Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 212-2019

City of Regina

July 22, 2020

Summary: The City of Regina (City) received a complaint regarding a breach of privacy involving a personal email address. The Commissioner found that a breach occurred, that the City took reasonable steps to contain the breach, provided appropriate notification, conducted an adequate investigation, and had an adequate plan for prevention. The Commissioner recommended that the City update its procedures and implement safeguards to prevent the same type of breach from occurring again in the future.

I BACKGROUND

[1] On June 30, 2019, and July 1, 2019, the Complainant contacted my office with concerns that the City of Regina (the City) had breached their privacy by disclosing their personal email address in a group email. Their personal email address contains the first letter of their first name plus their complete last name. The Complainant added that they were disappointed that the City did not report the breach to my office because, "we [the City] didn't think it was necessary as there were only 27 [26] email addresses affected".

[2] On July 5, 2019, my office notified the City of the complaint. On the same date, my office notified both the City and the Complainant that my office would undertake an investigation into the breach.

II DISCUSSION OF THE ISSUES

1. Does my office have jurisdiction?

[3] I note the email in question was forwarded by a City employee to the recipients concerning a City bylaw review meeting. The City qualifies as a local authority pursuant to subsection 2(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). My office, therefore, has jurisdiction.

2. Is there personal information involved in this matter?

[4] The Complainant takes issue that their email address, which I noted included the first letter of their first name and complete last name, was included in a mass email sent by the City to 26 individuals. The City stated it had inadvertently included the email addresses on the "to" line instead of on the "bcc" line, a practice which keeps email addresses from being visible to any other individual who receives the email. The City sent the email to advise recipients, "that had submitted a request to appear before City Council on [date] respecting the new [bylaw changes]".

[5] Upon review of all email addresses at question provided to me by the Complainant, it appears that at least 20 of them included either a full or partial name, but some of those appear to be business-related emails. In past reports, I have concluded that business-related email addresses are not personal information.

[6] In order for the privacy provisions to be engaged, personal information must be involved. Subsection 23(1) of LA FOIP defines "personal information" as follows:

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

[7] 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.

[8] The email contains the Complainant's first letter of their first name and complete last name and is their personal email address. This is also the case for the other individuals, in this matter, whose personal (non-business-related) email addresses containing either their partial or full name were also disclosed by the City, as well as why the email was being sent.

[9] In Investigation Report 230-2017, 237-2017, 238-2017, 240-2017 regarding Good Spirit School Division, I considered a matter whereby a principal disclosed the list of all approved substitute teachers to another substitute teacher. In that matter, I found that the combination of information, which included data elements of first and last name, email address and notes about some of the teachers, qualified as personal information pursuant to subsection 23(1) of LA FOIP. Similarly, I find that personal information is involved in this matter.

[10] As the City has not disputed that a breach occurred, my next step is to review how the City managed the breach.

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

[11] My office's resource, *Privacy Breach Investigation Questionnaire* (June 23, 2020), suggests local authorities take the following four best-practice steps when responding to a privacy breach:

1. Contain the breach (as soon as possible);
2. Notify affected individuals (as soon as possible);
3. Investigate the breach; and

4. Plan for prevention.

[12] I will use these steps to assess the City's response to the breach.

Contain the breach

[13] When a privacy breach has or may have occurred, a local authority should take immediate steps to confirm and contain the breach. Depending on the nature of the breach, this can include stopping the unauthorized practice, recovering the records, shutting down the breached system, revoking access privileges or correcting security vulnerabilities.

[14] In its investigation report, the City stated, "[t]he Access and Privacy Team recommended attempting an email recall and to send an email notification to all affected parties advising them of the incident, asking them to delete the email sent to them on June 14, 2019, and requesting that the email addresses shared in error not be used or shared".

[15] In the City's submission, it stated that it discovered a breach had occurred when one of the recipients (not the Complainant) emailed to ask why the City shared private email addresses. I note the day that individual sent their email was a Saturday, so the City did not receive the email and take note of the error until the next business day, which was June 17, 2019. It was three days later, then, that the City issued its recall notice and sent a notification email to all recipients.

[16] I am mindful that a recall notice is most effective when sent immediately after the error occurs, and that it is likely that three days later may have been too late for the recall to be effective. Nonetheless, this is an important step to take when managing a privacy breach of this nature. I also note that the City, in its email to the recipients on June 17, 2019, advising of the breach and what had occurred, asked that recipients, "please delete the email containing the email addresses of other individuals, and that you do not utilize or share any of the recipients' email addresses". The City stated to my office that it did not have further contact with email recipients after this contact, and that none of the affected parties contacted the City through its privacy complaint email address. I note that the June

17, 2019 email sent to recipients did not ask them to confirm, via response, that they had followed the instructions. While I find that the City took reasonable steps to contain the breach, I suggest in the future it follows best practice of asking recipients to confirm they followed the instructions of the notification email.

Notify affected individuals

[17] 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 a compelling reason not to, local authorities should always provide notification.

[18] The City appears to have notified affected individuals the same day it became aware of the breach. I note the City's notification contains the following elements: what occurred, how and on what date; number of individuals affected; who individuals could contact at the City with questions or concerns; the ability to contact the City's Access and Privacy Team or my office; and an apology. I find that the City provided appropriate notification.

Investigate the breach

[19] Once the breach has been contained and appropriate notification has occurred, the local authority should conduct an internal investigation. The investigation is generally conducted by the local authority's access and privacy unit because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. It should also consider whether the safeguards that were in place at the time of the incident were adequate. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the local authority should have a solid grasp on what occurred with the beginnings of a plan to prevent the same or similar breaches from occurring in the future.

[20] The City stated, "[w]hile there is no formal policy, procedure or guideline specific to the topic, it is considered common practice to use blind carbon copy when sending group email". The City further stated, "[t]his incident was caused by human error" and, "[t]he level of risk associated with this breach was low, the breach was contained and those affected notified". I find the City conducted an adequate investigation into the breach.

[21] I am mindful that a local authority does not have a legal obligation to proactively report a privacy breach to my office. I wish to add, however, that I commend the City's use of a risk assessment tool, as per its document, "Operational Guideline, Privacy Incident/Complaint" (effective May 1, 2015) in its section titled, "4.3.2 Risk Assessment", to assess level of risk in a privacy breach. I would suggest that local authorities who develop and use this type of tool, also include at what point it would proactively report a privacy breach to my office and then make this type of information available to complainants and the public. A local authority should also always conduct a root cause analysis to determine whether or not adequate safeguards were in place to prevent the breach; in this case, to determine what contributed to the human error. These types of errors are very common, but preventable, with adequate safeguards. For information on additional safeguards, I refer the City to my office's publication, *eCommunication Guidelines* (April 2019).

Plan for prevention

[22] Preventing future breaches means to implement measures to prevent similar breaches from occurring in the future. These could include implementing policies and procedures that help reduce the likelihood from the same or a similar type of breach from occurring in the future.

[23] In its investigation report, the City stated its plan for prevention was to "[e]nsure procedures indicate use of bcc for group and email messaging". It appears, however, that the City has not added this to its procedures, although it stated, "we touch on that caution [using bcc] in privacy training and will be reinforcing the practice in future training". Providing this caution in training is a good step, and while I find that the City's plan for prevention was

adequate, I recommend that the City follow-up on its initial goal of including the use of "bcc" in its written procedures, and implement safeguards, such as ensuring the "bcc" line shows up by default when sending an email, to prevent the same type of breach from occurring again in the future.

IV FINDINGS

[24] I find that personal information was involved and that a breach occurred.

[25] I find that the City took reasonable steps to contain the breach.

[26] I find that the City provided appropriate notification.

[27] I find that the City conducted an adequate investigation.

[28] I find that the City's plan for prevention was adequate.

V RECOMMENDATION

[29] I recommend that the City follow-up on its initial goal of including the use of "bcc" in its written procedures, and implement safeguards, such as ensuring the "bcc" line shows up by default when sending an email, to prevent the same type of breach from occurring again in the future.

Dated at Regina, in the Province of Saskatchewan, this 22nd day of July, 2020.

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