S-223955

ACTION NO.
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

TANIS SEMINOFF

PLAINTIFF

AND:

HER MAJESTY THE QUEEN

DEFENDANT

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

NOTICE OF CIVIL CLAIM

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: STATEMENT OF FACTS

Nature of the Action

1. This action concerns the unauthorized disclosure to a third party of the personal and financial information of thousands of Canadians from their online accounts with the Canada Revenue Agency ("CRA"), My Service Canada, and other Government of Canada online accounts where those accounts are accessed using the Government of Canada Branded Credential Service ("GCKey").

2. The information was disclosed to a third party during several unauthorized data breaches targeting the GCKey credential management service and targeting CRA accounts and My Service Canada accounts - and the personal and financial information included in those accounts. The Defendant was aware of cyber security concerns with these accounts and with GCKey and with its databases and online systems generally, and was aware of vulnerabilities in its security software, all of which put at risk the personal and financial information of the Plaintiff and other Class Members. Despite these concerns and vulnerabilities, the Defendant failed to take timely and reasonable steps and precautions to prevent harm to the Plaintiff and other Class Members.

3. The Defendant's own cyber security guidance acknowledges that the burden of password protection falls on the system, not the user. The Defendant should have followed its own cyber security guidance regarding passwords. The Defendant also should have offered a non-vulnerable security question mechanism for users of online CRA accounts and My Service Canada accounts and the GCKey credential management system and should have responded in a reasonable and timely manner to significant increases in failed login attempts to these accounts and to the GCKey credential management system. And the Defendant should have followed industry norms regarding two-factor authentication for these accounts.

4. As a result of the unauthorized data breaches, the personal and financial information of the Plaintiff and other Class Members - including their social insurance numbers ("SIN"), annual tax returns, notices of assessment, banking records and account information, financial records and salary information, T4s, T5s, family information, disability benefit information, immigration status, home addresses, and other inherently revealing and private information - was disclosed

to a third party without their consent.

5. The Plaintiff and other Class Members have had their privacy deeply invaded, and are distressed and fearful of the uses that may be made of their confidential personal and financial information by the third party. The Plaintiff and other Class Members have already spent numerous hours notifying the CRA, Service Canada, credit bureaus, banks, and other appropriate companies and agencies about the issue and will require credit monitoring services for the rest of their lives. Many Class Members have also suffered other damages including, *inter alia*: identity theft; monies being withdrawn from their bank accounts without their consent; loans being applied for (and taken out) in their names without their consent; Canada Emergency Response Benefits ("CERB"), Canada Emergency Student Benefits ("CESB"), Employment Insurance payments, Canada Child Benefits, Canada Pension Plan payments, and other benefits being redirected to bank accounts or addresses that do not belong to Class Members and losses that flow directly from Class Members not having access to these monies.

The Parties

6. The Plaintiff, Tanis Seminoff, is a resident of 901 Shearwater Street in Esquimalt, British Columbia with an address for service c/o Rice Harbut Elliott LLP, 820 – 980 Howe Street, Vancouver, British Columbia, V6Z 0C8.

7. The Defendant, Her Majesty the Queen (the "Crown"), is named as a representative of the Federal Government of Canada and is liable for the conduct, negligence and malfeasance of the CRA, Service Canada, Employment and Social Development Canada, and other individuals and agencies who were at all material times Crown employees, agents and servants, pursuant to the *Crown Liability and Proceedings Act*, RSC 1985, c. C-50.

8. The Class is defined as:

> All persons whose personal or financial information in their Government of Canada Online Account was disclosed to a third party without authorization on or after March 1, 2020 and who contacted Murphy Battista LLP about the CRA privacy breach class action, with Federal Court file number T-982-20, prior to June 24, 2021.
>
> "Government of Canada Online Account" means:
>
> a. a Canada Revenue Agency account;
> b. a My Service Canada account; or

c. another Government of Canada online account, where that account is accessed using the Government of Canada Branded Credential Service (GCKey).

(collectively "Class" or "Class Members").

Background

9. On or around March 15, 2020, the Defendant began providing eligible employed and self-employed Canadians directly affected by COVID-19 with CERB, a benefit that provided financial support to eligible applicants in the amount of $2,000 for a four week period.

10. On or around May 10, 2020, the Defendant began providing eligible Canadian post-secondary students, and recent post-secondary and high school graduates who were unable to find work due to COVID-19, with CESB, a benefit that provided financial support to eligible applicants in the amount of $1,250-$2,000 for a four week period.

11. With both the CERB and CESB programs, if a person required benefits beyond the initial four week period, they were required to re-apply for the CERB or CESB program.

12. The timing of the first unauthorized data breach correlated to the Crown's introduction of the CERB program in or around early March 2020 and the unauthorized data breaches continued throughout the period that the CERB and CESB programs were being offered by the defendant and even after these programs ended.

13. The Plaintiff and Class Members used unique usernames and passwords for their CRA, Service Canada, and GCKey accounts; they did not use usernames or passwords for these accounts that they used to log in to other online accounts in their names.

14. The online application system for the CERB and CESB programs was implemented hastily and recklessly by the Defendant and without taking the necessary precautions to ensure that the Plaintiff's and Class Members' inherently private personal and financial information included in their CRA accounts, My Service accounts, and other Government of Canada online account, where those accounts are accessed using the GCKey credential management system, was not compromised.

15. The Defendant knew, or ought to have known, that its databases and online systems and the Plaintiff's and Class Members' CRA accounts, Service Canada accounts, and other online Government of Canada accounts accessed using the GCKey credential management system

were vulnerable to unauthorized data breaches, and the Defendant failed to take timely, reasonable and adequate measures to protect the Plaintiff's and Class Members' personal and financial information both before and after launching the online CERB and CESB programs. The Defendant should have followed its own cyber security guidance regarding passwords, should have offered a non-vulnerable security question mechanism for users of CRA and My Service Canada accounts and the GCKey credential management system, and should have followed industry norms regarding two-factor authentication for these accounts.

16. All of the Defendant's duties *vis-à-vis* the Plaintiff and other Class Members were non-delegable.

17. As a consequence of the Defendant's conduct, the personal and financial information of the Plaintiff and other Class Members was disclosed to a third party following a series of unauthorized data breaches between approximately March 1, 2020 and at least the fall or winter of 2020 and may be ongoing into 2021 and beyond.

18. The CRA was aware that there was an increase in fraudulent activity at the beginning of each monthly CERB and CESB pay period and generally during the time period at issue but did nothing to notify or warn the Plaintiff or other Class Members of same in a timely manner or at all, and did nothing to reasonably prevent further unauthorized data breaches from occurring. Some Class Members have still not been notified by the Defendant, or any employees, agents, or servants of the Defendant, that their accounts were affected by the unauthorized data breaches and that their confidential information was compromised.

19. The CRA disclosed to CBC News, days prior to publicly announcing the unauthorized data breaches, that the CRA was aware that there was an uptick in fraudulent activity at the beginning of each monthly CERB pay period.

20. As a result of the unauthorized data breaches, the online Government of Canada accounts of thousands of Class Members – accessed using the GCKey credential management system – were compromised. Used by approximately 30 federal departments, GCKey allows Class Members to access services such as Employment and Social Development Canada's My Service Canada Account or their Immigration, Refugees and Citizenship Canada account. These accounts contain detailed personal and financial information, including personal and financial details related to Employment Insurance, immigration status, Canada Pension Plan, Canada Pension Plan Disability, and Old Age Security. The Defendant is aware that the Government of Canada accounts of at least 9,300 GCKey service users were accessed and the personal and financial information included in them disclosed to an external third party. The

Plaintiff and other Class Members did not provide their consent to the disclosure of their personal and financial information.

21. The My Service Canada accounts of thousands of Class Members were compromised by the unauthorized data breaches, during which the personal and financial information of Class Members was disclosed to an external third party. The Class Members did not provide their consent to such disclosure. My Service Canada accounts contain sensitive personal and financial information of Class Members, including information on Employment Insurance, Canada Pension Plan payments, Canada Pension Plan Disability payments, and Old Age Security payments. My Service Canada accounts also contain an e-link, which enables a user to link directly from their My Service Canada account to their CRA account without the need to sign in to their CRA account directly.

22. The CRA accounts of thousands of Class Members were also compromised by the unauthorized data breaches, during which the personal and financial information of the Plaintiff and other Class Members was disclosed to an external third party. The Plaintiff and other Class Members did not provide their consent to such disclosure. CRA accounts contain sensitive personal and financial information of Class Members, including financial records, notices of assessments, banking information, and information on income, disabilities, children, relationship status, and investments. The Defendant is aware of at least 48,500 CRA accounts having been compromised during the data breaches.

23. The Defendant has admitted that its security software was susceptible and vulnerable to the unauthorized data breaches and that it knew about vulnerabilities to the Plaintiff's and other Class Members' online accounts prior to the data breaches taking place.

24. Annette Butikofer, the chief information officer at the CRA, said during a news conference on August 17, 2020 that it was a "vulnerability in security software, which allowed [the third party] to bypass security questions and gain access" to Class Members' accounts.

25. Also on August 17, 2020, Marc Brouillard, the acting Chief Technology Officer for the Crown said that the third party was "also able to exploit a vulnerability in the configuration of security software solutions, which allowed them to bypass the CRA security questions and gain access to a user's CRA account".

26. Some Class Members alerted the CRA to the unauthorized data breaches and security vulnerabilities as early as March of 2020, yet the CRA failed to take timely and reasonable steps to prevent further harm to the Plaintiff and other Class Members.

27. As early as April 2020, some Class Members were notified by their service providers - such as accounting firms or investment firms - about the unauthorized data breaches and their potential ramifications. Some of these service providers alerted the CRA about the unauthorized data breaches and security vulnerabilities, yet the CRA failed to take timely and reasonable steps to prevent further harm to the Plaintiff and other Class Members.

28. The Defendant failed to have in place a mechanism for reasonably and effectively managing and addressing reports of unauthorized data breaches of the CRA, Employment and Social Development Canada, and My Service Canada, and other Government of Canada departments and agencies. Reports of unauthorized data breaches were routinely and recklessly ignored by the Defendant.

29. The CRA failed to notify the Privacy Commissioner of Canada, in a timely manner, that the personal and financial information of the Plaintiff and other Class Members had been compromised and was at risk of being further compromised.

30. The CRA failed to notify the Plaintiff, other Class Members, and the Canadian public, in a timely manner or at all, that the personal and financial information of the Plaintiff and other Class Members had been compromised and was at risk of being further compromised. No such disclosure was made public until on or around August 15, 2020. Even then, the Defendant failed to lock the GCKey, CRA, and My Service Canada online account systems to prevent further harm to the Plaintiff and other Class Members.

31. After announcing the unauthorized data breaches on or around August 15, 2020, an additional unauthorized data breach or breaches took place, further compromising the personal and financial information of the plaintiff and other Class Members. It was then that the defendant finally locked the GCKey credential management system and the CRA, and My Service Canada online account systems.

32. To date, the Defendant has been unable to determine who is in possession of the personal and financial information of the Plaintiff and other Class Members.

33. To date, the Defendant has been unable to provide the Plaintiff and other Class Members with any details regarding their identity theft and how their inherently revealing and private personal and financial information has been accessed, disseminated, copied, published, shared, or used, by whom, and for what purpose.

34. The Defendant's unauthorized disclosure to a third party of the confidential personal and financial information of the Plaintiff and other Class Members (which was communicated to

Canada in confidence for the purpose of being included in Class Members' CRA accounts, My Service Canada accounts, and other Government of Canada online accounts that were accessed using the GCKey credential management system), was intentional and reckless and without lawful justification. The information was misused by Canada, to the detriment of the Plaintiff and other Class Members. And its unauthorized disclosure by the Defendant to a third party invaded the private affairs and concerns of the Plaintiff and other Class Members. The information disclosed was inherently revealing and private, and its disclosure was offensive and caused distress, humiliation, and anguish to the Plaintiff and other Class Members.

35. As a result of the unauthorized data breaches, the Plaintiff and other Class Members have spent numerous hours notifying the CRA, Service Canada, credit bureaus, and other appropriate companies and agencies about the issue and will indefinitely require credit monitoring services.

36. As a result of the unauthorized data breaches, the Plaintiff and other Class Members have had their privacy deeply invaded, and are mentally distressed about and fearful of the uses that may be made of their personal and financial information by a third party.

37. As a result of the unauthorized data breaches, the disclosed personal and financial information of Class Members has already been used by a third party or parties to, *inter alia*:

a. steal the identity of Class Members;
b. fraudulently apply for CERB, CESB, and other government benefits in the name of Class Members;
c. fraudulently redirect CERB, CESB, Employment Insurance payments, Canada Pension Plan payments and other government benefits away from Class Members;
d. fraudulently gain access to Class Members' bank accounts to withdraw money;
e. fraudulently gain access to Class Members' credit cards to make purchases;
f. fraudulently apply for loans in the names of Class Members; and
g. damage the credit reputation of Class Members.

38. The Defendant has advised some Class Members that they would pay for credit monitoring, but this "credit monitoring" solely involves flagging the credit accounts of Class Members, a service that is already offered free of charge by credit monitors in Canada.

39. The Plaintiff and Class Members seek, *inter alia*, general damages for the Defendant's several liability, special damages, and punitive damages.

The Plaintiff

40. The Plaintiff, Tanis Seminoff, was assigned a SIN at a young age and has filed income tax returns for decades. She never applied for or received CERB.

41. The Plaintiff had an online account with CRA MyAccount, having created a credential at a time that is presently unknown to her.

42. The Plaintiff signed up for and used the CRA MyAccount, to the mutual benefit of herself and the Defendant, the latter gaining benefit by automating functions that otherwise would require increased staffing and expense.

43. The Plaintiff used the CRA MyAccount, expecting that the Defendant's security protocols would be designed and operated appropriately, in order to keep her personal and financial information secure.

44. The Plaintiff accessed her CRA MyAccount through the credential management system ("CMS") credential she created.

45. Due to the operational failures of the Defendant described herein, the Plaintiff's account was breached on a date prior to August 20, 2020 and the bad actor was able to successfully apply for the CERB.

46. The Plaintiff first learned that her CRA MyAccount had been breached when she received a letter from the CRA, dated August 20, 2020, advising her of the same. It was not until a phone call on December 17, 2020 that Ms. Seminoff specifically learned that an unauthorized actor had applied for CERB on her account and changed the direct deposit information such that payments were routed to the unknown actor's desired account. These steps were undergone without Ms. Seminoff's consent.

47. As a result of the above-mentioned breach, an unauthorized actor received $4,000 in CERB benefits.

48. Ms. Seminoff subsequently reinstated her direct deposit information and opted not to regain access to her CRA MyAccount. She is not interested in using this platform again.

49. In early 2021, the plaintiff received a letter from the CRA indicating that she was being taxed for the $4,000 in CERB payments that she had never applied for and had never received.

50. The Plaintiff first contacted Murphy Battista LLP about this proposed class proceeding on

April 22, 2021.

51. As a consequence of the unauthorized data breach, Ms. Seminoff has suffered from anxiety, stress, and mental distress. She is concerned that her personal and financial information disclosed in the CRA breach will be used inappropriately in the future by bad actors, to her detriment. She is also deeply concerned about the potential ramifications to her credit, and will require credit monitoring services for the rest of her life.

52. As a result of the breach to her CRA account and learning that the personal and financial information in her account had been compromised and disclosed to a bad actor without her consent, the Plaintiff spent at least 20 hours gathering information, filling out forms, and contacting different agencies to deal with the account breach and to protect her identity and to prevent further harm.

Part 2: RELIEF SOUGHT

53. The Plaintiff, claims on her own behalf and on behalf of the proposed Class (as defined above):

a. an order certifying this action as a class proceeding and appointing Tanis Seminoff as representative Plaintiff for the Class;

b. an order that the Defendant fund appropriate credit monitoring services for the Plaintiff and all Class Members;

c. general damages for the Defendant's several liability plus damages equal to the costs of administering the plan of distribution;

d. damages for the Defendant's several liability for time lost while communicating with the Canada Revenue Agency, Service Canada and other government agencies and while in engaging in precautionary communications with third parties to inform them about the unauthorized disclosure of the Plaintiff's and other Class Members' personal and financial information;

e. special damages in an amount to be determined, including but not limited to Canada Emergency Response Benefits, Canada Emergency Student Benefits, and other benefits owed, costs incurred in preventing identity theft, including costs incurred for the purpose of credit monitoring, and other out-of-pocket expenses;

f. punitive damages;

g. pre- and post-judgement interest;

h. costs; and

i. such further and other relief as this Honourable Court deems just.

Part 3: LEGAL BASIS

Systemic Negligence

54. The Defendant owed a common law duty to the Plaintiff and other Class Members to use reasonable care in the collection, storage, and retention of their personal and financial information and a duty to ensure that this personal and financial information was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party. The Defendant's duties were not delegable.

55. Pursuant to section 8(1) of the *Privacy Act*, RSC 1985, c P-21, personal information under the control of the Defendant cannot, without the consent of the individual to whom the information relates, be disclosed by the Defendant. The Defendant's breach of the *Privacy Act* is evidence that its conduct fell below the applicable standard of care.

56. Particulars of the Defendant's systemic breaches of duty, as set out in the whole of this claim, include:

a. failing to create or adhere to policies for the collection, storage, retention, and disclosure of personal and financial information prior to instituting the CERB and CESB programs;

b. failing to adhere to its own policies to ensure protection of the Plaintiff and other Class Members in the collection, retention and disclosure of their personal and financial information;

c. failing to take reasonable steps to ensure that the personal and financial information of the Plaintiff and other Class Members was kept safe, private, and protected was not retrieved, disseminated, or disclosed without the consent of the Plaintiff and other Class Members;

d. disclosing to a third party the personal and financial information of the Plaintiff and other Class Members without their consent;

e. failing to follow its own cyber security guidance regarding passwords;

f. failing to have offered a non-vulnerable security question mechanism for users of the GCKey credential management system and for users of CRA and My Service Canada online accounts;

g. failing to have followed industry norms regarding two-factor authentication for these accounts;

h. failing to take reasonable steps, including freezing the online systems, when there was a significant increase in the number of failed attempts for CRA accounts, My Service Canada accounts, and/or the GCKey credential management system;

i. failing to take reasonable steps, including freezing the online systems, when they knew or ought to have known that unauthorized data breaches were compromising the personal and financial information of the Plaintiff and other Class Members;

j. failing to act on reported concerns communicated by the Plaintiff and other Class Members about the unauthorized data breaches in a timely manner or at all;

k. failing to act on reported concerns communicated by financial institutions, accounting firms, or other institutions about the unauthorized data breaches in a timely manner or at all;

l. failing to take timely and reasonable steps that were required to ensure the integrity and security of its databases and online systems and to prevent unauthorized access to the personal and financial information of the Plaintiff and other Class Members;

m. failing to take timely and reasonable steps to ensure the application process for CERB and CESB programs did not compromise the security, safety, or privacy of the Plaintiff's and other Class Members' personal and financial information;

n. failing to disclose the unauthorized disclosure of the Plaintiff's and other Class Members' personal and financial information to its own security personnel and to the Plaintiff and other Class Members in a timely manner or at all;

o. failing to rectify the vulnerabilities in the configuration of its security software in a timely manner or at all when it knew or ought to have known about the vulnerabilities;

p. failing to provide adequate or any instructions to the plaintiffs and other Class

Members on how to mitigate their damages, including failing to provide adequate paid credit monitoring services to the Plaintiff and other Class Members;

q. failing to disclose the unauthorized data breaches and the unauthorized disclosure of the personal and financial information of the Plaintiff and other Class Members occurring at the start of each CERB and CESB monthly payment cycle or otherwise to the Plaintiff and other Class Members in a timely manner or at all; and

r. other particulars as counsel may advise.

57. Measures and steps finally taken by the Defendant in the fall and winter of 2020 to protect its databases, systems, and online CRA accounts, online My Service Canada accounts, and other Government of Canada online accounts – accessed using the GCKey credential management system – of the Plaintiff and other Class Members are all measures and steps that should have been taken by the Defendant prior to the unauthorized data breaches and, had they been taken, the unauthorized breaches in question would have been prevented.

58. The Defendant's breaches of duty caused the Plaintiff and other Class Members harm and ongoing damages, including distress, anxiety, mental anguish, lost time, lost opportunities, and out of pocket expenses.

Breach of Confidence

59. The personal and financial information of the Plaintiff and other Class Members - which was included in their CRA accounts, their My Service accounts, and other Government of Canada online accounts accessed using the GCKey credential management system – was confidential and was communicated to the Defendant in confidence. That information was misused by the Defendant, to the detriment of the Plaintiff and other Class Members, and constituted the tort of breach of confidence.

Intrusion upon Seclusion

60. The Defendant's unauthorized disclosure to a third party of the Plaintiff's and other Class Members' personal and financial information was intentional and reckless and, without lawful justification, invaded the private affairs and concerns of the Plaintiff and other Class Members. The information disclosed was inherently revealing and private, and a reasonable person would regard this invasion as highly offensive causing distress, humiliation, or anguish. The Defendant's conduct constituted the tort of intrusion upon seclusion.

61. Class Members and their agents reported unauthorized data breaches of their CRA

accounts, My Service Canada accounts, and other Government of Canada online accounts accessed using the GCKey credential management system, and their personal and financial information included in those accounts, to the Defendant in the spring of 2020, and the Defendant intentionally and recklessly and without lawful justification disregarded this information and failed to take reasonable and timely steps to protect the Plaintiff and other Class Members from further unauthorized data breaches.

Crown Liability and Proceedings Act

62. The acts, omissions, torts, and faults of the Defendant, as set out in detail in the whole of this claim, were also committed by servants of the Crown. Where the tort was committed by a servant of the Crown or where, in Quebec, damage was caused by the fault of a servant of the Crown, the Crown is liable for the damages for which, if it were a person, it would be liable, pursuant to section 3 of the *Crown Liability and Proceedings Act*, RSC 1985, c C-50.

Damages

63. As a result of the Defendant's negligence, breach of privacy, breach of confidence, and reckless intrusion upon seclusion, the Plaintiff and other Class Members have suffered damages including:

a. costs incurred in preventing identity theft;

b. identity theft;

c. increased risk of future identity theft;

d. damage to credit reputation;

e. mental distress, stress, anxiety, humiliation, and anguish;

f. monies withdrawn from their bank accounts without their consent;

g. loans applied for in their names without their consent;

h. credit card fraud;

i. inability to access the benefit funds and payments they were entitled to and financial and other losses flowing directly from their inability to access these benefits and payments;

j. the loss of employment insurance, Canada Pension Plan payments, Canada Child Benefits, and other benefits or payments they were entitled to that were redirected to bank accounts or addresses that do not belong to them, and other losses flowing directly from their inability to access these benefits and payments;

k. out-of-pocket expenses;

l. time lost waiting on hold for and speaking with the CRA, Service Canada, Employment and Social Development Canada, and other Crown agencies, departments, servants, and individuals to address the unauthorized data breaches and to mitigate their damages; and

m. time lost in precautionary communications with third parties such as credit card companies, credit agencies, creditors, utility providers, and other parties, to inform them of the potential that their personal and financial information may have been compromised.

64. The Plaintiff and Class Members seek, *inter alia*, general damages for the Defendant's several liability and special damages.

65. As set out in detail in this claim, the actions of the Defendant were reprehensible and showed a callous disregard for the rights of the Plaintiff and other Class Members. The conduct of the Defendant was deliberate and represented a marked departure from ordinary standards of decent behavior, and as such merits punishment and warrants a claim for punitive damages.

Relevant Legislation

66. The Plaintiff pleads and relies on, *inter alia*, the following statutes:

a. *Crown Liability and Proceedings Act*, RSC 1985, c C-50;

b. *Interpretation Act*, RSC 1985, c I-21;

c. *Privacy Act*, RSC 1985, c P-21; and

d. their predecessor and successor statutes.

Form 11 (Rule 4-5 (2))

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The Plaintiff claims the right to serve this pleading/petition on the Defendant outside British Columbia on the ground that:

The Plaintiff has at all material times have been a resident of British Columbia and has suffered loss in British Columbia. The Supreme Court of British Columbia has jurisdiction with respect to this matter and the Plaintiff pleads the *Court Jurisdiction and Proceedings Transfer Act*, 2003, SBC Chapter 28 and amendments thereto.

Plaintiff's address for service:	**RICE HARBUT ELLIOTT LLP** Barristers and Solicitors 820 - 980 Howe Street Vancouver, BC V6Z 0C8
Fax number address for service (if any):	(604) 682-0587
E-mail address for service (if any):	Nil
Place of trial:	Vancouver
The address of the registry is:	800 Smithe Street, Vancouver

Date: 16/MAY/2022

Counsel for the Plaintiff,
Anthony Leoni
John M. Rice, Q.C.

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.

Appendix

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

A claim for negligence, failure to warn and, *inter alia*, breach of consumer protection legislation relating to generic prescription medications contaminated with a probable carcinogen, with injury, loss and damages to the Plaintiff and a class of similarly situated persons resident in Canada.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

a motor vehicle accident

medical malpractice

X another cause

A dispute concerning:

☐ contaminated sites

☐ construction defects

☐ real property (real estate)

☐ personal property

☐ the provision of goods or services or other general commercial matters

☐ investment losses

☐ the lending of money

☐ 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:
[*Check all boxes below that apply to this case*]

X a class action

☐ maritime law

☐ aboriginal law

☐ constitutional law

☐ conflict of laws

☐ none of the above

☐ do not know

Part 4:
[*If an enactment is being relied on, specify. Do not list more than 3 enactments.*]

1. *Class Proceedings Act*, R.S.B.C. 1996, c. 50
2. *Health Care Cost Recovery Act*, S.B.C. 2008, c. 27
3. *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2