Applicant that an investigation would proceed. The notice outlined that the scope of the investigation would focus on the Town's disclosure of the Complainant's information to the tenants.

[12] On June 11, 2025, the Town provided its submission to OIPC. The Complainant did not provide a submission to OIPC.

II DISCUSSION OF THE ISSUES

1. Does OIPC have jurisdiction?

[13] The Town qualifies as a "local authority" as defined in section 2(1)(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)*. OIPC has jurisdiction and this investigation was conducted pursuant to section 32 of *LA FOIP*.

2. Did a privacy breach occur?

[1] This "account number" was the Complainant's property tax roll number as revealed on the tax receipt first sent to the tenants.

[14] A privacy breach occurs when a local authority collects, uses and/or discloses personal information without the authority of *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 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*.

a. Is personal information involved in this matter?

[15] Personal information is defined through the 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; a common example is if the information includes the name of the individual. Further, information is personal in nature if it provides something identifiable about the individual.[2]

[16] The Town issued a tax receipt to the tenants that contained the Complainant's property tax roll number and civic address. Sections 23(1)(d) and (e) 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:
>
> …
>
> (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;

[17] There is no question that the Complainant's property tax roll number[3] and civic address qualifies as personal information pursuant to sections 23(1)(d) and (e) of LA FOIP.

---

[2] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [14].

[3] In OIPC's Investigation Report LA-2007-002 at paragraph [33], OIPC had found that tax roll information qualifies as personal information.

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

[18] *LA FOIP* does not define the terms "collect, "use," or "disclosure". OIPC has defined the terms as follows:[4]

- "Collection" means the bring or come together, assemble, accumulate, obtain personal information from any source by any means.
- "Use" indicates the internal utilizations of personal information by a local authority and includes the sharing of the personal information in such a way that it remains under the control of the local authority.
- "Disclosure" is 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.

[19] The Town disclosed the Complainant's personal information to the tenants.

[20] 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.

[21] The Town, quite reasonably, conceded a privacy breach upon the disclosure of the Complainant's personal information in the tenants' tax receipt. There will be a finding that a privacy breach occurred when the Town disclosed the Complainant's personal information to the tenants without authority.

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

[22] The determination of a local authority's response to a privacy breach involves several considerations. Whether the local authority appropriately responds to a privacy breach and

[4] See OIPC Investigation Report 279-2024 paragraph [25] to [27].

takes proper correction measures is informed by sections 6-7 of OIPC's *Rules of Procedure*. The following considerations include:

(a) Was the breach contained;

(b) Were the affected individuals notified;

(c) Was the breach investigated; and

(d) Were appropriate steps taken to prevent future breaches.

a. Containment of the Breach

[23] Upon learning that a privacy breach has occurred, local authorities should take immediate steps to contain the breach. These steps will depend entirely upon the nature of the breach, but they may include:[5]

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

[24] This office applies a standard of reasonableness in analyzing the containment of a breach. The local authority must demonstrate that it has reduced 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 in the local authority, and a loss of faith and trust on the part of the citizens the local authority serves.[6]

[5] *Supra*, footnote 2, at paragraph [22]; see also OIPC's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*.
[6] *Supra*, footnote 2, at paragraph [23]. See also OIPC's resource *Privacy Breach Guidelines for Government institutions and Local Authorities*.

[25] On April 14, 2025, the Town sent an email to the tenants. Attached to the email was a letter of request on the part of the Town that the tenants delete or destroy the tax receipt. The Town followed up by email again on May 20, 2025, to confirm destruction or deletion of the tax receipt. The tenants confirmed full compliance with this request on the same date.

[26] There will be a finding that the Town has reasonably contained the privacy breach.

b. Notification to Affected Individuals

[27] It is best practice for local authorities to inform affected individuals as soon as possible when their personal information has been breached. This is an obvious and crucial step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps they deem necessary to protect themselves.[7]

[28] The information that a local authority should include in a notice to affected individuals may include:[8]

- 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 result from 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.

[7] *Supra*, footnote 2, paragraph [34]. See also OIPC's resource *Privacy Breach Guidelines for Government institutions and Local Authorities*.

[8] *Supra*, footnote 2, at paragraph [35]; see also OIPC's resource *Privacy Breach Guidelines for Government institutions and Local Authorities*.

- A notice that individuals have a right to complain to OIPC (provide contact information).

- Recognition of the impacts of the breach on affected individuals and an apology.

[29] In this case, it was the Complainant who discovered the Town's breach of their privacy and that of the tenants. As such, notification becomes irrelevant. However, in circumstances such as this a Town should explain the steps being taken to mitigate the harm and to prevent future breaches as well as offer an apology. We have noted that the Town did just this and we commend them for that. The Town sent the Complainant a letter dated April 14, 2025, where it addressed its plans for the rectification of the breach. These plans included notification of the tenants and a request to destroy the tax receipt. The Town also apologized to the Complainant in that letter. There will be a finding that the Town provided adequate notification to the Complainant of the remedial steps it was taking and the fact it was sorry for the breach of personal information in the first place.

c. Investigation of the Breach

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

[31] In assessing the root cause of a privacy breach, the local authority must formulate safeguards that would have prevented the privacy breach from occurring.[9] 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).

[32] In its submission, the Town identified two root causes of this breach. First, it noted that Town staff did not obtain the proper authority to convey the Complainant's information to the tenants via the tax receipt:

> Staff issued a standard tax receipt to the payors of a tax installment without verifying their authority to receive account-specific information related to the registered property owner.

[33] The Town's submission is correct. *LA FOIP* requires the Town to determine its authority to disclose personal information before it does so. In this case, the Town's actions violated sections 28(1), (2) and 29 of *LA FOIP* because the Town was never authorized to disclose either the tenants' or the Complainants' personal information to each other. There will be a recommendation that the Town familiarize itself with the privacy provisions set out in Part V of *LA FOIP*, including the collection, use and disclosure provisions. This would ensure that the Town always confirms its authority to disclose personal information before doing so.

[34] The Town correctly identified as the second root cause gaps in its processing of third-party payments when the payee is not the account holder. It did not specify the precise gaps in

[9] *Supra*, footnote 2, at paragraph [41]; see also OIPC's resource *Privacy Breach Guidelines for Government institutions and Local Authorities*.

its process but provided details of how it intended to prevent a similar privacy breach in its processing third-party payments. This will be discussed next in the analysis of the Town's prevention measures in the section below.

[35] There will be a finding that the Town made sufficient efforts to investigate the breach and identified areas in which it can improve.

d. Prevention of Future Breaches

[36] 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, providing additional training, and the regular monitoring/auditing of systems and system users. The following considerations are relevant:[10]

- 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?

Protection of the Privacy of Personal Information

[37] The Town explained that it will offer to mail the system-generated receipt to the account holder only when a payee, such as a tenant as in this case, is not the account holder. The Town noted that its system generates receipts only with account holder information. In this matter, the Town added the payee details into the "Payee Field" prior to issuing the receipt and that is how the tenants received the receipts. The Town warranted that in the future it

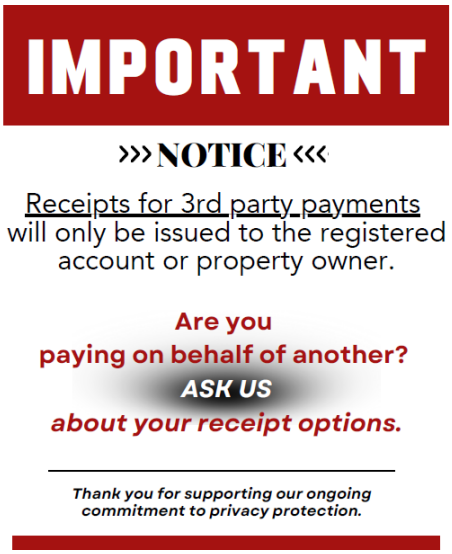
[10] *Supra*, footnote 2, at paragraph [50]; see also OIPC's resource *Privacy Breach Guidelines for Government institutions and Local Authorities*.

will only provide the receipt to the account holder and details of the payee will not be included.

[38] The Town also informed this office that it will provide a manually generated receipt to the payee, which will including the following:

- Date;
- Payee name;
- Dollar amount;
- Details of the payment (i.e. payment to Dad's property tax, payment to the landlord's utility); and
- Staff initials.

[39] The Town indicated that the new policy of issuing manual receipts when the payee is not the account holder is not formally recorded as of yet. However, it has provided training to its staff regarding this process. It has also posted a helpful sign at its reception desk to prompt individuals to ask the Town about receipt options:



[40] There will be a finding that the Town has taken reasonable steps to establish a procedure that will prevent a similar privacy breach in the future. There will be a recommendation

that the Town document its process in a written policy and/or procedure with respect to the new practice of issuing manual receipts when the payee is not the account holder. Even though the Town currently trains all staff on this new process, section 23.1 of *LA FOIP* requires a written policy and/or procedure. A written policy and/or procedure is crucial in the event of staff turnover. It would also inform residents and the public of the practice and provide assurances that the Town is managing personal information in accordance with *LA FOIP*.

Collection, Use and Disclosure of Personal Information

[41] On a separate note, the Town noted in its submission to this office that it revised its Policy 2.13 regarding *LA FOIP* and the collection, use and disclosure of personal information. The revisions to the policy were approved by council during its June 10, 2025, meeting and is now in effect. Staff are currently being trained on the revised policy.

[42] The privacy provisions within *LA FOIP* deal comprehensively with the collection, use and disclosure of personal information. OIPC reviewed the Town's Policy 2.13 and found that the policy only addresses the *collection* of personal information. The policy is silent on the proper "use" and "disclosure" of personal information. In this case, the Town disclosed personal information when it should not have. Therefore, the Town should provide guidance to its employees not only on the collection of personal information but also on the use and disclosure of personal information. The Town's Policy 2.13 is a good start but falls short in that it does not sufficiently address the root cause of this privacy breach. There will be a recommendation that within 60 days of issuance of this Review Report, the Town amend Policy 2.13 to provides additional guidance to employees on the proper use and disclosure of personal information. Upon revision of the policy, training should be offered to Town staff.

III FINDINGS

[43] OIPC has jurisdiction to undertake this investigation.

[44] A privacy breach occurred when the Town disclosed the Complainant's personal information to the tenants when it issued the tax receipt dated January 20, 2025 containing the Complainant's property tax roll number and civic address.

[45] The Town has contained the privacy breach.

[46] The Town sufficiently notified the Complainant of the privacy breach involving the Complainant's personal information.

[47] The Town made sufficient efforts to investigate the breach and identified areas in which it can improve.

[48] The Town has taken steps to establish a procedure that will prevent similar privacy breaches in the future.

[49] The Town's Policy 2.13 does not sufficiently address the root cause of the privacy breaches.

IV RECOMMENDATIONS

[50] I recommend that the Town familiarize itself with the privacy provisions set out in PART IV of *LA FOIP*, including the collection, use and disclosure provisions. This would ensure that, going forward, the Town confirm its authority to disclose personal information before doing so.

[51] I recommend that within 60 days of the issuance of this Review Report that the Town document the current practice into a written policy and/or procedure its process regarding the issuance of receipts when the payee is not the account holder.

[52] I recommend that within 60 days of issuance of this Review Report that the Town amend its Policy 2.13 so that it also provides guidance to employees on when they are authorized

to use and disclose personal information. Once it has revised its policy, the Town should provide training to its employees on the revised policy.

Dated at Regina, in the Province of Saskatchewan, this 18th day of August, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner