Attention: All Current Okanagan College Students
NOTICE OF PRIVACY INCIDENT
January 23, 2023

Re: **Notice of Privacy Incident**

Okanagan College would like to notify all current students, including full-time, part-time, and continuing education students currently enrolled online or at any one of our campuses, of an incident that may affect the security of their personal information.

WHAT HAPPENED?

On Monday, January 9, Okanagan College responded to an incident in which an unauthorized entity gained access to certain Okanagan College technology systems. As soon as the intrusion was detected, we shut down key systems to limit the potential impacts and we engaged cyber-security experts to assist with the response.

In the course of our ongoing investigation, we have determined that personal information belonging to current students may have been subject to risk as a result of the incident, including the following types of information:

- Personally Identifiable Information (PII), such as your name, date of birth, email address, mailing address and social insurance number (SIN).
- Student information, such as information contained on your transcript or enrollment application.
- If you are an International Student, the incident may have also resulted in the exposure of your passport number and/or visa.

In the wrong hands, this type of information can be used for fraud, identity theft and other harmful purposes. Although we have no evidence that any such activity has occurred, we want you to be aware of the situation, including the steps we are taking to address this issue, and the precautions that we recommend you take to protect your personal information.

Please note that Okanagan College uses a third-party payment processor for all credit and debit card transactions, whether made online or on campus. We have no evidence to suggest that such payment card information is at risk as is it not collected or stored directly by Okanagan College.

STEPS WE ARE TAKING TO PROTECT YOU

As a precautionary measure, we are offering all current students a free two-year subscription to *my*TrueIdentity, a premium credit monitoring and identity theft prevention service. The service is provided by TransUnion, one of Canada's main credit reporting agencies, and includes:

- Unlimited online access to the TransUnion Credit report, updated daily. A credit report is a snapshot of a consumer's financial history and the primary tool leveraged for determining credit-related identity theft or fraud.
- Unlimited online access to the TransUnion CreditVision® Risk score, with score factors and analysis updated daily. A credit score is a three-digit number calculated based on the information contained in a consumer's credit report at a particular point in time.

- TransUnion credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit monitoring alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Unlimited access to online educational resources concerning credit management, fraud victim assistance and identity theft prevention.
- Identity theft insurance of up to $50,000 in coverage to protect against potential damages related to identity theft and fraud.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect. consumers against identity theft.

How to activate *my*TrueIdentity

To access *my*TrueIdentity, you must be a Canadian Resident, the legal age of majority (18+ years), and you must have a Canadian Social Insurance Number. If you do not meet these requirements, please refer to the Q&A below.

- **Obtain your unique Activation Code** by contacting TransUnion at **1-833-806-1882.** Call centre hours are **Monday – Friday, 6:00 am to 3:30 pm PST, excluding statutory holidays.** You will be asked questions to confirm that you are an active student, including your name and student number (300-number).
- **Activate your account** with your unique activation code by **May 31, 2023,** by visiting https://www.mytrueidentity.ca/
- When activating your account, you will also need to provide TransUnion with your name, address, email address, date of birth, and SIN (optional), as well as answer certain authentication questions so that TransUnion can verify your identity and correctly link to your credit file.

Should you require assistance activating your account, you can contact TransUnion directly using the contact information provided on the https://www.mytrueidentity.ca/

OTHER STEPS YOU CAN TAKE

As a matter of best practice, we recommend that you remain vigilant, as always, to the possibility of fraud and identity theft by reviewing your financial statements and accounts regularly for any unauthorized activity. You should notify your local law enforcement of any suspicious activity.

You should also practice good cyber-hygiene. Use appropriately complex passwords (i.e., a password that is between 8-256 characters using a combination of uppercase and lowercase letters, numbers and symbols, and that is not based on information (e.g. birth date, street address, nickname, pet's name, etc.) that someone could easily associate with you. Never recycle passwords or repeat the same password (or a simple variation of the same password) across multiple accounts. Always be suspicious of emails, text messages, or phone calls you may receive asking you for personal information or that contain links or attachments, even if they appear to come from someone you know and trust.

- To educate yourself about identity theft and related scams and frauds, we encourage you to visit the Government of Canada's Anti-Fraud Centre website: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
- If you suspect someone is using your SIN: https://www.canada.ca/en/employment-social-development/programs/sin/protect.html#a6
- If you have been the victim of fraud: https://www.canada.ca/en/employment-social-development/programs/sin/protect.html#a7

THANK YOU FOR YOUR CONTINUED SUPPORT

We are incredibly grateful for your resilience, and we regret any concern or inconvenience the incident may have caused.

While no organization is immune to these types of attacks, we continue to seek opportunities to further strengthen our security infrastructure, and we will always prioritize your privacy and the protection of your information.

Should you have any questions or concerns, please do not hesitate to contact cyberincident@okanagan.bc.ca. We will get back to you as soon as possible.

Sincerely,

Neil Fassina
President, Okanagan College

Note: This notice does not pertain to former or prospective students, nor employees or any other individual who has association with the College. Should the investigation determine that information pertaining to other individuals may have been impacted by the incident, Okanagan College will notify those individuals accordingly.

QUESTIONS & ANSWERS FOR STUDENTS

1. **What Happened? How did this happen?**
   On Monday, January 9, Okanagan College responded to an incident in which an unauthorized entity gained access to certain Okanagan College technology systems. The College responded by immediately shutting down and disabling network access across all of our campuses. We have engaged external cyber-security experts to assist in our response and investigation.

2. **How did the College respond?**
   Upon discovery of the incident, we took immediate steps to secure our IT systems and out of an abundance of caution, issued a public statement to our students and staff. We immediately launched an investigation with a leading third-party forensic services firm.

   We have notified the RCMP, the Office of the Information and Privacy Commissioner for British Columbia, and the Canadian Centre for Cyber-Security, whose collective recommendations we have followed throughout this process.

3. **How did you determine student information may have been affected?**
   We have been conducting a comprehensive forensic investigation with the assistance of cyber-security experts. Through those efforts, we recently uncovered evidence that suggests that certain information, including information belonging to current students, was subject to risk.

4. **What are you doing to protect students?**
   As a precautionary measure, we are offering all current students a free two-year subscription to *my*TrueIdentity, a premium credit monitoring and identity theft prevention service. Students can obtain an activation code by calling TransUnion at **1-833-806-1882.**

5. **Are Okanagan College staff or students at increased risk of identity theft?**
   In the wrong hands, the type of student information that was subject to risk can be used for fraud, identity theft and other harmful purposes. Although we have no evidence that any such activity has occurred, we encourage you to take steps to protect yourself, such as:
   - Activating the credit monitoring service provided by the College;
   - notifying your credit card company or financial institutions of this incident;
   - monitoring your account statements for unusual activity or discrepancies and reporting them to your credit card company or financial institutions;

- obtaining a credit report to identify any unusual credit activity (such as evidence of accounts you did not open or inquiries from creditors you did not authorize to access your information) and notifying the credit agency immediately of any such activity; and
- being alert to other unusual inquiries or communications that you may receive.

If you identify any information on an account statement or credit report that you do not understand, it is important that you contact the credit agency or your financial institution immediately.

6. **Why weren't you able to prevent this incident?**
   We are working with experts to understand how the incident occurred. Unfortunately, no organization can be entirely immune to these types of incidents.

7. **Why are you only notifying students?**
   We have evidence that employee information was also subject to risk. As such, we have also notified employees and provided them with access to credit monitoring services.

8. **I am a former student/employee/other. What about me?**
   Our investigation is ongoing. Should the investigation determine that information pertaining to other individuals may have been impacted by the incident, Okanagan College will notify those individuals accordingly.

9. **Why did it take so long to notify?**
   We do not take information security and protection of information lightly, and we immediately engaged cyber-security experts to assist us with the response and investigation. As soon as it became clear that student information may have been exposed to risk, we took steps to notify you as quickly as possible.

10. **What information belonging to me was affected?**
    At this stage, it is not possible to know exactly what information belonging to you may have been involved, if any. As it became clear that student data was subject to risk, we made the decision to notify all students proactively rather than wait for the results of a potentially lengthy investigation.

11. **What is credit monitoring?**
    Credit monitoring services monitor your credit file and alert you to key changes and potentially suspicious activity such as a new account opened in your name. It also includes insurance and professional support to help victims recover from identity theft.

    You will need to provide your student number (300-number) when you call TransUnion to obtain your activation code, and potentially answer additional questions to verify your identity.

12. **I am under the age of 18. Why can't I access the credit monitoring service?**
    In Canada, there is no credit monitoring product that is offered to minors, as you must be the age of majority to obtain credit (18+). If you are under the age of 18 and have a Social Insurance Number, you can contact TransUnion at 1-888-228-4939 and they may be able to put an alert on your social insurance number. Since minors do not have credit files, TransUnion may require you to take additional steps to process the request.

13. **Why aren't you providing credit monitoring to international students?**
    Canadian services providers are only able to monitor Canadian credit files. If you are an international student and would like to determine what other protection may be available to you, please email cyberincident@okanagan.bc.ca

14. **What can students do to protect their passport from misuse?**
    If you provided your passport to us, for whatever reason, we would encourage you to visit Passport Canada's website for information on how to protect yourself from passport fraud. If your passport was issued by another country, we recommend you contact the foreign government agency that issued your passport for more information and advice.

15. **Why are you only providing monitoring through TransUnion, and not Equifax, or both?**
    There are two main credit reporting agencies and they both have access to similar information and provide similar services. It would be redundant to use both services.

16. **What should I do if I think any of my accounts has been compromised?**
    If you have reason to believe that you have been a victim of fraud, for any reason, we urge you to contact your local police, and to notify any financial institutions you have a relationship with. You can also contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or online at https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

17. **Should Okanagan College students or staff take extra precautions to monitor their financial and credit information?**
    We strongly encourage you to take advantage of the free two-year subscription to *my*TrueIdentity that we are providing to all students.

    To access *my*TrueIdentity, you must be a Canadian Resident, the legal age of majority (18+ years), and you must have a Canadian Social Insurance Number. If you do not meet these requirements, please refer to the Q&A below.

    1. **Obtain your unique Activation Code** by contacting TransUnion at **1-833-806-1882.** Call centre hours are **Monday – Friday, 6:00 am to 3:30 pm PST, excluding statutory holidays.** You will be asked questions to confirm that you are an active student and you will need to provide your student number (300-number).
    2. **Activate your account** with your unique activation code by **May 31, 2023,** by visiting https://www.mytrueidentity.ca/

18. **What should I do if I think I am the victim of fraud or identity theft?**
    If you have reason to believe that you have been a victim of fraud, for any reason, we urge you to contact your local police, and to notify any financial institutions you have a relationship with. You can also contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or online at https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

    1. If you suspect someone is using your SIN: https://www.canada.ca/en/employment-social-development/programs/sin/protect.html#a6
    2. If you think you have been the victim of fraud: https://www.canada.ca/en/employment-social-development/programs/sin/protect.html#a7

19. **What is identity theft?**
    Further information about identity theft is available at: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/

20. **How many community members have been impacted?**
    Our investigation is ongoing. It would be too early to know, and we would only be speculating.

21. **How do I get in contact with a privacy commissioner to learn about my rights?**
    Please note, we have notified the Office of the Privacy Commissioner for British Columbia of this incident and they are investigating the matter. If you would like to receive information from or file a complaint with the Office of the Privacy Commissioner for British Columbia, please contact info@oipc.bc.ca.