



Our File No.: CMBC/CASE/21-0083

February 22, 2021

Via Email: cheryl.shizgal@coastmountainbus.com

Cheryl Shizgal
Director, Corporate Services
Coast Mountain Bus Company
6th Floor – 13401 108th Avenue
Surrey, BC V3T 5T4

Dear Cheryl:

Re: Policy Grievance – Cyberattack and Privacy breach of Personal Data

This letter is further to the e-mail that was communicated with the MoveUP membership at Coast Mountain Bus Company (“CMBC”) on February 9, 2021. In the e-mail you confirm that TransLink has concluded that the personal information of current MoveUP members, retirees and spouses has been comprised to hackers.

The union is raising a policy grievance, pursuant to article 3.02 of the Collective Agreement.

The union alleges that the employer has violated the *Freedom of Information and Protection of Privacy Act* (“*FIPPA*”). In particular the union alleges that the employer has violated Part 3- Protection of Privacy & Division 1- Collection, Protection and Retention of Personal Information by Public Bodies.

Protection of personal information

30 A public body 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.

While this is an evolving section of law, there is a lot of discourse with the right to privacy of employees:

MoveUPTogether.ca

In a Court of Appeal decision, *Cash Converters Canada Inc. (dba Oshawa City)*, (supra) where at para. 29 the Court said this:

The right to privacy of personal information is interpreted in the context of the history of privacy legislation in Canada and of the treatment of that right by the Courts. The Supreme Court of Canada has characterized the Privacy legislation as quasi constitutional because of the critical role that privacy plays in the preservation of a free and democratic society. In Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002 SCC 53 \(CanLII\)](#), [2002] 2 S.C.R. 773, Gonthier, J. observed that exceptions from the rights set out in the Act should be interpreted narrowly, with any doubt resolved in favour of preserving the right and with the burden of persuasion on the person asserting the exception (at paras. 30 – 31). In Dagg v. Canada (Minister of Finance), (1997) [1997 CanLII 358 \(SCC\)](#), 2 S.C.R. 403, the Court articulated the governing principals of privacy law including the protection of privacy as a fundamental value in modern democracies and as enshrined in ss. 7 and 8 of the Charter, and privacy rights are to be compromised only where there is a compelling state interest in doing so (at para 65, 66, 71). In H.J. Heinz of Canada Ltd. v. Canada (Attorney General), [2006 SCC 13 \(CanLII\)](#), [2006] 1 S.C.R. 441 Deschamps, J. stated:

“In a situation involving personal information about an individual, the right to privacy is paramount ... (at para 26)”


*Today there is no question that the individual’s interest in personal privacy is the most pressing of the justifications advanced. That interest has been recognized by this Court as having constitutional significance. The foregoing approach is altogether fitting for a constitutional document enshrined at the time when, Westin tells us, society has come to realize that privacy is at the heart of liberty in a modern state; see Alan F. Westin, *Privacy and Freedom* (1970), pp. 349-50. Grounded in man’s physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. However that may be, there can be no doubt that in this modern age, it ranks high in the hierarchy of values meriting protection in a free and democratic society.*

When our members start employment with CMBC they place faith in the employer to keep their personal information safely stored. The employer has eroded the trust our members have with the information technology infrastructure at CMBC. The information technology breach gives rise to identity theft which can cause serious financial harm to our members. The union is prepared to advance this matter to arbitration in order to seek damages from the employer.

As a remedy, the union is seeking the employer provide all members, retirees and spouses lifelong credit monitoring through Trans Union and Equifax. In addition, the identify theft insurance maximum be increased from \$50,000 to \$500,000 per each employee/retiree. Furthermore, we ask the employer to immediately strike a working group committee with the union to address concerns we are hearing from our members and to discuss the necessary safeguards the employer has in place to ensure an event like this doesn’t transpire again.

Please advise when you are in position to discuss this issue with the union, respective of the timelines in article 3.02.

In Solidarity,

A handwritten signature in black ink, appearing to be 'PS', written in a cursive style.

Parm Sandhar, Union Representative

/LJ:USW2009

cc: Kevin Smyth, Senior Union Representative
Christy Slusarenko, Vice-President of Combined Units
Andrew Cheverie, Executive Councillor
Brendon Faustin, Executive Councillor
Sean Gosse, Executive Councillor
Vivian Ho, Executive Councillor