Employee FAQs – Cyberattack Update and Privacy Notifications

February 9, 2021

Contents

General

1. What information was stolen?

TransLink is conducting a comprehensive forensic investigation to determine what sensitive information was unlawfully accessed, including personal information. The investigation will be thorough and will take several months to complete.

To date, the investigation has confirmed that attackers accessed a restricted network drive and copied files containing some personal information related to payroll and benefit administration for current employees of TransLink and its subsidiaries, some former and retired employees, and a limited number of spouses of retired employees. These restricted network drives held files that contained banking information and social insurance numbers.

TransLink will begin mailing personalized notification letters to individuals whose sensitive personal information was compromised starting in mid-February. We will also be offering those individuals complimentary two-year credit monitoring and fraud protection services with TransUnion.

Notification letters

2. I haven't received a notification letter yet, when can I expect to?

TransLink will begin mailing personalized notification letters to individuals whose sensitive personal information was compromised starting in mid-February.

We are continuing with the investigation to determine what files may have been unlawfully accessed, including personal information. As the investigation is ongoing, it could reveal that additional personal information was compromised. Should this happen, we will continue to issue notification letters to affected individuals until the investigation is concluded. TransLink is following all the appropriate steps and guidelines set out by the Office of the Information and Privacy Commissioner for BC in these circumstances.

3. Why are employees being notified by mail? Can't you just email me?

We have more personal mailing addresses than personal email addresses for employees. In addition, if we send a letter to an incorrect mailing address, it will hopefully be returned to sender and TransLink will eventually find out that the intended recipient did not receive it. If we send the letter via email and the employee has changed their personal email address, TransLink has no way to know whether the email reached its intended recipient.

4. I recently moved and am not sure whether TransLink has my current mailing address. How can I check and update it?

Please review your pay stub. If your address is incorrect or you have moved in the last 18 months or so and you are unable to access your pay stub to verify, please email employee.benefits@translink.ca with your current mailing address.

5. Will I still be notified if I leave the organization?
Yes. If someone leaves the organization, they will receive a notification letter at the address we have on record for them. If you subsequently move, please update your mailing address with TransLink.

Compromised employee information

6. How do I know if my information has been compromised?

TransLink will begin mailing personalized notification letters to individuals whose sensitive personal information was compromised starting in mid-February.

As the investigation is ongoing, if we find any new evidence that would suggest employee personal information was compromised, you will be notified by mail.

7. Why is the investigation taking so long?

Through the forensic investigation, TransLink is seeking to understand exactly how the incident occurred and identify opportunities to further strengthen its defenses. The forensic investigation process is rigorous and comprehensive and must be handled with care. A team of internal and third-party forensic investigators are working as quickly as possible.

In addition, TransLink is carefully reviewing the files that were compromised, which is a detailed and time-intensive task that will take several months to complete.

8. My credit card has recently been compromised – is it because of this breach?

TransLink does not hold the personal credit card information of employees.

9. Should I cancel my credit cards or change my banking information?

TransLink does not hold personal credit card information of employees or bank account PINs for employees.

If TransLink, CMBC, BRCTC, WCE, or Transit Police employees change the bank account into which their payroll or benefits are deposited, please be aware that Human Resources will not be able to process payment. If you are concerned about your bank account, you can:

1. Contact your financial institution to have a flag placed on your account, and
2. Consider whether you want to arrange with your financial institution to have your payroll or benefits transferred into a different account as funds arrive into the existing account.

10. How long do I need to be worried about this for? Will this all be okay in two years when the credit-monitoring runs out?

Regrettably, these types of breaches are happening more often across all industry and business sectors. Even if you haven't received a notification letter, it is a good idea to be vigilant and regularly monitor your accounts, statements, and credit score.

11. Are former employees or retired employees also impacted by the privacy breach?

The investigation has determined that the sensitive personal information of current employees, former employees, retired employees, and a limited number of spouses of retired employees of TransLink and its subsidiaries was unlawfully accessed.

As the investigation is ongoing, should TransLink identify additional former employees or retired employees whose sensitive personal information has been compromised, it will send out additional notification letters to those affected individuals.

12. Are spouses or dependants also impacted by the privacy breach?

The investigation has determined that the personal information of a limited number of spouses of retired employees was compromised.

If TransLink identifies additional spouses of retired employees whose sensitive personal information has been compromised, it will send out additional notification letters to those affected individuals.

13. Why is TransLink offering credit monitoring and fraud protection services?

To help mitigate any potential misuse of the sensitive personal information of affected individuals, TransLink is offering credit monitoring and fraud protection services to those individuals.

14. Why is TransLink offering two years of credit monitoring and fraud protection services and not more?

Most companies offer one year of credit monitoring when there has been a privacy breach. TransLink has offered two years of credit monitoring for its employees.

15. Can we sign up for more than two years of credit monitoring and fraud protection services?

At this time, we are offering a two-year subscription to credit monitoring and fraud protection services for all current employees and impacted former, retired and spouses of retired employees. Should you wish to subscribe for additional credit monitoring and fraud protection services, it is recommended that you wait until the two-year period is over before signing up for additional services. Any additional services will be at your own expense.

16. What specifically is being offered in the credit monitoring service package?

- We are offering a two-year membership in credit monitoring and fraud prevention services to our employees and impacted former employees. Upon completion of the enrollment process, you will have access to the following features:
- Unlimited online access to the TransUnion Credit report, updated daily.
- Unlimited online access to the TransUnion CreditVision® Risk score, with score factors and analysis updated daily.
- TransUnion credit monitoring alerts with email notifications to key changes on a consumer's credit file.
- 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.

17. If I sign up credit for monitoring and fraud protection services, will this stop fraudulent activity from happening to me?

Credit monitoring and fraud protection services do not stop identity theft or fraud from happening. It is used as a detection system to warn you of any suspicious activity that may impact your credit score. If you are alerted to credit activity that you did not authorize, contact the creditor immediately.

18. What should I do if my credit is compromised or there is fraudulent activity? Will I be responsible for the charges? / What do I do if I believe I am a victim of identity theft? / What do I do if I believe my information is compromised?

If you ever believe you have been the victim of identity theft or have reason to believe your information is being misused, we urge you to immediately contact the police and file a police report. You can also contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or visit http://www.antifraudcentre.ca/. Make note of the police file number you are given in connection with the police report. If you see a fraudulent charge on your payment card, you should immediately contact the bank, credit union or other financial institution that issued your card. The phone number to call can be found on the back of the card. The bank, credit union or other financial institution might ask you if you have a police file number available, and you should provide it if you have it.

19. I have not been notified that my information was compromised. Why should I bother signing up for credit monitoring and fraud protection services?

Credit monitoring and fraud protection services can alert you to suspicious activity on your credit file in time to stop it from happening. The package also includes identity theft insurance up to $50,000 to protect against potential damages in the event you are a victim of fraud. It is important to note that if your personal information was stolen, there is no certainty criminals will misuse your information, but there is a risk. A TransUnion two-year credit monitoring and fraud protection service subscription is offered to you free of charge. You are encouraged to sign up.

20. Does this mean I am the victim of identity theft?

TransLink is offering credit monitoring and fraud prevention services in order to help protect you from the potential risk of identity theft and fraud. However, receiving a notification letter or being offered these services does not automatically mean you are the victim of identity theft. You should be vigilant about monitoring your credit report and statements from your bank, credit card company and other financial institutions on a monthly basis. If you see transactions that you did not authorize, you should contact your financial institution immediately.

21. How will I know if my information was used by someone else? How will 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.

22. Besides enrolling in credit monitoring and fraud protection services, what other steps can I take to protect myself?

Please refer to the Info Sheet for more information on steps you can take to protect yourself.

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.***