IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *G.D. v. South Coast British Columbia Transportation Authority,* 2026 BCSC 773

Date: 20260429
Docket: S210074
Registry: Vancouver

Between:

G.D., Allan Smith, Christopher Holt, James Thom and Brent Johnston
Plaintiffs

And

South Coast British Columbia Transportation Authority
Defendant

Before: The Honourable Madam Justice Wilkinson

Reasons for Judgment

Counsel for the Plaintiffs:	P. Bates S. Nematollahi
Counsel for the Defendant:	B.W. Dixon M.T. Maniago
Place and Dates of Hearing:	Vancouver, B.C. August 18-19, 2025
Written Submissions Received:	December 22 and 23, 2025
Place and Date of Judgment:	Vancouver, B.C. April 29, 2026

Table of Contents

[1] The plaintiffs seek certification of their proposed class proceeding under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 [*CPA*] on their own behalf and on behalf of all persons, excluding employees of the defendant who are members of MoveUp, who were notified by the defendant that their sensitive personal information may have been compromised as a result of a data security breach in 2020 that affected the computer networks and systems of the defendant.

[2] On June 5, 2023, I rendered my decision indexed at *G.D. v. South Coast British Columbia Transportation Authority*, 2023 BCSC 958 [*BCSC Decision*] on the plaintiffs' application for certification. In that decision I dismissed the application on the basis that the claims did not satisfy the requirements under s. 4(1)(a) of the *CPA*, because the claims were bound to fail. My decision did not address the remaining requirements for certification under the *CPA*.

[3] On July 4, 2024, the Court of Appeal allowed an appeal in this proceeding, indexed at *G.D. v. South Coast British Columbia Transportation Authority*, 2024 BCCA 252 [*BCCA Decision*], holding that the plaintiffs' pleadings disclose causes of action in negligence and under s. 1 of the *Privacy Act*, R.S.B.C. 1996, c. 373.

[4] On March 6, 2025, the Supreme Court of Canada denied leave to appeal the *BCCA Decision*: *South Coast British Columbia Transportation Authority v. G.D., et al.*, [2024] S.C.C.A. No. 373.

[5] The plaintiffs have amended their claim to pursue only the cause of action under section 1 of the *Privacy Act*.

[6] The *BCCA Decision* dealt with the pleadings alone under s. 4(1)(a), in which the facts pleaded are assumed to be true. This includes the plea that the class members' information was compromised or accessed by the cybercriminal(s). The Court of Appeal remitted the matter back to this Court to consider the remaining certification criteria to determine whether certification under the *CPA* is appropriate.

[7] For the reasons set out below, I grant the plaintiffs' application for certification.

Background

[8] The background to this matter is set out at paras. 3-16 of the BCSC *Decision*:

> [3] The defendant, South Coast British Columbia Transportation Authority ("TransLink"), is a statutorily-created entity continued under the *South Coast British Columbia Transportation Authority Act,* S.B.C. 1998, c. 30 [*SCBCTA Act*]. As set out in the *SCBCTA Act*, TransLink's purpose is to provide a regional transportation system in Metro Vancouver that moves people and goods and supports the regional growth strategy, provincial and regional environmental objectives, including air quality and greenhouse gas emission reduction objectives, and the economic development of the transportation service region.
>
> [4] TransLink handles the planning, financing and management required to run the regional transportation system. TransLink's transit services include bus, community shuttle, ferries (SeaBus), rapid transit (SkyTrain), commuter rail (West Coast Express) and custom transit services for persons with disabilities (Access Transit Program). Transit services are delivered through TransLink's operating subsidiaries: Coast Mountain Bus Company Ltd. ("CMBC"), British Columbia Rapid Transit Company Ltd. ("BCRTC"), and West Coast Express Ltd. ("WCE"). Policing services on the transit system are delivered through South Coast British Columbia Transportation Authority Transit Police ("Transit Police"). Certain third parties are also involved in the delivery of transit services.
>
> [5] The plaintiffs are previous employees of, and have all since retired from their employment with, TransLink. Together, they seek to be appointed as the proposed representative plaintiffs on their own behalf, and on behalf of all other persons whose personal information was impacted in or as a result of a data security breach in 2020 (the "Data Breach") that affected the computer networks and systems of TransLink (the "Class Members").
>
> [6] On December 1, 2020, TransLink's information technology team, Business Technology Services ("BTS"), discovered ransomware on TransLink's IT network. TransLink took steps to respond and contain the threat, including isolating and shutting down certain IT infrastructure and systems, notifying law enforcement, and launching an investigation.
>
> [7] On December 3, 2020, TransLink confirmed that part of its IT infrastructure had been the target of a ransomware attack. Despite TransLink's cybersecurity program, cybercriminals were able to gain unauthorized access into TransLink's network security and insert the ransomware following a successful phishing attempt on one of TransLink's operating subsidiaries' employees.
>
> [8] On December 4, 2022, TransLink submitted a breach report to the Office of the Information and Privacy Commissioner for British Columbia ("OIPC"). The OIPC opened a file in respect of the 2020 Cyberattack on December 7, 2022.
>
> [9] While its investigation was ongoing, TransLink offered a complimentary two-year credit monitoring and fraud protection service ("Credit Monitoring Package") to all then-current enterprise employees, former and retired

enterprise employees, TaxiSaver cheque payors, and affected third parties. Whether all of the persons affected received that information is disputed.

[10] In addition, TransLink created a dedicated public webpage with information about the 2020 Cyberattack, offered live online information sessions to current, former and retired enterprise employees, and set up a dedicated call centre for affected individuals

[11] TransLink's investigation continued through to June 2021. TransLink was able to confirm that various files and folders within the breached network drive were accessed by cybercriminals. The review confirmed that these files and folders contained a variety of information, including:

a) personal information related to payroll administration for TransLink, CMBC, and Transit Police employees;

b) sensitive personal information of some BCRTC and WCE employees;

c) sensitive personal information of some, but not all, former and retired enterprise employees and a limited number of their spouses and beneficiaries;

d) sensitive personal information about certain third parties, including:

   i. HandyDART operators who were not TransLink's employees but who had been provided with transit passes and tax receipts for the transit pass benefits;

   ii. former BC Transit employees; and

   iii. third parties involved in incidents involving TransLink vehicles, such as witnesses, injured third parties, and other drivers involved; and

e) scanned images of personal cheques written for the purpose of purchasing TaxiSaver coupons in TransLink's Access Transit Program or for the repayment of expenses or benefits paid for by the employer on behalf of employees. The payor on the cheques is not always an Access Transit customer (in the case of the TaxiSaver cheques) or an employee (in the case of the expense cheques), but in some cases is another person, such as a family member, friend, care provider, or spouse.

[12] In addition to confirming which files and folders were accessed by the cybercriminals, TransLink was also able to confirm that data was exfiltrated from, or copied out of, TransLink's systems. However, TransLink's records do not confirm what data in particular was exfiltrated, including whether or not the cybercriminals looked at or copied the sensitive personal information stored in the files and folders accessed by the cybercriminals. At most, TransLink's investigation enabled it to identify individuals' sensitive personal information that was subject to access, or exposed to view, by the cybercriminals.

[13] Around mid-February 2021, TransLink began to deliver personalized notification letters to individuals whose personal information was confirmed to

> have been subject to access by the cybercriminals. The personalized notification letters identified what specific sensitive personal information TransLink determined was contained in the folders or files accessed by the cybercriminals and provided activation codes for the Credit Monitoring Program. This personalized notification process continued throughout the following months as TransLink's investigation continued to reveal whose personal information was subject to access.
>
> [14] In all, a total of approximately 57,820 notification letters were sent out to 38,958 unique individuals. Because more than one restricted data folder was accessed and each folder contained different information, the categories of the sensitive information that was subject to access varied between individuals. The personalized notification letters set out what information was subject to unauthorized access.
>
> [15] A subset of TransLink's employees are members of labour unions. Those unions commenced grievances against TransLink or certain of its operating divisions in relation to the Data Breach.
>
> [16] On March 30, 2022, the OIPC closed its file with respect to its monitoring of the Data Breach.

Certification Requirements Under the *CPA*

[9] Pursuant to s. 4(1), the plaintiff at certification bears the onus of establishing that the pleadings disclose a cause of action and the onus of showing, on evidence, "some basis in fact" that the other requirements for certification of this proceeding are met: see *Hollick v. Toronto (City),* 2001 SCC 68, at para. 25; *Pro-Sys Consultants Ltd. v. Microsoft Corporation*, 2013 SCC 57, at paras. 99-100.

[10] Section 4(1) of the *CPA* provides as follows:

> **4** (1)Subject to subsections (3) and (4), the court must certify a proceeding as a class proceeding on an application under section 2 or 3 if all of the following requirements are met:
>
> (a) the pleadings disclose a cause of action;
>
> (b) there is an identifiable class of 2 or more persons;
>
> (c) the claims of the class members raise common issues, whether or not those common issues predominate over issues affecting only individual members;
>
> (d) a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues;
>
> (e) there is a representative plaintiff who
>
> (i) would fairly and adequately represent the interests of the class,

> (ii) has produced a plan for the proceeding that sets out a workable method of advancing the proceeding on behalf of the class and of notifying class members of the proceeding, and
>
> (iii) does not have, on the common issues, an interest that is in conflict with the interests of other class members.

[11] The "some basis in fact" standard to be applied to ss. 4(1)(b) through (e) requires the plaintiff to adduce some evidence and requires the Court to move beyond mere "symbolic scrutiny". Indeed, "some basis in fact" cannot amount to mere speculation. Instead, there must be a genuine evidentiary foundation to satisfy the Court that the conditions for certification have been met to such a degree as to allow the matter to proceed on a class-wide basis without foundering at the merits stage by reason of the requirements of s. 4(1) of the *CPA* not having been met: *Pro-Sys* at paras. 103-104.

[12] The plaintiffs are only required to provide enough evidence that certification of a common issue functions as a "meaningful screening device". In assessing the existence of common issues, including those related to alleged harm, the Court is called upon not only to consider whether there is a basis in fact for the commonality of the proposed question, or the potential for class-wide determination, including with the use of a proposed workable class-wide methodology, but also whether there is a basis in fact for the existence of the issue. There can be no purpose served by certification of abstract questions that do not resolve issues that actually exist. This test is assessed on the basis of admissible evidence: *Ernewein v. General Motors of Canada Ltd.,* 2005 BCCA 540 at para. 31; *Syngenta AG v. Van Wijngaarden,* 2025 BCCA 334 at paras. 60-63. There must also be a consideration of whether there is a basis in fact for the existence of a common issue: *Charlton v. Abbott Laboratories, Ltd.*, 2015 BCCA 26 at para. 85. As Justice Matthews stated, paraphrasing Chief Justice Hinkson, it is "difficult to conceive of how one can say there is evidence that an issue is common unless there is evidence that the issue exists": *Bowman v. Kimberly-Clark Corporation,* 2023 BCSC 1495 at para. 134, paraphrasing *O'Connor v. Canadian Pacific Railway Limited*, 2023 BCSC 1371, at para. 256.

[13] As set out in *Thorburn v. British Columbia*, 2012 BCSC 1585, at para. 117, leave ref'd, 2013 BCCA 480, this Court has recognized the overarching importance of its gate-keeping role to screen claims to ensure they are suitable for treatment in a class action, in fairness to all parties:

> The goal of the CPA is to be fair to both plaintiffs and defendants ... it is imperative to have a scrupulous and effective screening process, so that the court does not sacrifice the ultimate goal of a just determination between the parties on the altar of expediency.

CPA* s. 4(1)(a) - Cause of Action under the *Privacy Act

[14] The plaintiffs plead that the defendant violated its obligation to safeguard the putative Class Members' sensitive personal information under two provincial privacy statutes. The plaintiffs assert a statutory right of action for breaches of s. 1 of the *Privacy Act*. They further plead that TransLink is subject to ss. 30 and 30.4 of the *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165 [*FIPPA*]. They argue that TransLink violated the putative Class Members' privacy wilfully or recklessly and without a claim of right.

[15] The *CPA* s. 4(1)(a) criterion has been satisfied only with respect to the cause of action for the claim under the *Privacy Act* and no other cause of action is advanced. Therefore, I agree with the defendant that the pleadings related to relief disconnected from that cause of action and the plea regarding vicarious liability are bound to fail.

[16] For example, the plaintiffs seek an "accounting" and disgorgement of "all revenues or profits" generated by TransLink "from, as a result of, or reasonably connected with its violations at law to responsibly and diligently manage the Class Members' personal information, and to safeguard that information against unauthorized access or theft". There is no basis for that remedy on the cause of action relied upon.

[17] The plaintiffs also appear to continue to assert a claim in vicarious liability as set out under a proposed a common issue, despite that plea not finding any endorsement by the Court of Appeal. The claim is bare on this point and reads: "In

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

[18] Vicarious liability operates to hold one person responsible for the conduct of another because of the relationship between them. This doctrine is triggered in the context of certain relationships, including employer and employee or agents and principals: *Lee v. Transamerica Life Canada*, 2016 BCSC 191 at paras. 95 and 96. There is no question that TransLink is a statutory body corporate separate and apart from its operating subsidiaries. By statute, and for the purposes of the *Labour Relations Code*, R.S.B.C. 1996, c. 244, TransLink must not be treated as one employer with any person, including its subsidiaries: *SCBCTA Act*, SBC 1998, c 30 at s. 13; *British Columbia Rapid Transit Company Ltd v. Canadian Union of Public Employees, Local 7000,* 2014 CanLII 52789 (BC LRB). To the extent that the plaintiffs ignore the legal persona of TransLink and base their vicarious liability claim on the doctrine of piercing the corporate veil, their claim is without merit.

[19] The claim does not set out material facts relating to employment, agency, or another recognized category that could support a claim in vicarious liability, nor any material facts that impugn corporate separateness. The claim of vicarious liability is bound to fail.

***CPA* s. 4(1)(b) - Identifiable Class**

[20] The defendant criticized the use of the term “impacted” in the proposed class definition, which may be too vague. The plaintiffs proposed an alternative definition which in my view addresses any concern with regard to the use of the term “impacted” and is acceptable for certification under s. 4(1)(b):

> All persons who were notified by the Defendant that their sensitive personal information may have been compromised in the TransLink Data Breach, excluding the Defendant's employees who are members of MoveUp.

CPA s. 4(1)(c) Proposed Common Issues

Proposed Common Issue 1: Access

[21] Proposed common issue 1 is "Was the Class Members' sensitive personal information accessed by unauthorized parties in the Data Breach?"

[22] All other proposed common issues flow from this first question.

[23] In its submissions the defendant acknowledges that its records confirm that an unknown criminal hacker was able to access its network system, and that folders and files containing the putative Class Members' personal information were accessed. The defendant further acknowledges that data was removed or copied from its systems, but its records do not confirm which (if any) of the sensitive personal information was compromised.

[24] Based on this information, the defendant argues that there is no basis in fact that the issue of access to the personal information can be determined commonly. This is because, it submits, the defendant's records do not allow it to determine what sensitive personal information within those folders and files was actually looked at by the unknown criminal hacker or whether or not that sensitive personal information was copied out of or stolen (or "exfiltrated") from its network system. In other words, while sensitive personal information was potentially compromised or "subject to access", in that the hacker had the ability to open various documents within the breached system, look at the information inside, and copy it, it has no records that can confirm which specific personal information was in fact looked at or copied or stolen.

[25] However, "access" to information in the context of data privacy laws is not synonymous to examining—or in the defendant's word, "look[ing] at"—the information. While the Court in *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 did not require a finding that the hackers examined the personal information, whether that information was accessed was not in issue. In *Sweet v. Canada*, 2022 FC 1228 at paras 1-6, 68, there was evidence that the hackers had misused the

personal information. In the case before me, whether or not the hackers misused the personal information of some or all of the Class Members has no bearing at the certification stage or at trial of the common issues. The plaintiffs have confined their claim to s. 1 of the *Privacy Act* and need not show or prove any kind of harm in order to succeed.

[26] Also, "access" to personal information is not synonymous with obtaining a copy of the personal information. For the plaintiffs to establish at trial that the putative Class Members' sensitive personal information was accessed, therefore, they do not need to prove that the information was also copied. The defendant itself made that distinction in the breach notification it sent to the putative Class Members, which stated as follows:

> The investigation into the privacy breach is now complete. All individuals whose sensitive personal information was identified as having been accessed by the cyberattackers will be sent a written notification. While there is no way to know for certain what information the attackers copied, we hope you will take the suggested precautions to protect yourself from the potential risk.
>
> What sensitive personal information was accessed?
>
> The accessed folders contained the following sensitive personal information about you:
>
> social insurance number
>
> bank account number
>
> WorkSafe reports/summaries
>
> Home address
>
> date of birth
>
> salary/wage rate with tax withholding and/or deductions

[27] Lastly, there will be a common issue amongst the putative class member as to whether their information was in fact accessed. This fact can be determined at the trial of the common issues. The trial judge may agree with the plaintiffs that the personal information was "accessed" in violation of Translink's obligation to safeguard the information, irrespective of whether or not the hackers also downloaded the information. If, however, the trial judge determines that "access" requires that the hackers also downloaded copies of the personal information, there is some basis in fact that this fact can be determined on a class-wide basis, given

the defendant acknowledges that: (a) the folders containing the information were exposed to the hackers; and (b) the hackers downloaded at least some data.

[28] With the benefit of the full evidentiary record, the trial judge may find that the sensitive personal information of a subset of the putative Class Members was not "accessed." That possibility would however not be a bar to certification: *CPA* at ss. 27-28. The plaintiffs are required to prove this fact on a balance of probabilities. The defendant already acknowledges that the personal information at question "may have been compromised." This further establishes some basis in fact that the plaintiffs can meet this burden on a class-wide basis.

[29] The defendant also argued that it would be impossible to determine which types of sensitive personal information were "accessed" with respect to each putative Class Member. However, it is a matter of record that the information that was contained in the folders at issue is known, and the defendant has itself been able to determine that information with precision with respect to each putative Class Member. The variability of the sensitive personal information would otherwise not bar certification, as the evidence is clear that, with respect to each putative Class Member, a combination of their sensitive personal information was affected.

[30] Common issue 1 is approved.

Proposed Common Issue 2: Breach of FIPPA

[31] Proposed common issue 2 is "If the answer to question 1 is yes, was the unauthorized access to the Class Members' sensitive personal information as a result of the defendant violating its statutory duties under s. 30 of *FIPPA*?"

[32] As this is an integral and necessary ingredient of the cause of action as pleaded, its determination would substantially advance the claims of all of the putative Class Members. Because all of the putative Class Members were subject to the same Data Breach, there is some basis in fact that determination of this question is not contingent on individual inquiries.

Proposed Common Issue 3: Privacy Act

[33] The plaintiffs propose the following common issue related to the *Privacy Act* claim: "If the answer to question 2 is yes, did the defendant violate the privacy of the Class Members, or any of them, wilfully, without a claim of right?"

[34] This common issue addresses the cause of action prescribed in s. 1 of the *Privacy Act.* It asks whether the defendant's conduct—in the manner in which it stored the Class Members' personal information and the manner in which it maintained the information—violated the privacy of the Class Members wilfully without a claim of right.

[35] The Court of Appeal recently declined to clarify the meaning of the term “wilful” in the *Privacy Act*, noting that recklessness may not be sufficient to establish wilfulness in the context of the *Privacy Act*: *Situmorang v. Google,* 2024 BCCA 9 at paras. 79-80.

[36] This is not the appropriate time to resolve the meaning of “wilful” in the context of the *Privacy Act*: *Jiang v. Peoples Trust Company,* 2017 BCCA 119 at para. 64; *Lin v. Airbnb, Inc.,* 2019 FC 1563 at para. 54. Even if recklessness is not the same as “wilful” within the meaning of the *Privacy Act,* the plaintiff has provided evidence showing that there is some basis in fact not only that the defendant’s violations were merely reckless, but also that they may satisfy other definitions of “wilful” based on greater intentionality.

[37] Mr. Vogel, a cybersecurity expert, opines that certain of the apparent deficiencies in the defendant's computer security measures existed in basic foundational areas, including:

a) cyber security framework;

b) cyber security awareness;

c) access control;

d) data encryption;

e) cyber security threat monitoring;

f) endpoint protection;

g) user authentication;

h) vulnerability assessment and penetration testing; and

i) executive oversight.

[38] This issue is common amongst all putative Class Members, and approved.

Proposed Common Issues 4-7: Damages and Compensation

[39] The plaintiffs propose the following common issues regarding damages and compensation:

a) Common issue 4: If the answer to question 3 is yes, is the defendant liable to pay damages (whether general, compensatory, consequential, moral, restitutionary, punitive, nominal, aggravated or exemplary damages) or other monetary relief or compensation to the Class Members?

b) Common issue 5: If the answer to question 4 is yes, can some of the damages or monetary compensation to the Class be calculated in the aggregate pursuant to s. 29 of the *CPA*?

c) Common issue 6: Is the answer to question 5 is yes, what is the proper aggregated monetary relief to be awarded?

d) Common issue 7: If any portion of the Class Members' damages or other monetary relief or compensation should be assessed on an individual basis, what is the appropriate measure of the compensation to be paid to the Class Members?

[40] If each class member's damages may need to be individually assessed after determination of the common issues, it is not an impediment to certification: *CPA* at s. 7.

[41] General and nominal damages may be awarded for the breach of the *Privacy Act,* without proof of damages or losses, and on an aggregated basis: *Ari v. Insurance Corportaiton of British* Columbia, 2022 BCSC 1475 *[Ari BCSC 2022]* at paras. 78-82; *Douez v. Facebook, Inc*., 2022 BCSC 914 at para. 134.

[42] The determination of punitive damages turns on a consideration of the defendant's conduct. The plaintiffs are required to show some basis in fact that the defendant's conduct constituted a marked departure from ordinary standards of decent behaviour: *Ari v. Insurance Corporation of British Columbia*, 2019 BCCA 183 at para. 29. Aggregated punitive damages may also be certified as a common issue: *Escobar v. Ocean Pacific Ltd*., 2021 BCSC 2414 at para. 197.

[43] Mr. Vogel provides some basis in fact that the defendant's cybersecurity controls and system were deficient in foundational areas. For example, the defendant continued to retain the personal information while it no longer needed it, and failed to encrypt the personal information, despite being on notice of the heightened risk of cyberattacks. There is some basis in fact for punitive damages.

[44] Consequential damages are a form of compensatory damages that arise indirectly from the injurious incident. In *Young v. British Columbia*, 2016 BCCA 25 at para. 39, the Court of Appeal defined consequential damages as: "[l]osses that do not flow directly and immediately from an injurious act but that result indirectly from the act."

[45] Here, the plaintiff claims consequential damages for the costs of responding to the data breach, such as the time spent to change bank account information or credit card information as a result of the compromise of the plaintiffs' and putative Class Members' personal information. Even though they are an indirect result of the Data Breach, they are arguably proximate and foreseeable: the defendant would

have reasonably foreseen that the plaintiffs and putative Class Members would suffer this kind of damage as a result of the Data Breach. Some basis in fact for this is found in the remedial credit monitoring and insurance offered to the putative Class Members by the defendant.

[46] The Court of Appeal in *Tucci v. Peoples Trust Company,* 2020 BCCA 246 at paras. 120-122, held that consequential damages arising from the expenses and injuries of responding to a data breach may be determined on an aggregated basis. In *Sweet* at paras. 23-30 the Federal Court similarly decided that there are methodologies that could be used to determine the costs of a data breach on an aggregated basis. Dr. Cavoukian's report provides some basis in fact that psychological harms can be assessed by way of structured interviewing, psychometric assessment, and reviewing victims' medical and occupational records. There is some basis in fact for consequential damages.

[47] Restitutionary damages require a defendant to give up a benefit acquired from the plaintiff. This is in contrast to disgorgement, which is exclusively in respect to a defendant's wrongful gain. The plaintiffs have provided no basis in fact that TransLink benefitted from any alleged wrongdoing, the value of that benefit, or that corresponding loss was suffered on a class-wide basis. This head of damages is not certifiable.

[48] Compensatory, moral and aggravated damages can include pecuniary and non-pecuniary awards. The plaintiffs concede that the determination of these damages would require individual inquiries.

[49] The plaintiffs depose to time and out of pocket costs they have incurred which they say is a result of the Data Breach.

[50] The plaintiffs agree that moral damages for stress and anxiety would be awarded only when they are serious and prolonged and rise above life's ordinary annoyances: *Mustapha v. Culligan of Canada Ltd*., 2008 SCC 27, at para 9. Dr. Cavoukian, a privacy expert with training in psychology, opines that a data breach

that compromises sensitive information as well as financial information, or detailed personal information such as a birth date and home address, exposes those whose information is compromised to a real risk of psychological and financial harm beyond mere inconvenience. None of the plaintiffs deposed that they have suffered psychological harm, although some depose they believe their sensitive information or identity is at risk or they feel insecure as a result of the Data Breach. There is no basis in fact to support a possible finding of a serious and prolonged stress and anxiety.

[51] In *Ari BCSC 2022*, the Court drew a distinction between the class members who were entitled to compensation for general damages, and those who claimed to have suffered compensatory damages or additional non-pecuniary damages. For the latter group, the Court directed that a process to be devised in the future would deal with those individual issues:

> [80] *Pootlass v. Pootlass* (1999), 1999 CanLII 6665 (BC SC), 63 B.C.L.R. (3d) 305 (S.C.) involved slander, another tort that is actionable *per se*. The Court said at para. 62 that the law presumes that some damage will flow in the ordinary course of events from the mere invasion of the plaintiff's rights. I find that in creating a tort that is actionable *per se,* the legislature created a presumption that some compensable loss flows from the invasion of privacy rights. I also agree with the plaintiff that any compensation awarded in the absence of proof of damages must, by definition, be non-pecuniary.
>
> [81] ICBC may be correct that, in the absence of specific proof of damages, class members may only be entitled to a nominal or modest conventional award, but the issue of quantum of damages is not before me.
>
> [82] I conclude that all class members are entitled to an award of non-pecuniary damages arising from the mere fact that their privacy was violated and that award can be made on a class-wide basis. Individual class members who claim they suffered additional non-pecuniary damages over and above that award will be able to advance that claim in a future process to deal with individual issues.

[52] I agree with the plaintiffs that a similar process would be appropriate in this case.

[53] The catchall "or other monetary relief or compensation" is simply too vague.

Proposed Common Issue 8: "Miscellaneous" - Vicarious Liability

[54] Under the heading "miscellaneous", proposed common issue 8 asks "Is the Defendant vicariously liable for the acts and/or omissions of its operating companies, subsidiaries, partners, and their respective directors, officers, employees and agents?"

[55] There is no basis in fact for this issue. The record discloses no evidence that supports vicarious liability or collapsing the separate corporate existence of TransLink and its operating subsidiaries. The Data Breach involved the unlawful access of various folders and files by unknown cybercriminals. This is distinguishable from *Ari,* which involved an employee of the defendant unlawfully accessing class members' personal information deliberately during the course of her employment. To the extent that the plaintiffs rely on Ms. Johnston's evidence that cybercriminals were able to breach TransLink's network security after a phishing email was opened by one of TransLink's operating subsidiaries' employees, such evidence does not provide some basis in fact for a common issue regarding vicarious liability on the part of TransLink. The claim as framed is in direct liability, not vicarious liability, and the common issues must be rationally connected to the pleadings.

[56] There is no basis in fact for vicarious liability.

***CPA* s. 4(1)(d): Preferable Procedure**

[57] Section 4(2) of the *CPA* provides as follows:

> (2) In determining whether a class proceeding would be the preferable procedure for the fair and efficient resolution of the common issues, the court must consider all relevant matters including the following:
>
> > (a) whether questions of fact or law common to the members of the class predominate over any questions affecting only individual members;
> >
> > (b) whether a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate actions;
> >
> > (c) whether the class proceeding would involve claims that are or have been the subject of any other proceedings;

> (d) whether other means of resolving the claims are less practical or less efficient;
>
> (e) whether the administration of the class proceeding would create greater difficulties than those likely to be experienced if relief were sought by other means.

[58] The preferability analysis involves a comparative consideration of the proposed class proceeding against the other available means of resolving the proposed common issues: *Jiang v. Vancouver City Savings Credit Union*, 2019 BCCA 149 at para. 47 [*Jiang 2019 BCCA*].

[59] In *Campbell*, the Court noted:

> [170] The preferability analysis asks whether, in the context of the action as a whole, a class action proceeding is a better way of resolving the common issues than another type of proceeding in light of the goals of access to justice, judicial economy and behaviour modification: *AIC Limited v. Fischer*, 2013 SCC 69 at para. 19.

[60] The determination of the proposed common issues, save for the proposed common issue 7, requires no individual inquiries. As for the proposed common issue 7 itself, the determination of it would only partially require individual inquiries. As such, the common questions overwhelmingly dominate over individual inquiries.

[61] There is no indication that a significant number of the members of the class have a valid interest in individually controlling the prosecution of separate actions.

[62] Similar class proceedings have been certified in British Columbia and elsewhere, which indicates that where causes of action are properly pleaded and there are predominant common issues, a class proceeding is indeed preferable for the resolution of those common issues. Privacy class proceedings have been found to "meet the goals that animate class proceedings," including access to justice, judicial economy and behaviour modification: *Sweet* at paras. 186-188.

[63] The defendant argues that even if some general baseline damages could be assessed on a class-wide basis for a violation of privacy, some courts have found that certification of a class proceeding is not the preferable procedure where the

possible common damages are negligible, *de minimus*, or nominal, as such actions do not promote judicial economy and access to justice, particularly where other claims for compensatory damages are left for individual resolution*: Chow v. Facebook, Inc.*, 2022 BCSC 137, at paras. 97, 101-103; *Setoguchi v. Uber B.V.*, 2023 ABCA 45 at paras. 58, 71, and 73.

[64] Even if the defendant is correct that the only damages that are at issue in the within case would be nominal damages, that fact is not in itself an obstacle to certification. As noted in *Donegani v. Facebook*, 2025 ONSC 6020 at para. 40, British Columbia law recognizes the availability of nominal damages in the privacy law context. The Court in *Donegani* went on to find that the adequacy of nominal damages ought not be considered at the certification stage: at para. 53. However, unlike in *Donegani*, nominal damages in the present case are not woven into individual inquiries, as the Class Members have already been identified.

[65] In *Donegani*, the determination of class membership and privacy violations depended on a seemingly indeterminate inquiry into the behaviours of numerous third-party apps and millions of users' activities over nearly two decades. However, the alleged liability in the within case arises from the single event of the data breach. The issues around the event of the data breach and the defendant's alleged breaches of its duties can be answered efficiently, and it would advance the claim of all Class Members in a manageable way. There is also no evidentiary limitation or gap in this case. The defendant has completed an investigation into the data breach. It has identified the evidence with precision, including the "actual files" containing the Class Members' sensitive personal information and the personal information that may have been accessed in the Data Breach. The defendant's evidence is unequivocal that its investigation has been complete and thorough; and the defendant sent notification letters to all individuals whose sensitive personal information was identified as having been accessed by the cyberattackers.

[66] In *Donegani*, the Ontario Court determined that regulatory proceedings were preferable to advance behaviour modification given the absence of consequential

damages, as well as structural defects in the design of the class definition that hindered the determination of nominal damages as a common issue. In the within case, conversely, the regulatory investigation did not address the status of TransLink's operations at the time of the breach or the impact of the breach on the Class Members. Further, the defendant has undertaken to not rely on anything in the affidavit of its affiant Ms. Johnston, including that the regulator carried out an investigation, to argue that there is no basis that the defendant violated s. 30 of *FIPPA*.

[67] The defendant submits that a class proceeding is not the preferable procedure because it offered a two-year complimentary credit monitoring package with identity-theft protection up to $50,000 as part of its response to the Data Breach. The defendant further submits that to the extent that there is any cause of action, the offered credit monitoring package is preferable to the class proceeding: it provides benefits to class members, with no requirement that they prove any actual violation of their privacy or any existing loss, and offers to makes them whole if any claim could be established, under the parameters of the insurance coverage. However, credit monitoring is not necessarily the same as nominal damages, and I do not find that an individual insurance claim process is preferable to individual claims within a class proceeding.

[68] The defendant also submits that any concerns related to the goal of behaviour modification have been achieved with these efforts: *Cole v. FCA Canada Inc*., 2022 ONSC 5575, at paras. 153-170. However, the evidence of Dr. Cavoukian provides some basis in fact that recognizing and awarding remedies which address the harm to data breach victims would likely result in data custodians improving their overall security practices in order to better protect personal information. Credit monitoring and identity theft insurance have now been a go-to remedy offered by custodians for many years now. The fact that the data breach occurred can be taken as some basis in fact to indicate that behaviour modifications are warranted.

[69] In the circumstances I find that a class proceeding is the preferable procedure for a fair and efficient resolution of the common issues.

CPA s. 4(1)(e): Proposed Representative Plaintiffs

[70] The plaintiffs have each filed evidence stating that they understand their role as a proposed representative plaintiff, are able and willing to represent the other putative Class Members, and do not have any conflicting interests with the interests of the other putative Class Members.

[71] The plaintiffs' updated proposed litigation plan contains the information made available by the defendant regarding the composition of the class, as well as further particulars regarding the determination of class-wide and individual damages.

[72] The only claim advanced in this action is s. 1 of the *Privacy Act*. There is no individual inquiry to establish liability, which revolves around the defendant's conduct. Nor is there any individual issue in order to establish class-wide damages that requires proof of no harm or damage.

[73] While there may be individual issues to establish certain types of individual harms, that process will be established once the parties learn of the issues to be addressed, which is consistent with the plan in *Ari 2022 BCSC* at paras. 78-86 and consistent with s. 27-28 of the *CPA*.

[74] In *Jiang 2019 BCCA at para. 57*, the Court of Appeal held:

> The purpose of the plan is to provide a framework for the class proceeding that shows that the representative plaintiff and class counsel understand the complexities of the case. It is not to resolve all procedural issues before certification has taken place.

[75] The plaintiffs' updated proposed litigation plan meets that standard.

Conclusion

[76] The plaintiffs’ action is certified as a class proceeding.

[77] The claim in vicarious liability is not certified as is the claim in restitutionary, damages.

[78] The plaintiffs' proposed alternative class definition set out at para. 20 of these reasons is approved.

[79] Common issues 1-3 and 5, 6, and 8 are approved.

[80] Common issues 4 and 7 are approved excluding references to restitutionary and moral damages and other monetary relief or compensation.

[81] Common issue 9 is not approved.

[82] The representative plaintiffs are approved.

[83] The litigation plan is approved.

"Wilkinson J."