Update on TransLink Cyberattack & Privacy Investigation

June 28, 2021

As you are aware, TransLink was the victim of a sophisticated cyberattack in December 2020. Since then, we have been working tirelessly to investigate what happened and to what extent sensitive personal information was unlawfully accessed.

In my last cyberattack update to you in early March, I committed to write to you again once the investigation was complete. Today, I am writing to provide you with a final update as we conclude our investigation.

Privacy review update

A few months ago, while the investigation was still in its earlier stages, we became aware that certain sensitive personal information had been unlawfully accessed. We moved quickly to notify affected individuals and offer credit monitoring and fraud protection services at that time, even though our investigation was still ongoing.

We then continued to undertake a comprehensive review of the accessed information. The privacy review has proven to be a complex and time-consuming process that unfolded over the past several months, involving extensive analysis and manual data reviews. The review is now complete, and we are in a position to provide affected individuals with a complete list of all sensitive personal information that was unlawfully accessed.

We previously advised that files containing banking information and social insurance numbers of current and former employees of TransLink, CMBC, BCRTC, and Transit Police, and a limited number of spouses had been accessed. With the investigation completed, we now advise that information related to salary or wage rates, deductions, and tax withholdings was also accessed. For some former CMBC employees, records related to WorkSafeBC incidents were also accessed.

Additionally, our investigation recently produced evidence that a restricted network drive that held personal information related to our Access Transit TaxiSaver Program, was unlawfully accessed. We are in the process of notifying affected individuals and informing stakeholder groups.

Notification letters
We are currently in the process of mailing personalized notification letters to impacted individuals. The letters will provide a complete list of the recipients' sensitive personal information, which was subject to access, including the personal information noted in my previous letter.

Credit monitoring
TransLink is taking this incident very seriously. We have been monitoring the situation closely. To date, TransLink is not aware of any misuse of this sensitive personal information. As a precautionary measure, we previously provided you with credit monitoring and fraud protection services, as well as information about how to protect yourself. This information is available on our website and your company's employee portal for your convenience.

I.T. systems recovery efforts
The BTS team has been working diligently over the past six months and they continue to work towards the full recovery of TransLink's information systems.

The majority of TransLink's systems are now back and fully functional while some systems – including core applications such as PeopleSoft and MyK2 – are available, but with only basic features enabled. This allows users to access the application while the team works to restore the full features that were available pre-incident.

Most recently, BTS was able to restore VPN access to more than a thousand employees and has brought back most of our main customer-facing systems such as Trip Planner, Real-Time Transit Info, and Customer Alerts.

As our focus shifts to resuming normal business operations, the remaining work to restore TransLink systems to pre-incident functionality will continue through the summer.

I.T. security & phishing emails
Our I.T. Security program has been a top priority for the TransLink enterprise for many years. As part of those efforts, we have developed multi-year strategies and roadmaps for investing in I.T. security, infrastructure, and software. In recent years, we have continued to expand the program with investments in new systems and

practices. We also conduct regular studies, audits, and exercises such as our annual maturity assessments, penetration tests, and compliance audits.

Over the past six months, BTS has taken many additional steps and measures to build upon our existing information security practices. These include:

- Implementing a red warning banner to identify external emails and risk
- Implementing a "Report Phishing" button at the top of emails
- Expanded use of multi-factor authentication for VPN
- Installing Carbon Black, Microsoft Defender and Cisco Security Umbrella to provide enhanced protection
- Continuing the regular patching of computer assets
- Installing additional vulnerability management agents, including Microsoft's advanced threat protection tools, for continuous scanning and monitoring, to further leverage cyber security intelligence and be proactively alerted of potential threats
- Expanding our security controls to provide enhanced Cloud Security

All these investments and initiatives have been undertaken in addition to our annual awareness campaigns and the ongoing mandatory I.T. security awareness training and exercises for employees.

Cybersecurity is a constantly moving target and we re-evaluate our objectives and targets every year. We also work with an external review partner to update our plans, policies, and standards annually, to ensure we are doing as much as possible to stay ahead of the curve.

I want to remind you that ***cybersecurity is everyone's responsibility.*** Please be vigilant and **report** any suspicious emails, links or attachments through Outlook's Report Message feature or by forwarding the email to the Service Desk (**servicedesk@translink.ca**). Please do not forward the email to your colleagues. The sooner suspicious emails are reported, the quicker BTS can respond to them.

Moving forward

Instances of cybercrime are on the rise globally. Although TransLink has a robust cybersecurity program in place and conducts regular cybersecurity training for employees, this incident shows that no organization is immune. It also confirms the need for continuous monitoring and improvement of our security measures.

We had several security projects that were planned to begin in 2021. We will continue to pursue those projects and will also be making additional investments, to further strengthen our safeguards and protect the security and confidentiality of sensitive personal information in light of evolving cybersecurity threats. We are continuing to review our existing policies, practices, training programs and physical and technical security measures as well, with a view and commitment to continuous improvement. We have also taken the opportunity to harden our systems as we bring them back online.

In addition, we are looking at ways to work with other public agencies, organizations, and businesses to share lessons learned from this incident, to help them avoid falling victim to future cyberattacks. We will all need to be ever vigilant.

You may be aware that a ransom demand ($6M USD) was made when the attack first took place. In the end, TransLink decided to not make any ransom payments to the cybercriminals. There was no guarantee that these cybercriminals would keep their word and not misuse the sensitive personal information that they unlawfully accessed. We were also concerned that any payment to cybercriminals would embolden further attacks on us and other agencies. It was fortunate that we were able to restore our systems from backups, although recovery has certainly been a long and arduous process.

More information
We recognize you may have questions about this incident or its impact on you. Please visit your employee portal or **www.translink.ca/cyberincident** for more information. We have updated these sites with new Frequently Asked Questions and resource information.

We regret that this incident has occurred, and we thank you for your patience throughout our investigation and recovery efforts.

Gigi

Gigi Chen-Kuo
Interim Chief Executive Officer, TransLink