Protecting yourself from potential risk of fraud

Due to the recent cyberattack on TransLink, it is possible personal information may have been compromised.The information and resources provided here are intended to help detect and prevent potential fraud. These are precautionary measures that may help inform good cyber and financial health practices.

What immediate actions can I take to protect myself?

Sign up for free credit monitoring and fraud protection services:

- TransLink is providing employees of TransLink and its subsidiaries, as well as directly affected individuals who receive notification letters, with two years of credit monitoring services through TransUnion.
- Credit monitoring is a tool that notifies you of suspicious activity that affects your credit report, including inquiries from lenders or new account activations. This can help you see if someone is attempting to apply for credit under your name. Early detection is key.
- If the reports you receive from TransUnion indicate that you may be the victim of identity theft, please visit ***www.antifraudcentre.ca*** for information on what to do next.
- The credit monitoring service package also includes identity theft insurance up to $50,000 in coverage to protect against potential damages in the event you are a victim of fraud.

Sign up for a Fraud Alert for any new activity on your TransUnion credit file:

- A Fraud Alert encourages a lender or creditor to take reasonable steps to confirm your identity with you before processing an application for a loan.
- This process makes it more difficult for criminals to secure loans or credit cards in your name.
- If you receive notice that your personal information has been compromised but there has been no reported misuse thus far, you can put a Potential Fraud Alert on your credit file with TransUnion. This service is included in the TransUnion package offered to employees.
- To sign up for a Fraud Alert with TransUnion, click ***here***.

Continue to monitor your credit score and credit report:

- Check your credit score frequently to detect any sudden and unwarranted changes.
- By registering for credit monitoring, you can set up alerts to immediately flag indicators of potential fraud.
- Review your credit report from TransUnion for any suspicious or fraudulent activity. If you find any information that does not pertain to you, contact the creditor and question the account and/or inquiry.

Reconcile your credit card and banking statements regularly:

- Always review your credit card, loan, and other financial statements promptly upon receipt and immediately report discrepancies to your provider.

Create stronger, unique passwords for all your accounts:

- Enable multi-factor authentication wherever possible.
- Passwords should be unique and hard to guess, using a mix of upper and lowercase letters, numbers, and special characters.
- Create different passwords for each secure account (credit card, banking, mobile phone, internet, hydro, etc.).
- Change passwords often, and **DO NOT** recycle them.

How would I know if I am the victim of fraud?

Warning signs vary but typical indicators may include:

- Sudden and unwarranted changes to your credit score.
- A notification from TransUnion indicating a change to your credit score, provided you have signed up for credit monitoring services.
- Suspicious activity showing up in your credit report, such as accounts or inquiries from companies you do not recognize.
- Unrecognized charges on your statements.
- Bills received for items you did not purchase or apply for.
- Credit card or other financial statements that you typically receive by mail stop showing up.
- Collections agencies try to collect on defaulted accounts not opened by you.
- Credit card providers or financial institutions advise you that they have approved or declined an application that you never submitted.

What should I do if I suspect I am the victim of fraud?

- Gather all the information: documents, receipts, messages, etc.
- Contact the financial institution that transferred the money.
- Place flags on all your accounts.
- Change your passwords.
- Report the fraud to both credit bureaus: Equifax and TransUnion.
- Escalate the incident as necessary, including reporting the incident to police.
- You can find more information on next steps at ***www.antifraudcentre.ca.***

You are strongly encouraged to subscribe to TransUnion's credit monitoring service. For questions or more information, please contact ***cyberincident@translink.ca.***