

NOTICE OF DATA BREACH

Dear Trillium College Community Member:

We hold our relationship with you in the highest regard and we respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

Sometime, between Thursday September 24th at 7:00 pm and Friday September 25th at 10:00 am, Trillium College experienced a “cyber attack”, in which certain unknown actors illegally accessed our data systems.

WHAT INFORMATION WAS INVOLVED?

The data accessed may have included personal information such as names, addresses, phone numbers and passwords. To our knowledge, the data accessed did not include any type of financial information.

WHAT WE ARE DOING

Trillium College values your privacy and deeply regrets that this incident occurred. As soon as it was discovered, all affected systems were shut down and taken offline. Our systems continued to be offline, to facilitate an investigation. Trillium College is conducting a thorough review of the potentially affected records and computer servers and will notify you if there are any significant developments. As we bring services back online, we will implement additional security measures designed to prevent a recurrence of such an attack and to continue to protect the privacy of the Trillium College Community.

As part of this process, Trillium College has engaged a third-party cyber security consultant, with a team of professional forensic data and systems specialists, to investigate how this breach happened, who is responsible and evaluate our security systems to ensure the incident is properly addressed and shared with the appropriate authorities and law enforcement.

WHAT YOU CAN DO

While we conduct our review, we suggest that you also review the information included in this communication for further information on steps you can take to protect your information, including but not limited to those steps set out at the end of this letter.

FOR MORE INFORMATION

For further information and assistance, please contact the College at privacy@trilliumcollege.ca.

Sincerely,



Andrew Jones
President

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify your financial institution and credit card company. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your local police force and the Canadian Anti-Fraud Centre (CAFC).

To report an incident to the CAFC, go to <http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm> or call 1-888-495-8501. The CAFC is Canada's central repository for data, intelligence, and resource material as it relates to fraud and it is a collaboration of the RCMP, Competition Bureau, and the Ontario Provincial Police.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the two major credit reporting agencies. You can access a free copy of your credit report at any time. Contact information for the two national credit reporting agencies to request a copy of your credit report or for general inquiries is set out below:

Equifax Canada

1 (800) 465-7166

<https://www.consumer.equifax.ca/personal/>

<http://assets.equifax.com/assets/canada/english/creditReportRequestForm.pdf>

National Consumer Relations

P.O. Box 190 Station Jean-Talon

Montreal, Quebec H1S 2Z2

TransUnion Canada

1 (877) 525-3823

<https://www.transunion.ca>

Attention: Consumer Relations

P.O. Box 338, LCD1

Hamilton, Ontario L8L 7W2

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. This alert will remain on file for six years. To place a fraud alert on your credit report, contact the two national credit reporting agencies identified above. Additional information is provided by the RCMP and available at <http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm>.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the RCMP on how to avoid identity theft and steps to take if you are a victim of identity theft. For more information, please visit

<http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm> and <http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm>.