Court File No. VLC-S-S-210074

NO.

VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

G. D.

PLAINTIFF

AND:

SOUTH COAST BRITISH COLUMBIA TRANSPORTATION AUTHORITY

DEFENDANT

NOTICE OF CIVIL CLAIM

Brought under the *Class Proceedings Act*, RSBC 1996, c. 50

This action has been started by the Plaintiff for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the Plaintiff,

(a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,

(b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,

(c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF

PART 1: NATURE OF THE ACTION

1. This is a putative privacy class action arising out of a massive data breach affecting the personal information in the custody or under control of the Defendant ("**TransLink Data Breach**"). The TransLink Data Breach, which was disclosed in December of 2020, resulted in the loss, theft or compromise of highly sensitive personal information of the Defendant's employees and its other stakeholders including, but not limited to, their extremely sensitive and highly valuable banking information.

2. The Plaintiff brings this action on his own behalf and on behalf of all other persons whose personal information was impacted in or as a result of the TransLink Data Breach ("**Class**" or "**Class Members**").

3. The TransLink Data Breach occurred as a result of the Defendant's failure to comply with its obligations under the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 ("**FOIPPA**") and at common law:

a. To protect the Class Members' personal information in their custody or under their control by way of reasonable security measures against such risks as unauthorized access, collection, use, disclosure or disposal; and

b. to not disclose that information without authorization.

4. The TransLink Data Breach has resulted in damages and losses to the Class Members as well as the risk of significant harm to their property, finances, creditworthiness, reputation and relationships. On his own behalf and on behalf of the Class, the Plaintiff seeks to recover compensation by way of general, compensatory, consequential, restitutionary, punitive, aggravated and/or exemplary damages.

PART 2: STATEMENT OF FACTS

A. The Defendant

5. The Defendant South Coast British Columbia Transportation Authority is an entity established under the *South Coast British Columbia Transportation Authority Act*, SBC 1998, c 30. Also known as TransLink, the Defendant is responsible for planning, financing and managing transportation modes and services in the Metro Vancouver region (hereinafter, "**TransLink**").

6. TransLink operates several operating companies through which it provides the transportation services in the Metro Vancouver region, including:

a. Coast Mountain Bus Company, the largest operating company in the integrated TransLink enterprise, which operates more than 96 percent of the Metro Vancouver region's bus service;

b. Metro Vancouver Transit Police, a designated policing unit that operates on Metro Vancouver's transit system;

c. British Columbia Rapid Transit Company which, on behalf of TransLink, maintains and operates two of the three SkyTrain lines in Metro Vancouver; and

d. West Coast Express, a commuter rail service that serves lower mainland.

7. TransLink and each of its operating companies are public bodies within the meaning and for the purposes of the FOIPPA, British Columbia's public sector information privacy and access legislation. As elaborated herein, TransLink and its operating companies violated their obligations outlined in the FOIPPA and at common law to properly manage and protect the Class Members' personal information.

B. The Plaintiff

8. The Plaintiff is an individual residing in British Columbia, and a retiree of the Defendant TransLink.

9. The Plaintiff reasonably believes that his personal information was compromised as a result of the TransLink Data Breach.

10. The Plaintiff is extremely concerned about the loss of his highly valuable personal information. He is furthermore extremely concerned about the implications of the TransLink Data Breach and the risks to him and his fellow retirees as well as other TransLink stakeholders arising thereof.

11. The Plaintiff is furthermore extremely concerned about the lack of meaningful communication on the part of TransLink in regard to the data breach. The Defendant has not provided meaningful clarification regarding the scope and the impact of the TransLink Data Breach on the retirees of TransLink and many of its other stakeholder groups. The Plaintiff is extremely concerned that the Defendant has not been entirely forthright regarding the breadth and implications of the TransLink Data Breach, or the risks to which he and other similarly situated persons are exposed.

12. The Plaintiff has incurred significant damages and losses, and he has gone through significant inconvenience, as a result of the TransLink Data Breach, including to acquire information regarding the scope and the implications of the TransLink Data Breach, its implications with respect to his life and financial affairs, and to mitigate the risk of harm to him as a result thereof.

13. The Plaintiff brings this action in order to hold the Defendant accountable for its breaches of the duty to responsibly manage and safeguard his and the Class Members' personal information, to represent and protect the interests of his fellow retirees and the other stakeholders impacted as a result of the data breach, and to recover compensation for affected individuals.

14. The Plaintiff also brings this action in order to encourage and promote best practices, diligence and accountability in managing highly valuable and sensitive personal information of the residents of British Columbia.

C. The TransLink Data Breach

15. On Thursday, December 3, 2020, Global News reported that, following reports of of significant "suspicious network activity" across major parts of TransLink's computer systems, it had confirmed that TransLink had experienced a cybersecurity attack.

16. According to Global News, a letter allegedly communicated to TransLink by threat actors stated that TransLink's network had been compromised, its computers and servers were locked, and its private data had been downloaded by unauthorized third parties.

17. Following Global News' report on the incident, TransLink acknowledged the data breach, further confirming that various parts and components of TransLink's computer systems had been taken offline. Those included major TransLink systems including employee payroll operations, customer payment systems and various other customer service platforms and features.

18. Although the Defendant declined to confirm the timing or scope of the incident, Global News quoted anonymous "internal sources" as confirming that the data breach was carried out on the evening of Monday, November 30, 2020. Global News' sources also confirmed that the incident "is believed to have started with a successful phishing email," and that it resulted in the breach of TransLink's "entire database."

19. On December 30, 2020, nearly a month after the initial reporting on the TransLink Data Breach, the Defendant confirmed that its employees' highly sensitive social insurance and banking information was compromised as a result of the TransLink Data Breach. It, accordingly, strongly advised employees to sign up for credit monitoring, thereby acknowledging the real risk of significant harm to the employees as a result of the incident.

20. The Defendant has to date failed to provide meaningful disclosure regarding the scope of the TransLink Data Breach and its implications for the other stakeholders of TransLink. Nonetheless, given the nature of the incident, the Plaintiff reasonably believes that all personal information in the custody or under control of the Defendant has been impacted and compromised as a result of the TransLink Data Breach including, but not limited to, employees' information, retirees' information and customers' information.

21. The Defendant possesses regarding the scope of the TransLink Data Breach, the individuals affected thereby, and the personal information impacted or compromised as a result thereof.

D. The Defendant Violated Its Duty to Safeguard the Class Members' Personal Information, and It Violated Class Members' Privacy

22. TransLink and its operating companies are public bodies within the meaning and for the purposes of the FOIPPA. The FOIPPA's purpose is to make public bodies more accountable to the public and to protect personal privacy by, among other things, preventing the unauthorized disclosure of personal information by public

bodies. TransLink and its operating companies are, accordingly, subject to specific requirements outlined in the FOIPPA, including, for the purposes of this proceeding, the following two obligations.

23. *First*, in accordance with section 30 of the FOIPPA, TransLink and its operating companies were (and are) required that they must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

24. *Second*, in accordance with section 30.4 of the FOIPPA, TransLink and its operating companies were (and are) required that they must not disclose the personal information in their custody or under their control except as authorized under the FOIPPA.

25. Additionally, at all material times, the Defendant maintained a stated Privacy Policy applicable to its operations, as well as its operating companies. The Privacy Policy, which constitutes a part of the Defendant's contractual obligations with the Class Members, outlines the TransLink's obligations consistent with those outlined in the FOIPPA, including the following:

> **Accountability**
>
> TransLink is accountable for the personal information in its custody and/or under its control. … Our procedures are reviewed regularly to ensure compliance with FOIPPA, other pertinent laws and leading practices … In addition to developing this Policy, TransLink has established policies that address the prohibition to the unauthorized access, use or disclosure of personal information ….
>
> […]
>
> **How We Protect Your Personal Information**
>
> At TransLink, we recognize the importance of protecting your personal information during the course of providing transit services.

> We take reasonable steps to protect your personal information using physical, electronic and procedural security measures appropriate to the sensitivity of the information in our custody or control. The standards may include safeguards to protect your information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification regardless of the format in which it is held. Our internal policies and procedures, based on "need-to-know" principles, restrict access to your information. We audit our procedures and measures regularly to ensure they are being administered properly and remain effective.
>
> [...]

26. The Defendant violated its obligations at law, as confirmed and acknowledged in its stated Privacy Policy, to responsibly manage the Class Members' personal information and to safeguard it against unauthorized access or theft, as follows:

    a. the Defendant failed to introduce, implement or maintain proper technical or technological measures and capabilities or procedures to ensure that the personal information in its custody or under its control was properly managed and protected appropriate to the sensitivity of that information;

    b. the Defendant failed to validate, review, update or audit its technical and technological defences and its procedural safeguards to ensure they remained effective in protecting the personal information in its custody or under its control;

    c. the Defendant failed to properly manage the risk of improper access, disclosure or theft of personal information by restricting access to the personal information in its custody or under its control based on "need-to-know" principles;

    d. the Defendant failed to properly encrypt the personal information in its custody or under its control;

e. the Defendant failed to provide proper and adequate training, and it failed to introduce, implement or maintain proper human resources or information technology policies and procedures to ensure its employees or agents acting on its behalf properly managed and protected the personal information in its possession or under its control;

f. the Defendant failed to effectively monitor its computer systems and networks for improper activities to detect and respond to the data breach diligently and in a timely fashion;

g. the Defendant failed to introduce, implement or maintain a proper and effective incident response plan to isolate and respond to the date breach, and to mitigate the damages resulting thereof in a timely fashion; and/or

h. the Defendant failed to act diligently and in a timely fashion to communicate to the Class Members regarding the scope and the implications of the data breach and deprived the Class Members of the opportunity to take steps to mitigate their risks for nearly a month.

27. The Defendant's actions and omissions and its breaches of duty were carried out knowingly or recklessly. The Defendant knew or it ought to have known that it possessed a significant volume of highly valuable personal information on the residents of British Columbia and that, as a result, it was the subject of a heightened risk of cyberattacks. It, accordingly, knew or ought to have known that, consistent with its legal obligations, it was required to implemented enhanced security measures appropriate to the sensitivity of the personal information its custody or under its control. The Defendant failed to do exercise the diligence required of it in the circumstances, disregarding its legal obligations offending the Class Members' trust, and violating the Class Members' reasonable expectation of privacy.

E. The Plaintiff's and the Class Members' Damages and Losses

28. The Defendant is entrusted with significant, highly valuable personal and personally identifiable information regarding the Class Members. That information provides a nearly fulsome picture about an individual as a person, their preferences, daily lives, daily movements, whereabouts, activities, and finances. The information in the Defendant's possession is, as such, highly valuable and attractive to various groups for various purposes, including for illicit activities that are harmful to the Class Members, their livelihood or reputation.

29. The Defendant's actions and omissions and its breaches of duty resulting in the TransLink Data Breach constitute intentional, wilfull or reckless conduct without due regard to its specific obligations under the FOIPPA, as acknowledged in its own Privacy Policy, or the Plaintiff's and the other Class Members' reasonable privacy expectations.

30. Some of the Class Members' personal information compromised in the TransLink Data Breach is irreplaceable, or it can be changed only with significant costs and through a burdensome process, including the Class Members' names, dates of birth, social insurance information and banking information.

31. The Plaintiff and the other Class Members have incurred and will continue to incur significant damages and losses as a result of the TransLink Data Breach, including significant costs and time required to respond to it.

32. The TransLink Data Breach also exposes the Plaintiff and the Class Members to a real risk of significant harm, including identity theft, humiliation, damages to reputation or relationships, loss of employment, business or professional opportunities, financial loss and negative effects on the credit record.

33. The Plaintiff pleads and he seeks to recover general, compensatory, consequential, aggravated and/or exemplary damages for:

    a. loss of valuable personal information;

    b. loss of privacy;

c. damages stemming from, or caused by, identity fraud schemes including, without limitation, damage to credit ratings, damage to perceive credit worthiness;

d. damage to reputation or relationships;

e. costs and expenses incurred or required to protect against identity theft or other misuse or abuse of personal information;

f. lost or wasted time and inconvenience in responding to the TransLink Data Breach, including time wasted on learning information regarding the circumstances and consequences of the data breach and to mitigate the risk of significant harm resulting thereof.

34. The Plaintiff also claims the costs of credit monitoring for the benefit and on behalf of every Class Member whose social insurance number, banking or credit information was exposed for the duration of seven years.

PART 3: RELIEF SOUGHT

1. On behalf of himself and the Class, the Plaintiff seeks:

a. an order pursuant to the *Class Proceedings Act*, RSBC 1996, c. 50, certifying this action as a class proceeding and appointing the Plaintiff as the representative plaintiff for the Class, defined as follows:

> all persons whose personal information was impacted in or as a result of the TransLink Data Breach, which TransLink disclosed in December of 2020;

b. general, compensatory, consequential, aggravated and/or exemplary damages, in an amount to be determined to the extent possible in an aggregated basis, for:

i. breaches of section 1 of the *Privacy Act*, RSCB 1996, c. 373, as amended;

ii. intrusion upon seclusion;

iii. breach of contract;

iv. negligence;

v. breach of confidence; and/or

vi. vicarious liability;

c. an order directing a reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

d. pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, RSBC 1996, c.79;

e. costs of this action; and

f. such further and other relief as this Honourable Court may deem just.

PART 4: LEGAL BASIS

1. The Plaintiff incorporates, repeats and pleads herein the pleadings contained in Parts 1, 2 and 3 hereof.

2. The Defendant violated its duties under the FOIPPA, contractually and at common law to properly, responsibly and diligently manage and protect the Class Members' personal information.

3. As a result of its actions and omissions and its breaches of duties, as elaborated herein, the Defendant enabled the TransLink Data Breach, improperly disclosed the Class Members' personal information or caused it to be exposed to unauthorized third parties. The Defendant as such violated the Class Members'

privacy willfully or recklessly, without a claim of right, and in a manner that is offensive to a reasonable person causing anguish, distress or humiliation.

4. TransLink's stated Privacy Policy constituted part of the Class Members' contracts with the Defendant. The Defendant breached the terms of its contract with the Class Members or it failed to perform its obligation to reasonably safeguard the Class Members' personal information; the breach was unexcused; all conditions precedent to defendant's duty to perform were fulfilled by the Class Members; the Class Members incurred damages as a result of the breach; and causation and damages were a foreseeable consequence of the Defendant's breach of contract as a result of its failure to reasonably safeguard the Class Members' personal information against unauthorized access or theft. The Class Members' contract with the Defendant is a contract of adhesion to which the doctrine of *contra proferentem* applies.

5. The Defendant owed a duty of care to the Class Members to properly manage and protect their personal information, with which the Class Members entrusted the Defendant. The Class Members are current or former employees, customers and other stakeholders of the Defendant, and are known or identifiable to it. The duty of care as such does not result in an unlimited liability. It was reasonably foreseeable to the Defendant, as it has acknowledged in its Privacy Policy, it was important to the Class Members that their personal information be reasonably protected. It was as such also reasonably foreseeable to the Defendant that the Class Members would incur damages and losses as a result of the Defendant's breaches of its duty of care. The Class Members did incur damages as a result of the Defendant's breaches of duty of care and the TransLink Data Breach.

6. The Defendant was entrusted with the Class Members' private and confidential information with the expectation that it would maintain the confidentiality of that information. The Defendant, however, improperly disclosed Class Members' private information to unauthorized third parties without or in excess of

authorization, thereby breaching the Class Members' confidence in providing the Defendant with their highly valuable and sensitive personal information.

7. The Class Members' personal information is highly valuable. The Defendant's failure to protect the Class Members' personal information has caused them damages for, among other things, wasted time and inconvenience in responding to the TransLink Data Breach and other costs and out of pocket expenses. Additionally, the Defendant's breaches of duty have exposed the Class Members to a real risk of significant harm including, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft and/or negative effects on the credit record.

8. The Plaintiff seeks damages, to the extent possible to be assessed in the aggregate, for:

   a. loss of valuable personal information;

   b. loss of privacy;

   c. damages stemming from, or caused by, identity fraud schemes including, without limitation, damage to credit ratings, damage to perceive credit worthiness;

   d. damage to reputation or relationships;

   e. costs and expenses incurred or required to protect against identity theft or other misuse or abuse of personal information;

   f. lost or wasted time and inconvenience in responding to the TransLink Data Breach, including time wasted on learning information regarding the circumstances and consequences of the data breach and to mitigate the risk of significant harm resulting thereof;

   g. costs of appropriate credit monitoring for a duration commensurate with the sensitivity of the information that was improperly compromised as a result

of the Defendant's conduct and its breaches of duty to protect the Class Members' personal information.

9. In the alternative, the Plaintiff and the Class plead an entitlement to compensation and claim an accounting or such other restitutionary relief as may be available for all revenues or profits generated by the Defendant from, as a result of, or reasonably connected with its violations contractually and at law to responsibly and diligently manage the Class Members' personal information, and to safeguard that information against unauthorized access or theft.

10. In addition to its direct liability, TransLink is vicariously liable for the acts and omissions of its operating companies, subsidiaries, partners, and their respective directors, officers, employees and agents.

Plaintiff's address for service: 1727 W Broadway Suite 400, Vancouver, BC V6J IY2

Place of trial: Vancouver, British Columbia.

The address of the registry is: 800 Smithe Street, Vancouver, BC V6Z 2E1.

Date: January 6, 2021

DIAMOND & DIAMOND LAWYERS LLP
1727 W Broadway Suite 400
Vancouver, BC V6J IY2
T: (778) 897-0080
F: (778) 897-0208

Richard Chang
rchang@diamondlaw.ca

Darryl Singer
darryl@diamondlaw.ca

KND COMPLEX LITIGATION
1186 Eglinton Ave West
Toronto, ON M6C 2E3
T: (416) 769-4107

Eli Karp
ek@knd.law

Sage Nematollahi
sn@knd.law

Counsel for the Plaintiff

Rule 7-1(1) of *the Supreme Court Civil Rules* states:

> (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
>
> (a) prepare a list of documents in Form 22 that lists
>
> (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
>
> (ii) all other documents to which the party intends to refer at trial, and
>
> (b) serve the list on all parties of record.

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28 (the "*CJPTA*") in respect of the Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to section 10 of the *CJPTA* because this proceeding:

(e) concerns contractual obligations, and

(i) the contractual obligations, to a substantial extent, were to be performed in British Columbia;

(f) concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

APPENDIX

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

his is a putative privacy class action arising out of a massive data breach in or around December 2020 affecting the personal information in the custody or control of the Defendant ("**TransLink Data Breach**"). The TransLink Data Breach resulted in the loss, theft or compromise of highly sensitive personal information of the Defendant's employees and other stakeholders including, but not limited to, extremely sensitive and highly valuable banking information. The Plaintiff brings this action on his own behalf and on behalf of all other persons whose personal information was impacted in or as a result of the TransLink Data Breach ("**Class**" or "**Class Members**"). On his own behalf and on behalf of the Class, the Plaintiff seeks to recover compensation by way of general, compensatory, consequential, restitutionary, punitive, aggravated and/or exemplary damages.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident
[ ] medical malpractice
[ ] another cause

A dispute concerning:

[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] the provision of goods or services or other general commercial matters
[ ] investment losses
[ ] an employment relationship
[ ] a will or other issues concerning the probate of an estate
[X] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[X] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know

Part 4: ENACTMENTS RELIED ON:

1. *Class Proceedings Act*, RSBC 1996, c. 50, as amended
2. *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c.28, as amended
3. *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, as amended
4. *Privacy Act*, RSCB 1996, c. 373, as amended
5. *Court Order Interest Act*, RSBC 1996, c.79, as amended