Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 260-2017

University of Regina

May 18, 2018

Summary: My office learned of an alleged breach of privacy involving the University of Regina (U of R) after a news article reported that "the University of Regina is investigating the possibility that one or more students hacked into its computers in order to adjust grades." The Information and Privacy Commissioner (IPC) initiated a privacy breach investigation into this matter and requested the U of R provide its internal investigation report. The IPC found that the U of R had appropriately contained and investigated the breach of privacy incident. The IPC recommended the U of R ensure its policies and procedures promote the use of strong passwords for systems using PIN authentication. It was also recommended the U of R conduct regular random audits of its Dynamic Online Mark Entry (DOME) system. The IPC also recommended that all U of R employees be required to complete mandatory annual access and privacy training. Further, it was recommended the U of R notify all affected individuals of the personal information that was inappropriately accessed.

I BACKGROUND

[1] On October 6, 2017, a CBC News article reported, "the University of Regina is investigating the possibility that one or more students hacked into its computers in order to adjust grades."

[2] On October 26, 2017, my office notified the University of Regina (U of R) that my office would be undertaking an investigation into the alleged breach of privacy. My office requested that the U of R provide details surrounding the alleged breach of privacy, a copy

of its internal investigation report and copies of any relevant policies or procedures related to this matter.

[3] On December 11, 2017, my office received the U of R's internal investigation report regarding this matter. The U of R's internal investigation report provided that on August 26, 2017, a U of R instructor noticed grades for six students had been altered in its grading system, Dynamic Online Mark Entry (DOME) and reported the altered grades to Information Services. DOME showed that the account of a U of R Dean had been used to alter the grades. On September 1, 2017, it was confirmed that the Dean had not accessed DOME or made any grade changes.

II DISCUSSION OF THE ISSUES

1. Does *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) apply in these circumstances?

[4] LA FOIP applies to matters where three elements are present; first element is a local authority, second element is personal information and the third element is if the personal information is in the possession or under the control of the local authority.

[5] The U of R qualifies as a local authority pursuant to subsection 2(f)(xii) of LA FOIP.

[6] Subsection 23(1) of LA FOIP provides the definition of personal information and a list of examples of the type of information that would qualify as personal information. However, this list is not exhaustive.

[7] The information accessible in DOME would have included the first and last name of the students, the class they were enrolled in, their student ID number and the grade assigned in the class. Subsections 23(1)(b), (d) and (k)(i) of LA FOIP identify this type of information as personal information:

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

> …
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> …
>
> (d) any identifying number, symbol or other particular assigned to the individual;
> …
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

[8] As such, I find that personal information is at issue in this matter.

[9] Finally, the personal information was prepared by the U of R and was stored in the U of R's DOME system. As such, I find that the U of R had possession and control of the personal information.

[10] I find that LA FOIP applies in this circumstance.

2. Did the U of R respond appropriately to the privacy breach?

[11] When there is a privacy breach, my office's focus is determining whether the public body has appropriately handled the privacy breach. My office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* (Privacy Breach Guidelines), recommends public bodies take the following five steps when responding to a privacy breach:

- Contain the breach;
- Notification;
- Investigate the breach;
- Prevent future breaches; and
- Write a privacy breach report.

[12] I will consider each of these steps to assess the U of R's response to the privacy breach.

Write a privacy breach report

[13] The U of R provided my office with its internal investigation report detailing what had occurred and steps taken as will be discussed in this Investigation Report.

Contain the breach

[14] My office's Privacy Breach Guidelines provide the following regarding containing the breach:

> It is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:
>
> - Stopping the unauthorized practice.
> - Recovering records.
> - Shutting down the system that was breached.
> - Revoking access to personal information.
> - Correcting weaknesses in physical security.

[15] On August 28, 2017, the Instructor noticed grades entered on August 26, 2017 had been altered. The Instructor contacted Information Services to inquire about the grades being altered, and it was found that the Dean's DOME account had altered the grades. After receiving confirmation from the Dean that they had not accessed their DOME account or made any changes to grades, Information Services began its investigation of DOME activity logs. The U of R's investigation found activity that was deemed abnormal. Due to the grading anomalies and the potential for unauthorized use of the Dean's account, the Dean's PIN for the DOME account was reset on September 1, 2017 and the Dean was required to change the PIN for DOME upon initial log-in.

[16] As the U of R took steps to prevent further unauthorized access to the Dean's DOME account, I find that the U of R took appropriate steps to contain the breach.

Investigate the breach

[17] Once a breach of privacy has been contained, the next step is to investigate the breach. In my office's Privacy Breach Guidelines, it lists some of the key questions to ask during a privacy breach investigation including:

- What occurred?
- How did the breach of privacy occur?
- 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?
- Who are the affected individuals?

[18] After learning of the suspicious activity using the Dean's DOME account, Information Services and the Registrar's Office conducted data analysis and investigated DOME for other suspicious activities. This included:

1. Approvals using the Dean's DOME account
2. Courses in the spring/summer 2017 and previous terms in which the Students of Interest were enrolled
3. Approvals by other deans that to be abnormal activity
4. Approvals by other users that had abnormal activity
5. Approvals in short sequence that appeared to be abnormal activity

[19] Based on its data analysis and investigation, the U of R found that five instructor/dean DOME accounts had been inappropriately accessed resulting in 31 students in four spring/summer 2017 courses impacted by grade changes. The investigation also revealed that it appeared a faculty member's webmail account also may have been inappropriately accessed. The U of R indicated that while the authentication is not the same as DOME, the access looked suspicious due to the time/location where the access had taken place. The time/location of this access appeared to be the same time/location as the inappropriate accesses into DOME. As a security precaution, the U of R forced a change to the credentials for this account on October 6, 2017.

[20] In its internal investigation report, the U of R reported that they believed "the breach resulted from the utilization of weak passwords, and failure of impacted faculty members to change password from the default."

[21] Based on the details provided by the U of R regarding the breach of privacy, I find that the U of R appropriately investigated this breach of privacy incident.

Prevent future breaches

[22] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

[23] In its internal investigation report, the U of R outlined that many employee-facing application, including DOME, had been placed behind the campus firewall, and now required the use of a Virtual Private Network (VPN) for access from off-campus locations. As well, the U of R made changes to its PIN authentication practices to prevent future unauthorized accesses. Finally, the U of R advised that it plans to eliminate the use of PIN authentication in the summer of 2018.

[24] In correspondence with my office, the U of R advised that it continues to follow its past practice to set the initial PIN, but the PIN must be changed on first log-in and cannot be reused by the user. Setting up an initial PIN using this type of information could be interpreted by the user as the type of information that would create a strong password for future use. The U of R should ensure it is demonstrating the use of strong passwords in its initial PIN.

[25] The U of R does have Password Guidelines, however in the Password Policy FAQs found on its website, it states that PINS are exempt from these guidelines as PINS do not have the ability to meet the standards outlined. The U of R's Password Guidelines provide as follows:

A strong password has the following characteristics:

- Is at least 8 characters in length…
- Is different from previously used passwords
- Contains a combination of characters…

…

Password guidelines

…

- Do not use a password containing a word found in dictionary.
- Do not use any part of your first, middle or last name to form a password. Do not use maiden names, initials or nicknames.
- Do not use information that can be obtained about you. This may include pet names, names of friends or relatives, phone numbers, name of the street you reside on.

…

- Do not use a password consisting entirely of numbers of letters…

…

- Do not use dates, in any format, for passwords.

[26] In my office's resource *Helpful Tips: Mobile Device Security – Privacy tips for Public Bodies/Trustees* using mobile devices it states:

> The use of passwords is a basic security measure that should be taken. Strong passwords are comprised of at least eight characters, with 14 or more being the ideal. They can include a combination of upper and lower case letters, numbers and symbols, rather than dictionary words. Avoid using predictable passwords like birthdates, favorite sports teams or easy-to-guess dictionary words like "password" or "Letmein"…

[27] Further, the International Organization for Standardization (ISO) and the International Electronic Commission (IEC) *ISO/IEC* 27002 *Information Technology Security Techniques: Code of practice for information security controls, Second edition* (ISO Standards) provides:

> **9.3.1 Use of secret authentication information**
>
> …
>
> All users should be advised to:
>
> …

> d) when passwords are used as secret authentication information, select quality passwords with sufficient minimum length which are:
>
> 1) easy to remember;
> 2) not based on anything somebody could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth, etc.;
> 3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
> 4) free of consecutive identical, all numeric or all-alphabetic characters;
> 5) if temporary changed at the first log on;
>
> …
>
> **9.4.2 Secure log-on procedures**
> …
>
> The procedure for logging into a system or application should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance…

[28] The U of R should ensure its practices for PINs, whether the initial PIN, reset PIN or policies and procedures related to PIN authentication promote the use of strong PINs for authentication.

[29] I recommend the U of R ensure it has appropriate policies or procedures in place to ensure staff and students are using strong passwords for their PIN authentication to prevent unauthorized access.

[30] I recommend that the U of R increase the minimum number of characters for PINs.

[31] I recommend the U of R ensure authentication requirements being considered in the summer of 2018 to replace PIN authentication meet the requirements found in the ISO Standards.

[32] My office also inquired if the U of R conducted regular audits of DOME. The U of R responded advising regular audits are not currently conducted.

[33] Auditing is a technical safeguard and is necessary to assess compliance with and measure effectiveness of policies and procedures, assess compliance with legislation, assess if appropriate measures are in place to control access and monitor access.

[34] I recommend the U or R conduct regular random audits on DOME to screen for abnormal activity or unauthorized access. It is also recommended that the U of R consider auditing capabilities when updating its DOME system.

[35] My office also asked the U of R to speak to access and privacy training for employees. The U of R responded indicating that an online Information Security Awareness training program is available to all U of R employees and students. It is mandatory for some departments, such as Financial Services and Information Services to attend, but optional for all other employees. At the time of my investigation, the U of R had reported that 488 employees were enrolled in the program and 339 had successfully completed the training. The U of R also indicated that it offers half-day workshops on access and privacy on an annual basis to interested employees and average 50 attendees per session.

[36] I recommend the U of R implement mandatory annual privacy training for all employees.

Notification

[37] My office's Privacy Breach Guidelines provides the following guidance to public bodies regarding notification of a breach of privacy:

> The following is a list of individuals or organizations that may need to be notified in the event of a privacy breach:
>
> - Contact your organization's privacy officer immediately.
> - Proactively report the breach to the IPC.
> - If criminal activity is suspected (e.g. burglary), contact police.
> - Contact the affected individuals unless there are compelling reasons why this should not occur.

[38] The U of R advised in its internal investigation report that it had notified all student, faculty and staff in the Faculty of Engineering and Applied Science of *grade irregularities* in

emails dated October 6, 2017. The emails advised that the U of R was investigating the grade irregularities in four Faculty of Engineering classes during the spring/summer term. It advised that affected students would be contacted directly. The email also requested that all student, faculty and staff of the Engineering department follow its best practices for information security and provided a link to its policy. It also suggested students, faculty and staff regularly change their passwords and ensure passwords are sufficiently strong.

[39] On November 3, 2017, the U of R sent emails to the affected students advising that they had been assigned incorrect grades in some courses and advising that the recorded grade had been adjusted to correctly reflect the grades calculated by the professor. The correspondence advised the students of the corrected grade for the affected courses and advised that it did not expect any additional grading adjustments. The email also apologized for the inconvenience and advised it had taken steps to ensure the irregularities were addressed. Finally, the email advised that if students had any questions regarding the change in their grade to contact the Registrar's Office.

[40] The Privacy Breach Guidelines provides that notifications to affected individuals should include:

- 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.)
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number, etc.).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individual have a right to complain to the IPC. Provide contact information.
- Recognition of the impacts of the breach on affected individuals and an apology.

[41] While the U of R advised individuals affected by altered grades, it does not appear it notified these individuals that their personal information had been inappropriately accessed, or addressed any other elements outlined above. Further, while the U of R identified those with grade changes as the affected individuals, the individual that

inappropriately accessed DOME would have had the ability to access personal information of any students that the DOME users had access to.

[42] As of January 1, 2018, amendments of LA FOIP provides the following regarding notification:

> **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.

[43] Thus, now the obligation of local authorities to notify affected individual is clear.

[44] I recommend the U of R take steps to determine which students' personal information the individual had access to and ensure all affected individuals are provided with notification confirming all elements outlined at paragraph [40] are included.

III FINDINGS

[45] I find that LA FOIP applies.

[46] I find that the U of R took appropriate steps to contain this privacy breach.

[47] I find that the U of R adequately investigated this privacy breach.

IV RECOMMENDATIONS

[48] I recommend the U of R ensure it has appropriate policies or procedures in place to ensure staff and students are using strong passwords for their PIN authentication to prevent unauthorized access.

[49] I recommend that the U of R increase the minimum number of characters for PINs.

[50] I recommend the U of R ensure administrative software package being considered in the summer of 2018 ensure the authentication requirements meet the requirements found in the ISO Standards.

[51] I recommend the U or R conduct regular random audits on DOME to screen for abnormal activity or access. It is also recommended that the U of R consider auditing capabilities when updating its DOME system.

[52] I recommend that the U of R implement mandatory annual access and privacy training for all employees.

[53] I recommend the U of R take steps to determine which students' personal information the individual had access to and ensure all affected individuals are provided with notification confirming all elements outlined at paragraph [40] are included.

Dated at Regina, in the Province of Saskatchewan, this 18th day of May, 2018.

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