No.
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

JOSHUA ELLIOTT TEMPLE

PLAINTIFF

AND:

EQUIFAX, INC. and EQUIFAX CANADA CO.

DEFENDANTS

Brought pursuant to the *Class Proceedings Act*, RSBC 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

The parties and their relationship

1. The Plaintiff is a businessman residing in Tofino, British Columbia.

2. The Defendant, Equifax, Inc. is a U.S. company with headquarters at 1550 Peachtree Street NW, Atlanta, Georgia. Equifax, Inc. operates in many different countries, including Canada, either directly or through entities it owns, controls or is otherwise affiliated with, including the Defendant Equifax Canada Co. ("Equifax Canada").

3. Equifax Canada is a company incorporated pursuant to the laws of Nova Scotia and extra-provincially registered in British Columbia, with a delivery address at 2700 – 700 West Georgia St. in Vancouver, British Columbia. Equifax Canada is owned and controlled by Equifax, Inc.

4. At all material times, Equifax, Inc. and Equifax Canada (collectively, "Equifax") carried on business as providers of fraud detection, credit reporting and credit monitoring services worldwide, including in British Columbia, as follows:

    a. Equifax provided credit report and credit score information about British Columbia residents to those persons, or to third parties in British Columbia or in other Canadian provinces or territories or abroad (the "Credit Reporting Services"); and

    b. Equifax sold credit monitoring and ID theft services to British Columbia residents (collectively the "Credit Monitoring Services").

5. In the course of providing its Credit Reporting Services and Credit Monitoring Services, Equifax accessed, received, collected, used and stored a vast amount of confidential personal information of British Columbia residents, including their name, date of birth, social security number, driver's license number, credit card numbers, income and other financial information (collectively, the "Personal Information"). Additionally, Equifax transferred or transmitted Personal Information of British Columbia residents to persons or corporations within British Columbia, in other Canadian provinces or territories or abroad.

6. Equifax's extensive access, receipt, collection, use, storage, transfer or transmission of Personal Information, as particularized herein, made it foreseeable to Equifax that its electronic databases are a prime target for criminal activity including attempts to hack and steal the Personal Information.

The Proposed Class

7. The Plaintiff brings this action on his own behalf and on behalf of a proposed class defined as: "all persons residing in British Columbia whose Personal Information was contained on electronic databases in the control of Equifax and which was compromised and/or accessed by others between March 8, 2017 and July 31, 2017" (collectively, the "**Class**" or the **"Class Members"**).

8. The Plaintiff also brings this action on behalf of a subclass, defined as "all Class Members who at any time between March 8, 2017 and July 31, 2017 were subscribers to one of Equifax's Credit Monitoring Services" (the "**Credit Monitoring Subclass**") and whose Personal Information was compromised and/or access by others.

Equifax's Privacy Policy

9. At all material times, Equifax Canada and Equifax, Inc. maintained a Privacy Policy that governed their access, receipt, collection, use, storage and transmission of Personal Information of Class Members ("Equifax's Privacy Policy").

10. Pursuant to Equifax's Privacy Policy, Equifax represented, among other things, as follows:

> Equifax Canada prides itself on being a trusted steward of personal information and we are committed to protecting the personal information under our control…
>
> …
>
> **Safeguarding your personal information**

> Equifax maintains strict security safeguards when storing or destroying your personal information in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. These standards are in place for all information, regardless of how it is stored and we regularly review, test and enhance our systems to ensure they meet accepted industry standards. We also limit the number of employees who may access your personal information on a need-to-know basis: this means that only employees who would need to discuss your information with you, generate a credit report or other related products or services, or conduct investigations to verify and correct your credit report, would have access to your personal information. We conduct due diligence on, and impose the same high standards that we implement internally for, our members who are permitted to access your information from us.
>
> In the event that we transfer your personal information to a third party in Canada or across borders for processing, we contractually require such third party to protect your personal information in a manner consistent with our privacy safeguarding measures, subject to the law in the third party jurisdiction.
>
> …

Equifax's Credit Monitoring Agreements

11. In order to subscribe to Equifax's Credit Monitoring Services, Credit Monitoring Subclass Members entered into standard form agreements (collectively, the Credit Monitoring Agreements").

12. While Equifax sold different types of Credit Monitoring Services, all those services and the corresponding Credit Monitoring Agreements included a common agreement to provide credit protection and fraud management, including "daily credit monitoring with email alerts to key changes to the customer's credit file".

13. The current cost of Equifax's Credit Monitoring Services ranges from $16.95 per month to $29.95 per month.

14. At all material times, it was an express or alternatively implied term of the Credit Monitoring Agreements that Equifax would abide by its Privacy Policy. In particular, it was an express or alternatively implied term of the Credit Monitoring Agreements that Equifax would maintain strict security safeguards to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information of the Credit Monitoring Subclass.

15. At all material times, it was an express or alternatively implied term of the Credit Monitoring Agreements that Equifax would provide accurate and timely reports to

Credit Monitoring Subclass Members about their credit information, and would immediately notify them if their Personal Information was stolen and disclosed on the Internet, or was the subject of unauthorized access, collection, use, disclosure, copying, modification or disposal, and that they would be provided with protection against fraud including identity theft.

The security breach and Equifax's failure to respond

16. At all material times, Equifax maintained an online disputes portal where consumers, including BC residents, could view and dispute information being reported on their credit reports (the "Disputes Portal").

17. On or about March 8, 2017, the US Department of Homeland Security, Computer Emergency Readiness Team ("US CERT") sent Equifax and others a notice informing them of the need to patch a vulnerability in certain versions of Apache Struts, a software used by Equifax in its Disputes Portal (the "Vulnerability Notice").

18. Equifax had an internal policy requiring that any necessary software patching occur within 48 hours.[1]

19. Although there were internal communications acknowledging the existence of the Vulnerability Notice and the need to upgrade Apache Struts, Equifax did not identify or patch the vulnerability. Further, Equifax allowed the Disputes Portal to remain accessible on the Internet while the vulnerability had yet to be patched.

20. On or about March 15, 2017, Equifax's information security department ran routine internal scans. While those scans were conducted at a time when it was known there were vulnerability issues, the scans were either not adequate or improperly conducted and failed to detect the vulnerability in Equifax's Disputes Portal. Again, the Disputes Portal remained accessible on the internet.

21. On or about July 29, 2017, Equifax's security department detected some suspicious network traffic in connection with the Disputes Portal. While Equifax's security department blocked the suspicious traffic, it nevertheless allowed the Disputes Portal to remain accessible on the Internet while the vulnerability had yet to be patched.

[1] This information comes from the opening remarks of Equifax's former CEO Richard Smith in testimony provided to US Congress on October 3, 2017, as reported on https://www.secureworldexpo.com/industry-news/day-by-day-timeline-of-equifax-breach

22. On July 30, 2017, Equifax's security department detected additional suspicious activity in connection with its Disputes Portal. It was only then that the Disputes Portal was taken offline. Equifax then initiated an investigation.

23. By August 11, 2017, the investigation team engaged by Equifax had determined that cybercriminals had access to dispute documents from the Disputes Portal, as well as a database table containing a large amount of Personal Information (the "Security Breach").

24. By August 15, 2017, Equifax knew that Personal Information of consumers had been stolen. However, Equifax did not publicly disclose this fact until September of 2017.

25. On September 7, 2017, Equifax issued a press release in the US indicating that criminals had exploited a vulnerability of a US website application to gain access to certain files from mid-May through July 2017, including "personal information for certain UK and Canadian residents"[2]. This press release was the first public notification that Personal Information kept by Equifax was compromised.

26. On the Form 10-Q that Equifax, Inc. filed with the U.S. Securities & Exchange Commission on November 9, 2017, Equifax, Inc. indicated that the Personal Information of Class Members that was accessed included names, social insurance numbers, birth dates, addresses, driver's license numbers and credit card numbers, as well as other identifying information contained in dispute documents. Equifax, Inc. also reported that "personal information of approximately 8,000 Canadian consumers was impacted".

27. Notwithstanding its knowledge that (a) the Disputes Portal had a vulnerability, and subsequently, that (b) criminals had exploited that vulnerability, Equifax did not promptly notify the persons whose Personal Information had been compromised, including the Plaintiff and the proposed Class Members.

28. Further, after July 1, 2017, Equifax had communications with persons who purchased Credit Monitoring Services, and whose Personal Information was later determined to have been compromised, but failed to provide timely notice of the security breach. On the contrary, and as exemplified by the Plaintiff's dealings with Equifax, as particularized below, Equifax provided ongoing assurances to its customers, including the Plaintiff and the proposed Credit Monitoring Subclass Members, that there were no critical developments to be reported, such as the access to and theft of their Personal Information.

[2] September 7, 2017 press release issued by Equifax, and available at https://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html

The Plaintiff's dealings with Equifax

29. On or about October 31, 2003, the Plaintiff enrolled in one of Equifax's Credit Monitoring Services, namely, Equifax's Complete Premier Plan. As was the case with all Credit Monitoring Services, the Complete Premier Plan's services included daily credit monitoring by Equifax and alerts of key changes, and other benefits. Every year thereafter, the Plaintiff renewed his subscription to Equifax's Complete Premier Plan, and paid an annual fee. In order to pay his annual fee, the Plaintiff provided his credit card information to Equifax.

30. As a subscriber to Equifax's Complete Premier Plan, the Plaintiff was entitled to receive and did receive certain periodic updates from Equifax reporting on the monitoring of the Plaintiff's credit file.

31. On September 1, 2017, the Plaintiff received an email from Equifax with the subject: "Equifax Complete (TM) Premier Plan – No News is Good News". The email went on to state as follows:

> Equifax has been monitoring your credit file and we are pleased to inform you that there were no critical events reported in the last month. In this case, no news is good news!
>
> What does "no news is good news" mean to you? This means key changes that could be indicators of fraud were not detected. If any key changes are reported in the future, we will notify you via e-mail.

32. On or about October 17, 2017, the Plaintiff received a letter from Equifax. The letter indicated that the Plaintiff's name, address, date of birth, telephone number, email address, username, password and secret question / secret answer had been "impacted" by the vulnerability of the Disputes Portal. The letter also incorrectly reported that "upon discovery" of the vulnerability of its Disputes Portal, "Equifax acted immediately to stop the intrusion, and the web application was taken offline and patched".

33. The Plaintiff, the Class Members and the Credit Monitoring Subclass Members have suffered damages as a result of the access to and theft of their Personal Information, particulars of which are set out in Part 3 below and incorporated in this Part 1 as a material fact.

34. The damages were caused by the statutory breaches, negligence, negligent misrepresentations and breaches of contract of Equifax, and Equifax has been unjustly enriched. Particulars are set out in Part 3 below and incorporated in this Part 1 as material fact.

Part 2: RELIEF SOUGHT

35. An order certifying this action as a class proceeding pursuant to the *Class Proceedings Act*, RSBC 1996, c 50;

36. An order appointing the Plaintiff as the representative plaintiff for the Class and the Credit Monitoring Subclass;

37. An order requiring that the defendants, and each of them fund credit monitoring services for the Plaintiff and Class Members;

38. A declaration that the defendants, and each of them, owed a duty of care to the Plaintiff and the Class Members in the handling and protection of their Personal Information, and breached the standard of care owed to them;

39. A declaration that the defendants, and each of them, owed an additional duty of care to the Plaintiff and the Credit Monitoring Subclass Members to not issue any reports representing that there were no critical developments to be reported, and the defendants breached the standard of care owed to them;

40. A declaration that the defendants, and each of them, was in breach of contract in respect of their Credit Monitoring Agreements with the Plaintiff and the Credit Monitoring Subclass Members;

41. A declaration that the defendants, and each of them, made false and misleading representations to the Plaintiff and the other Class Members and Credit Monitoring Subclass Members, as alleged in this claim;

42. A declaration that the defendants, and each of them, breached s. 1(1) of the *Privacy Act*, RSBC 1996, c 373;

43. A declaration that the defendants, and each of them, breached s. 34 of the *Personal Information Protection Act*, SBC 2003, c 63;

44. A declaration that the defendants, and each of them, breached s. 5(1) of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5;

45. General damages for negligence, breach of contract, negligent misrepresentation and breach of the *Privacy Act*;

46. Restitution for unjust enrichment and waiver of tort;

47. Special and pecuniary damages;

48. Punitive damages;

49. An order for the aggregate assessment of monetary relief and distribution thereof to the Plaintiff and the Class Members;

50. Pre- and post-judgment interest; and

51. Such further and other relief as this Court may deem just.

Part 3: LEGAL BASIS

52. The Plaintiff pleads and relies on the *Class Proceedings Act*, RSBC 1996, c 34, the *Personal Information Protection Act*, SBC 2003, c 63 ("PIPA"), the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("PIPEDA"), the *Privacy Act*, RSBC 1996, c 373, and the *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c 28 ("CJPTA").

Equifax's Statutory Obligations and Breach of the *Privacy Act*

PIPA

53. As private sector corporate entities handling personal information while carrying on business in British Columbia, Equifax was subject to the provisions of PIPA. Section 34 of PIPA provides:

> An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

PIPEDA and Information Protection Principles

54. As private sector corporations that transfer Personal Information across provincial or national borders, Equifax was subject to the provisions of PIPEDA. Section 5(1) of PIPEDA provides:

> Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

55. Schedule 1 to PIPEDA are Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 (collectively, the "Information Protection Principles"). The Information Protection Principles provide, among other things, that:

> 4.7 Principle 7 – Safeguards
>
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection…

4.7.3 The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

(collectively, the "Information Safeguard Principles")

Privacy Act

56. Equifax was also subject to the provisions of the *Privacy Act*, RSBC 1996, Chapter 373 (the "Privacy Act"). Sections 1(1)-(3) of *Privacy Act* provide:

(1) It is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another.

(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, having regard to the lawful interests of others.

(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.

57. Equifax intentionally chose to collect a vast amount of Personal Information of Class Members to advance its own commercial purposes. However, Equifax

failed to take proper precautions to safeguard the Personal Information of Class Members, and in fact, completely ignored the Vulnerability Notice and failed to prevent unauthorized access by third parties to the Personal Information. Equifax is therefore liable for the statutory tort in s. 1(1) of the *Privacy Act*.

Negligence

58. Equifax owed the Plaintiff and Class Members a duty of care in the handling and protection of their Personal Information. Equifax markets itself as an expert in protecting secure data.

59. Once Equifax knew that Personal Information had been accessed, it owed the Plaintiff and the Credit Monitoring Subclass Members an additional duty not to issue any reports representing that there were no critical developments to be reported.

60. The duty of care owed by Equifax in relation to the Personal Information of Class Members is informed by and no less onerous than what is required by s. 34 of *PIPA* and by the Information Safeguard Principles.

61. Equifax breached the standard of care. Particulars of that breach include, but are not limited to:

    a. Failure to handle the collection, retention, security, and disclosure of the Personal Information in accordance with its Privacy Policy, in accordance with the standards imposed by PIPA and PIPEDA, and in accordance with the common law;

    b. Failure to make reasonable security arrangements to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

    c. Failure to maintain or alternatively implement physical, organizational and technological safeguards or control procedures to prevent loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

    d. Failure to use organizational safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having regards to the sensitivity of the information, and below the reasonable standard currently used in the credit reporting industry;

    e. Failure to use technological safeguard measures to protect the Personal Information, or use of measures that were outdated, inadequate having

regards to the sensitivity of the information, and below the reasonable standard currently used in the credit reporting industry;

f. Failure to ensure that Equifax's employees were aware of the importance of maintaining the confidentiality of the Personal Information;

g. Hiring incompetent employees, failing to properly supervise its employees, or failing to provide proper training to its employees;

h. Failure to employ ongoing monitoring and maintenance that would adequately identify and address evolving digital vulnerabilities and threats;

i. Failure to take adequate steps to ensure that the vulnerability of the Disputes Portal would not result in exposure of Personal Information;

j. Failure to detect loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

k. Ignoring the Vulnerability Notice;

l. After it received the Vulnerability Notice, failure to take immediate steps to eliminate the vulnerability and to ensure that the Personal Information of the Plaintiff and other proposed Class Members could not be stolen or the subject of unauthorized access, collection, use, disclosure, copying, modification or disposal;

m. Failure to update Apache Struts after receipt of the Vulnerability Notice or at all;

n. Failure to immediately disable the Disputes Portal after receipt of the Vulnerability Notice, or after Equifax detected suspicious activity;

o. Failure to immediately notify the Plaintiff and the other Class Members after receipt of the Vulnerability Notice, or after Equifax detected suspicious activity;

p. Failure to immediately notify the Plaintiff and other Class Members that their Personal Information had been left unprotected and subjected to loss, theft, unauthorized access, collection, use, disclosure, copying, modification or disposal;

q. Failure to immediately notify the Plaintiff and the other Class Members when their Personal Information was stolen and disclosed on the Internet to unauthorized parties;

r. Failure to immediately notify the Plaintiff and the other Class Members when their Personal Information was the subject of unauthorized access, collection, use, disclosure, copying, modification or disposal;

s. Failure to provide any means for Class Members to determine whether their Personal Information was subject to loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal; and

t. Advising the Plaintiff and other Credit Monitoring Subclass Members that there were no critical developments to be reported when Equifax knew that their Personal Information had been left unprotected and subjected to loss, theft, unauthorized access, collection, use, disclosure, copying, modification or disposal.

62. Equifax knew or ought to have known that a breach of its duty of care would cause loss and damage to the Class Members.

63. As result of Equifax's breach of its duty of care, the Plaintiff and other Class Members suffered loss and damage.

Negligent Misrepresentation

Class Members

64. Through Equifax's Privacy Policy, as set out in paragraph 10 of this claim, Equifax represented to the Plaintiff and Class Members that they would safeguard their Personal Information (the "Safeguarding Representations").

65. The Safeguarding Representations were untrue, inaccurate or misleading in that Equifax did not handle the collection, retention, security, and disclosure of the Personal Information in accordance with Equifax's Privacy Policy.

66. Equifax acted negligently in making the Safeguarding Representations.

67. Equifax knew or alternatively ought to have known that the Plaintiff and other Class Members were going to rely on the Safeguarding Representations.

68. The Plaintiff and other Class Members relied on the Safeguarding Representations to their detriment, and suffered damage as a result.

Credit Monitoring Subclass Members

69. After the Security Breach, Equifax sent written reports to the Plaintiff and other Credit Monitoring Subclass Members as set out in paragraph 31 of this claim. In those communications, Equifax represented that there were no news to report, and that there were no "critical events" in relation to the credit files of the Plaintiff

and other Credit Monitoring Subclass Members (collectively, the "No Critical Events Representations").

70. The No Critical Events Representations were untrue, inaccurate or misleading in that there had been access to and theft of the Personal Information.

71. Equifax acted negligently in making the No Critical Events Representations.

72. Equifax knew or alternatively ought to have known that the Plaintiff and other Credit Monitoring Subclass Members were going to rely upon the No Critical Events Representations.

73. The Plaintiff and other Credit Monitoring Subclass Members relied upon the No Critical Events Misrepresentations to their detriment, and suffered damage as a result.

Breach of Contract

74. It was an express or alternatively implied term of the Credit Monitoring Agreements that, *inter alia*, Equifax would:

    a. Abide by its Privacy Policy and maintain strict security safeguards to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information of the Credit Monitoring Subclass;

    b. Provide accurate and timely reports to Credit Monitoring Subclass Members about their credit information;

    c. Immediately notify Credit Monitoring Subclass Members if their Personal Information was stolen and disclosed on the Internet, or was the subject of unauthorized access, collection, use, disclosure, copying, modification or disposal; and

    d. Provide Credit Monitoring Subclass members with protection against fraud including identity theft.

75. In breach of the Credit Monitoring Agreements, Equifax:

    a. Failed to abide by its Privacy Policy;

    b. Failed to maintain strict security safeguards;

    c. Failed to protect the Personal Information;

d. Exposed the Personal Information of the Plaintiff and the Credit Monitoring Subclass Members, resulting in loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information;

e. Failed to provide timely notification to the Plaintiff and the Credit Monitoring Subclass Members of the loss, theft, and unauthorized access, collection, use, disclosure, copying, modification or disposal of the Personal Information; and

f. Failed to protect the Plaintiff and the Credit Monitoring Subclass Members from fraud including identity theft;

76. The Plaintiff and the Credit Monitoring Subclass Members suffered damages as a result of Equifax's breaches,

Unjust Enrichment and Waiver of Tort

77. The plaintiff pleads that he and other Class Members are entitled to recover under restitutionary principles.

78. Equifax has been unjustly enriched by receipt of payment fees, interest, and service charges generated on products or services it provided to or about the Plaintiff and other Class Members. The Plaintiff and other Class Members have been correspondingly deprived.

79. Since the money that Equifax received resulted from wrongful acts, including breach of the *Privacy Act*, breach of *PIPA*, breach of *PIPEDA*, negligence, negligent misrepresentation and breach of contract, there is no juristic reason justifying Equifax retaining any part of such monies received and Equifax must disgorge and make restitution of the monies received to the Class Members.

80. As a result of Equifax's conduct described herein, specifically, its failure to provide adequate security measures for the Personal Information while representing and warranting to the Plaintiff and the Class Members that the Personal Information was secure and maintained pursuant to statutory privacy obligations and Equifax's Privacy Policy, the Plaintiff reserves the right to elect at the trial of the common issues to waive the tort of negligence and to have damages assessed in an amount equal to the gross revenue received by Equifax, or alternatively, the net income received by Equifax as a result of the fees, interest, and service charges generated on products or services it provided to or about the Plaintiff and the other Class Members.

Damages

81. As a result of Equifax's negligence, breach of contract, misrepresentation and breach of the *Privacy Act*, the Plaintiff and the other Class Members suffered damages including, but not limited to:

    a) Damage to credit reputation;

    b) Mental distress;

    c) Costs incurred in preventing identity theft;

    d) Costs incurred in paying for Credit Monitoring Services;

    e) Out of pocket expenses;

    f) Wasted time, inconvenience, frustration, and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft or improper use of credit information, and to address the credit flags placed on their credit files; and

    g) Time lost engaging in precautionary communications with third parties such as credit card companies, credit agencies, banks, and other parties to inform them of the potential that the Class Members' Personal Information may be misappropriated and to resolve delays caused by flags placed on Class Members credit files.

82. In addition, the Class Members have suffered or will likely suffer further damages from identity theft because the Personal Information was downloaded and reproduced by cybercriminals for criminal purposes, including identity theft and phishing. It is likely or alternatively there is a real and substantial chance that these cybercriminals will use the Personal Information in the future for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft, thereby causing the Class Members to suffer damages.

Punitive Damages

83. Equifax's conduct, as particularized above, was high-handed, outrageous, reckless, wanton, entirely without care, deliberate, callous, disgraceful, willful, and in complete disregard of the rights of the Class Members, and as such, renders Equifax liable to pay punitive damages.

Jurisdiction

84. There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The plaintiff and other Class Members plead and rely upon 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 sections 10 (e) – (h) of the CJPTA because this proceeding:

    a. concerns contractual obligations that, to a substantial extent, were to be performed in British Columbia;

    b. concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;

    c. concerns a tort committed in British Columbia; and

    d. concerns a business carried on in British Columbia.

Plaintiffs' address for service:

BRANCH MACMASTER LLP
1410 - 777 Hornby Street
Vancouver, BC V6Z 1S4
Telephone: (604) 631-2564
(File No.: X01-054)

CAMP FIORANTE MATTHEWS MOGERMAN
#400 – 856 Homer Street
Vancouver, BC V6B 2W 5
Telephone: (604) 689-7555
Fax: (604) 689-7554

Place of trial: Vancouver, British Columbia

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

Dated January 10, 2018

Signature of lawyers for plaintiff

Luciana P. Brasil and Chelsea Hermanson
Branch MacMaster LLP

and

David G. A Jones
Camp Fiorante Matthews Mogerman LLP

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The plaintiff, Joshua Elliott Temple, claims the right to serve this pleading on the defendants outside British Columbia on the ground that there is a real and substantial connection between British Columbia and the facts alleged in this proceeding and the plaintiff and other Class Members plead and rely upon the *CJPTA* in respect of these defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to ss. 10 (e) – (h) of the *CJPTA* because this proceeding:

> (e) concerns contractual obligations that, 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.

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:

Proposed class proceeding regarding damages suffered as a result of an information security breach at the defendant financial institution.

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
[x] 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:

[x] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws

[ ] none of the above
[ ] do not know

Part 4:

1. *Class Proceedings Act*, RSBC 1996, c 34.

2. *Personal Information Protection Act*, SBC 2003, c 63.

3. *Personal Information Protection and Electronic Documents Act* , SC 2000, c 5.

4. *Privacy Act*, RSBC 1996, c 373.

5. *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c 28.