Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 060-2016

Cumberland College

June 10, 2016

Summary: Cumberland College's website was breached through a brute force attack. This may have resulted in the unauthorized disclosure of the personal information of 2800 individuals. The Commissioner found that Cumberland College has taken reasonable steps in responding to the breach. He recommends that Cumberland College perform privacy impact assessments when looking at new ways to collect personal information.

I BACKGROUND

[1] On Monday, March 28, 2016, Cumberland College's website was breached through a brute force attack. Noticeable signs of the attack included changes to images on its website replaced with the text "You Have Been Hacked" and entries in the server's log. Also at risk, as a result of this attack, was the database that contains personal information of students that was collected through the website.

[2] On April 8, 2016, Cumberland College proactively reported the potential breach to my office. On April 12, 2016, a formal investigation file was opened and we asked Cumberland College to provide us with an internal investigation report.

II DISCUSSION OF THE ISSUES

[3] Cumberland College qualifies as a local authority pursuant to subsection 2(f)(ix) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) as it is a regional college within the meaning of *The Regional Colleges Act*.

1. Was personal information involved?

[4] Cumberland College has indicated that there is database connected to its website which contained information about 2800 students or former students. This information is collected from the students through the website when they enroll for continuing education classes or apply for scholarships. The type of information in the database includes names, addresses, telephone numbers, e-mail addresses, birth dates, gender, whether an individual has a disability, social insurance numbers (SIN), credit card information, emergency contact information, education history, marital status, citizenship status and ancestry information.

[5] Section 23 of LA FOIP defines personal information. All of the data that Cumberland College has indicated is in the database would qualify as personal information pursuant to section 23 of LA FOIP. Cumberland College recognizes that some of the personal information is sensitive, especially the SINs and credit card information.

[6] Subsection 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.

[7] Cumberland College has indicated that it cannot be sure at this point in time if the hackers accessed or copied the personal information in the database. If so, this would qualify as an unauthorized disclosure of personal information. Cumberland College has told my office that it is operating on the basis that there has been a disclosure of personal information.

2. Has Cumberland College taken appropriate steps to respond to this privacy breach?

[8] My office's resource *Privacy Breach Guidelines* recommends the following five steps to take when responding to a privacy breach:

1. Contain the breach - ensure that personal information is no longer at risk;
2. Notification – Notify various individuals who may have an interest in knowing the breach occurred such as affected individuals, my office and the police.
3. Investigate the Breach – find out what occurred, how did it occurred, what laws apply, etc.;
4. Prevent future breaches – implement strategies and safeguards that will prevent similar breaches in the future; and
5. Complete a privacy breach report.

[9] The following is a summary of the steps that Cumberland College has taken in response to this report.

Contain the Breach

[10] Cumberland College indicated that the hackers had access to its server for approximately two minutes. Some of the initial steps that it took to contain the breach included migration efforts, implementation of additional security features and continuous monitoring of server log files.

Notification

[11] March 28, 2016 was a holiday Monday, Cumberland College management was not notified until March 29, 2016.

[12] Cumberland College contacted my office on April 8, 2016 to proactively report the breach to my office.

[13] In its investigation report, Cumberland College reported that approximately 2800 students or former students were affected. All were notified of the breach by e-mail. Efforts were made to contact the 112 individuals with credit card information in the database by telephone.

Prevent future breaches

[14] At the Ministry of Advanced Education's request, Cumberland College hired an external IT Security firm to review the incident. Cumberland College shared this with my office. The report from the IT firm made several suggestions to Cumberland College to improve the security of our website. Cumberland College has indicated it has implemented all of these suggestions.

[15] Cumberland College has also advised that it is no longer collecting SINs or credit card information directly over its website. For credit card information, it plans to engage an Internet payment company such as PayPal to facilitate the transactions. Credit card information will no longer be held in Cumberland College's database. I encourage other small public bodies to consider this solution as a means to collect payment over the Internet. Cumberland College has not indicated if it has performed privacy impact assessments for this plan.

[16] Cumberland College will also be exploring other ways to collect SINs for the purpose of issuing tax forms.

III FINDING

[17] I find that Cumberland College has taken adequate steps to respond to this breach.

IV RECOMMENDATION

[18] I recommend that Cumberland College perform privacy impact assessments when it explores new methods of collecting personal information and share them with my office.

Dated at Regina, in the Province of Saskatchewan, this 10th day of June, 2016.

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