



S=203198

No.
Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN

DONNA OLSON

Plaintiff

AND:

LIFELABS INC., LIFELABS LP, LIFELABS BC INC., LIFELABS BC LP, and
EXCELLERIS TECHNOLOGIES INC.

Defendants

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

- (c) 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
- (d) 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,

- (e) if you were served with the Notice of Civil Claim anywhere in Canada, within 21 days after that service,
- (f) if you were served with the Notice of Civil Claim anywhere in the United States of America, within 35 days after that service,
- (g) if you were served with the Notice of Civil Claim anywhere else, within 49 days after that service, or
- (h) 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

A. NATURE OF THE ACTION

1. This action arises from the largest cybersecurity privacy breach in Canadian history, which was announced by the defendants (collectively, “LifeLabs”) in December 2019. The plaintiff claims damages and relief on her own behalf, and on a class-wide basis pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c. 50, on behalf of all persons resident in British Columbia, Yukon, the Northwest Territories, Alberta, Saskatchewan and Manitoba who were impacted by the privacy breach.

2. LifeLabs is among the largest medical testing laboratory companies in the world. It conducts over a third of all laboratory tests in the province of British Columbia. Through their activities, the defendants collect and store information about identifiable individual clients (“personal information”), including information that is related to the clients’ health, or the provision of health services to the clients (“personal health information”). Both categories of information are of a highly sensitive and personal nature.

3. On or about October 28, 2019, LifeLabs was subject to a cyberattack involving disclosure of the personal information of some 15 million of LifeLabs’ Canadian customers (the “cyberattack” or the “breach”).

4. The cyberattack compromised personal information of LifeLabs’ customers, including their: names, addresses, email addresses, login, passwords, dates of birth, health card numbers, genders, phone numbers, password security questions, and lab test results.

5. On or about December 17, 2019, the defendants released an open letter acknowledging the cyberattack and the compromise of their customers’ personal information. LifeLabs’ letter announced: the date of the breach; that it had notified government privacy regulators on November 1, 2019; that investigations were ongoing from the British Columbia and Ontario privacy commissioners; that the breach occurred when hackers extracted the personal

information of 15 million Canadians from LifeLabs' servers; and that LifeLabs had paid a ransom in connection with the breach.

6. Subsequent reports confirmed that the cyberattack also affected the personal information of approximately 21,670 residents of Alberta, 93,000 residents of Saskatchewan, and 2,900 residents of Yukon. Although residents of Manitoba and the Northwest Territories were also affected by the cyberattack, the precise number of residents affected is presently unknown.

7. In addition to the investigations in Ontario and British Columbia, investigations were subsequently launched by privacy regulators in Alberta and Saskatchewan in respect of the breach.

8. Personal information like the compromised information in this case, including in particular personal health information, is highly sensitive and lies at the core of individual privacy. Personal health information also is accorded the highest value in the black market, and compromised personal health data has a lasting impact. Accordingly, personal health information demands enhanced and special protection.

9. LifeLabs intentionally, wilfully and recklessly failed to have proper information technology ("IT") protection in place to protect the personal information of the proposed class.

10. LifeLabs knew it was a valuable target for hackers and ransomware. LifeLabs knew its IT security was inadequate and vulnerable to hackers.

11. LifeLabs should have had multiple, redundant, overlapping and consistently updated IT security measures in place, including the use of encryption, to ensure the protection of the personal health information in this case and to ensure that, even in the event of a breach, any stolen data would be inaccessible and useless to hackers.

12. At a minimum, among other things, the defendants should have had the following protections in place to prevent the personal information of some 15 million Canadians from being exfiltrated:

- (a) Personal health information should have been encrypted in storage and in transmission throughout the defendants' IT networks;
- (b) Encrypted personal health information should have been accessible on a record-by-record basis only, and using common standards such as role-based access control (ensuring specific employees have access to data for limited, specific purposes only) to limit the scope of potential breaches;
- (c) Multi-factor authentication should have been mandatory for employee user accounts, to ensure redundant security if user passwords were compromised;
- (d) Encrypted databases should have been further protected by use of a master password accessible to only a limited number of trusted and well-trained users;

- (e) Appropriate network segmentation should have been implemented, to limit access to sensitive personal health information even if a network breach occurred;
- (f) Proactive network monitoring processes should have been implemented, including activity logs and system alerts using next-generation persistent threat monitoring, to flag and stop the unauthorized exfiltration of sensitive information; and
- (g) Advanced endpoint detection and response tools should have been in place to stop breaches before they occurred.

13. LifeLabs' wilful, intentional and reckless behaviour—in permitting the breach to occur, failing to prevent the breach, failing to limit the extent of the breach, and failing to respond to the breach appropriately—falls below the standard of care of a repository of personal information, and in particular personal health information, and constitutes both a violation of the privacy rights of the class under the applicable privacy statutes, and the tort of intrusion upon seclusion.

14. LifeLabs' payment of a ransom to the anonymous criminal hackers, combined with only one year of free credit protection services, provides no short-term or long-term protection or remedies to proposed class members.

B. THE DEFENDANTS

15. LifeLabs offers standard medical lab testing through its corporate division LifeLabs Medical Laboratory Services, genetic testing through its corporate division LifeLabs Genetics, and naturopathic testing through its corporate division Rocky Mountain Analytical.

16. LifeLabs Inc. is federally incorporated company. Its headquarters are located in Toronto, Ontario. It is registered extra-provincially in a number of provinces and territories, including Manitoba, Saskatchewan, Alberta, British Columbia, Yukon, and Northwest Territories.

17. LifeLabs LP is a limited partnership formed under the laws of Ontario. Its headquarters are located in Toronto, Ontario. It is registered extra-provincially in a number of provinces and territories, including Manitoba, Saskatchewan, Alberta, British Columbia, Yukon, and Northwest Territories. LifeLabs LP's general partner is LifeLabs Inc.

18. LifeLabs BC Inc. is a company incorporated under the laws of British Columbia with a registered office located in Burnaby, BC.

19. Lifelabs BC LP is a limited partnership formed under the laws of Ontario and registered extra-provincially in British Columbia. LifeLabs BC LP's general partner is LifeLabs BC Inc.

20. Excelleris Technologies Inc. is a company incorporated under the laws of British Columbia with a registered office is located in Vancouver, British Columbia. It is a wholly owned subsidiary of the defendant LifeLabs Inc.

21. Excelleris provides IT systems and IT security to the LifeLabs group of companies.

22. At all material times, LifeLabs represented on its websites that it collects, stores, and uses personal information, including personal health information, in accordance with its own privacy policies and terms of service, which provide in part as follows (collectively, the “Privacy Representations”):

(a) **LifeLabs Terms of Service**

How do we protect your information

Data security

All data on our servers is encrypted when it is stored or in transit. All personal data (genetic or otherwise) is encrypted with AES-256 when it is stored on our servers, and is always transmitted over SSL. Internally, industry standard guidelines and access controls protect [customer] data.

(b) **LifeLabs Privacy Policy**

Accountability: [LifeLabs is] accountable to protect and safeguard [customer] Personal Health Information...

Limiting Use, Disclosure and Retention: Personal health information will not be used or disclosed for purposes other than those for which the information is collected or as required or permitted by law.

...

Safeguards: LifeLabs takes security measures to ensure [customer] personal health information is protected from loss, theft, unauthorized access, use, copying or disclosure. As a health information custodian, [LifeLabs] review[s] and update[s] security measures to meet industry standards. [LifeLabs has] implemented safeguards to protect [customer] personal information and these include but are not limited to:

Physical safeguards: locking filing cabinets and restricting access to [LifeLabs] facilities to only authorized employees, vendors or visitors

Technical safeguards: passwords, encryptions and firewalls

Administrative safeguards: role based access, staff training, signing a confidentiality pledge.

(c) **LifeLabs Genetics Privacy and Security FAQs**

The privacy, security, and confidentiality of [customer] information and biological samples are maintained at every step of the process. At LifeLabs, protecting the privacy and security of personal information is essential and is fundamental to our values and to the way we do business.

(d) **Rocky Mountain Analytical Privacy Policy**

Rocky Mountain Analytical is committed to protecting your privacy. Our employees have been trained to respect your privacy at all times and those employees with access to your personal information shall use your personal information strictly in accordance with Rocky Mountain Analytical's Privacy Policy and the laws applicable to each specific business.

(e) **Excelleris Website and Excelleris Privacy Policy**

Privacy and security are at the core of Excelleris and are embedded in all our solutions. We apply privacy by design principles to meet the highest standard of compliance and earn the confidence of all our clients. Not only do we adhere to privacy regulations, but we also follow industry best practices to ensure the security of all data. You can count on Excelleris for:

- Provincial and federal privacy compliance
- Integrated privacy work flows and monitoring
- Data protection, tracking and notification
- Incident management and disaster recovery

(f) Excelleris has appropriate physical, technical and procedural safeguards in place to protect Personal Information.

C. THE PLAINTIFF AND THE CLASS

23. The plaintiff Donna Olson ("**Ms. Olson**" or "**the plaintiff**") is an individual residing in Vancouver. Ms. Olson attended at LifeLabs facilities in British Columbia for medical tests prior to the cyberattack, and, in each case, entered into a standard form contract with LifeLabs for medical testing services (the "**Testing Contract**").

24. The Testing Contract provided that, in exchange for Ms. Olson's use of LifeLabs' services, LifeLabs could collect and use Ms. Olson's personal information, including personal health information, in accordance with, amongst other things, the Privacy Representations.

25. Pursuant to the Testing Contract, Ms. Olson provided personal information, including personal health information, to LifeLabs, including her name, address, date of birth, health card number, and relevant medical history. The collection and storage of all of this information was governed by the Privacy Representations.

26. LifeLabs stored the personal information including personal health information Ms. Olson provided pursuant to the Testing Contract, including lab test results.

27. Prior to the cyberattack, the plaintiff also entered into a standard form contract with Lifelabs for use of a “My Results” online account on the LifeLabs website (the “**Online Account Contract**”). Pursuant to the Online Account Contract, Ms. Olson agreed to provide personal information in exchange for LifeLabs’ collection and use of that information in accordance with, amongst other things, the Privacy Representations.

28. Pursuant to the Online Account Contract, and in addition to the personal information which was collected and retained by LifeLabs pursuant to the Testing Contract, the plaintiff provided LifeLabs with additional personal information in order to sign up for an online account, including her email, login information, password, and credit card information.

29. On or about January 9, 2020, LifeLabs notified Ms. Olson that its investigations indicated that her online booking account was within the group of systems that were potentially impacted by the breach.

30. Ms. Olson’s personal information was knowingly, wilfully or recklessly compromised by the defendants in the breach. As a result of the breach of her privacy, Ms. Olson has suffered and will continue to suffer damage including:

- (a) costs incurred to remedy and/or prevent identity theft;
- (b) damage to reputation;
- (c) serious and prolonged emotional and mental distress;
- (d) humiliation;
- (e) out-of-pocket expenses;
- (f) general damages to be assessed in the aggregate; and,
- (g) special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable to LifeLabs’ breaches as alleged herein.

31. The plaintiff seeks to represent the following class (the “**Proposed Class**” or “**Class Members**”): all persons resident in British Columbia, Yukon, the Northwest Territories, Alberta, Saskatchewan and Manitoba whose personal information was accessed in the breach announced by the defendants on December 17, 2019.

PART 2: RELIEF SOUGHT

32. The plaintiff, on her own behalf and on behalf of all Class Members, seeks:

- (a) an order pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 (the “**CPA**”) certifying this action as a class proceeding and appointing the plaintiff as the representative plaintiff;

- (b) an aggregate assessment of damages in the amount of \$100 million for:
 - (i) breaches of the *Privacy Act*, R.S.B.C. 1996, c. 373, the *Privacy Act*, R.S.S. 1978, c. P-24, and the *Privacy Act*, C.C.S.M., c. P125;
 - (ii) negligence;
 - (iii) intrusion upon seclusion;
 - (iv) breach of contract; and
 - (v) engaging in unfair practices contrary to s. 4 of the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2 and equivalent provisions of Equivalent Consumer Protection Statutes (as defined below);
- (c) an order pursuant to s. 27 of the *CPA*, directing individual hearings, inquiries and determinations for Class Members who have suffered or may have suffered special damages as a result of unlawful conduct by third parties, including identity theft or fraud, which was occasioned by or attributable to LifeLabs' breaches as alleged, and all necessary directions relating to the procedures to be followed in conducting such hearings, inquiries and determinations;
- (d) exemplary, punitive damages and/or aggravated damages in the amount of \$25 million;
- (e) a reference to decide any issues not decided at the trial of the common issues;
- (f) the costs of administering and distributing a damages award;
- (g) pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c 79; and
- (h) such further and other relief as this Honourable Court may deem just.

PART 3: LEGAL BASIS

A. BREACH OF PRIVACY LEGISLATION

33. Section 1 of the *Privacy Act*, R.S.B.C. 1996, c. 373 ("BC Privacy Act") provides:

1 (1) It is a tort, actionable without proof of damage, for a person, wilfully 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, giving due 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.

(4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

34. Section 2 of the *Privacy Act*, R.S.S. 1978, c. P-24 ("Saskatchewan Privacy Act") similarly provides:

Violation of privacy

2 It is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person.

35. Section 2 of the *Privacy Act*, C.C.S.M., c. P125 ("Manitoba Privacy Act") provides:

Violation of privacy

2(1) A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.

2(2) An action for violation of privacy may be brought without proof of damage.

36. LifeLabs is governed by the BC Privacy Act, Saskatchewan Privacy Act and the Manitoba Privacy Act.

37. The nature and degree of the Class Members' privacy in this case is particularly strong. Persons outside the Class Members' circle of medical care have no lawful interest in the personal information of the Class Members.

38. LifeLabs failed to take appropriate steps to guard against unauthorized access to sensitive personal information, including personal health information, involving Class Members' private affairs or concerns. The actions of LifeLabs constitute intentional, wilful and reckless violations of the plaintiff and the Class' privacy, for which LifeLabs is liable.

39. LifeLabs' actions were highly offensive, causing distress and anguish to Class Members for which LifeLabs is liable and should pay damages.

B. NEGLIGENCE

40. LifeLabs owed Class Members a duty of care in the collection, retention, use, and disclosure of their personal information, including in particular personal health information, and a duty to safeguard the confidentiality of their personal information in accordance with legislative and industry standards.

41. LifeLabs breached the standard of care by:
- (a) failing to encrypt Class Members' data and to implement and maintain appropriate, adequate and effective cybersecurity measures to safeguard Class Members' personal information;
 - (b) failing to comply with the minimum standards provided in: the *Personal Information Protection Act*, S.B.C. 2003, c. 63; the *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c. 38; the *Personal Information Protection Act*, S.A. 2003, c. P-6.5; the *Health Information Act*, R.S.A. 2000, c. H-5; the *Health Information Privacy and Management Act*, S.Y. 2013, c. 16; the *Health Information Protection Act*, S.S. 1999, c. H-0.021; and the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, as applicable;
 - (c) failing to collect, store, use, retain, and/or disclose Class Members' personal information in accordance with industry standards for healthcare information and in accordance with its own privacy policies, including the Privacy Representations; and,
 - (d) subsequent to learning of the existence of the breach on October 28, 2019, failing to inform Class Members of the breach in a timely way and waiting over seven weeks before making a public disclosure of the breach.
42. As a result of LifeLabs' negligence, Class Members suffered reasonably foreseeable damages and losses for which LifeLabs is liable.

C. INTRUSION UPON SECLUSION

43. The actions of LifeLabs constitute intentional or reckless intrusions upon the Class Members' seclusion that would be highly offensive to a reasonable person, for which LifeLabs is liable.
44. LifeLabs failed to take appropriate steps to guard against unauthorized access to sensitive personal information involving the Class Members, including in particular their personal health information. Their actions were highly offensive, causing distress and anguish to Class Members, for which the defendants are liable and should pay damages.
45. Specifically, the tort of intrusion upon seclusion is made out because:
- (a) the unidentified hackers intentionally invaded the Class Members' privacy;
 - (b) LifeLabs' wilfully blind or reckless conduct regarding cybersecurity and the protection of the Class Members' personal information facilitated the hackers' ability to invade the Class Members' privacy and led directly to the invasion of the Class Members' privacy;

- (c) there was no lawful justification for the invasion of the Class Members' privacy; and,
- (d) a reasonable person would consider the invasion of the Class Members' personal information, and in particular their personal health information, to be highly offensive.

D. BREACH OF CONTRACT

46. When LifeLabs entered into standard form contracts with the plaintiff and Class Members, including the Testing Contract, Online Account Contract and equivalent contracts with Class Members, LifeLabs stated and represented as follows in its Privacy Representations, amongst other things:

- (a) "protecting the privacy and security of personal information is essential and is fundamental to [LifeLabs'] values and to the way [LifeLabs does] business";
- (b) privacy is "embedded" in "all [LifeLabs'] solutions"; and
- (c) LifeLabs' IT security met "the highest standard" of compliance and followed "industry best practices".

47. LifeLabs' privacy policies, including the Privacy Representations, formed express or implied terms of service of the Testing Contracts and Online Account Contracts between LifeLabs and Class Members.

48. LifeLabs breached the Testing Contracts and Online Account Contracts by failing to collect, store, use, retain, and/or disclose Class Members' personal information in accordance with its own privacy policies, including the Privacy Representations, causing damage to the Class Members.

E. BREACH OF CONSUMER PROTECTION LEGISLATION AND THE COMPETITION ACT

49. LifeLabs engaged in unfair practices by making false, misleading and/or deceptive representations to the Class Members regarding LifeLabs' privacy and cybersecurity practices, contrary to the *Competition Act*, R.S.C. 1985, c. C-34, the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2 ("**BPCPA**") and consumer protection statutes in other Canadian provinces, including: the *Consumer Protection Act*, R.S.A. 2000, c. C-26.3; the *Consumer Protection Act*, S.S. 1996; the *Consumer Protection and Business Practices Act*, S.S. 2013, c. C-30.2; and *The Business Practices Act*, C.C.S.M. c. B120 (collectively, the "**Equivalent Consumer Protection Statutes**").

50. LifeLabs is a "supplier" and Class Members are "consumers" within the meaning of the *BPCPA*. The Equivalent Consumer Protection Statutes also have application to the consumer relationship between LifeLabs and Class Members.

51. LifeLabs made the Privacy Representations for the purpose of promoting its business interests, and in particular:

- (a) to represent that it takes “industry best standard” security measures to ensure Class Members’ personal information is protected from loss, theft, unauthorized access, use, copying or disclosure; and
- (b) to represent that its security measures include encryption of data and other technical safeguards, as well as staff privacy training and ongoing audits of staff access to personal information.

52. Although LifeLabs represented that it meets the highest standards of privacy compliance, it failed to safeguard Class Members’ personal information, including personal health information, appropriately and did not meet the industry standards for privacy compliance at all, let alone the highest industry standards. LifeLabs’ representations were and are therefore false.

53. At the time of the breach, LifeLabs knew or ought to have known that their IT security and privacy policies were ineffective and inadequate and rendered their customers’ personal information vulnerable to theft or compromise.

54. Lifelabs’ Privacy Representations were knowingly or recklessly false or misleading to the public in a material respect and offended s. 52 of the *Competition Act*.

55. Contrary to the *BPCPA* and the Equivalent Consumer Protection Statutes, LifeLabs made false, misleading, or deceptive representations that it takes extensive security measures to protect Class Members personal information, when in fact it does not. Class Members suffered damages as a result of LifeLabs’ breaches of the *BPCPA* and the Equivalent Consumer Protection Statutes.

56. As consumers, Class Members are entitled to an award of damages pursuant to s. 171 of the *BPCPA* and equivalent damage provisions of the Equivalent Consumer Protection Statutes, as a result of LifeLabs’ false, misleading and/or deceptive representations.

F. DAMAGE SUFFERED BY CLASS MEMBERS

57. As a result of LifeLabs’ actions, Class Members have suffered and will continue to suffer damage including:

- (a) costs incurred to remedy or prevent identity theft;
- (b) damage to reputation;
- (c) serious and prolonged emotional and mental distress;
- (d) humiliation;
- (e) out-of-pocket expenses;

- (f) general damages to be assessed in the aggregate; and,
- (g) special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable to LifeLabs' breaches as alleged herein.

58. Damages should be awarded on an aggregate and an individual basis. LifeLabs' conduct as detailed above has materially increased the risk of identity theft for all Class Members and accordingly has materially increased the quantum of damages that will arise from identity theft to Class Members.

59. The plaintiff requests individuals hearings under s. 27 of the *CPA* for a determination of the special damages described above.

60. By virtue of the loss or damage she has suffered as a result of LifeLabs' conduct contrary to s. 52 of the *Competition Act*, the plaintiff requests the costs of investigation and prosecution of this action pursuant to s. 36(1) of the same statute.

G. PUNITIVE DAMAGES REQUESTED

61. LifeLabs' conduct was high-handed, reckless, without care, deliberate, and offends the moral standards of the community. LifeLabs knew that medical service providers are at a particularly elevated risk of being targeted by hacking efforts, that they had been subject to previous hacking efforts, investigations and audits, that they were particularly vulnerable to being hacked, and knew that their systems would be a treasure trove for hackers. LifeLabs knew or ought to have known that their actions would have a significant adverse effect on all Class Members.

62. Moreover, subsequent to learning of the existence of the extensive privacy breach on October 28, 2019, LifeLabs waited over seven weeks before making a public disclosure of the breach. This conduct was further high-handed, reckless, without care, deliberate, and offensive to moral standards of the community.

**ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE
OUTSIDE BRITISH COLUMBIA**

63. The plaintiff claims the right to serve this pleading/petition on the defendants outside British Columbia on the grounds that there is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The plaintiff pleads and relies upon the *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003, c. 28 (“*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 s. 10 of the *CJPTA* because this proceeding:

- (a) concerns contractual obligations that, to a substantial extent, were to be performed in British Columbia;
- (b) concerns a tort committed in British Columbia; and,
- (c) concerns a business carried on in British Columbia.

Plaintiff's address for service:

Brent B. Olthuis/ Julia E. Roos
Hunter Litigation Chambers
1040 West Georgia Street
Suite 2100
Vancouver, BC V6E 4H1

Sotos LLP
180 Dundas Street West
Suite 1200
Toronto, ON M5G 1Z8

Fax number address for service (if any):

(604) 647-3540

E-mail address for service (if any):

bolthuis@litigationchambers.com
jroos@litigationchambers.com
jleclerc@sotosllp.com

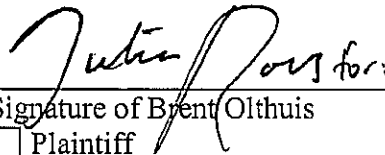
Place of trial:

Vancouver Law Courts

The address of the registry is:

800 Smithe Street
Vancouver, BC V6Z 2E1

Date: March 16, 2020



Signature of Brent Olthuis
 Plaintiff
 Lawyer for Plaintiff

APPENDIX

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This action arises from a cybersecurity privacy breach involving the personal information of approximately 15 million Canadians.

The claim seeks damages and relief on behalf of all residents in British Columbia, Yukon, the Northwest Territories, Alberta, Saskatchewan and Manitoba, affected by the privacy breach.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

- a motor vehicle accident
- medical malpractice
- another cause

A dispute concerning:

- contaminated sites
- construction defects
- real property (real estate)
- 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
- a matter not listed here

Part 3: THIS CLAIM INVOLVES:

- a class action
- maritime law
- aboriginal law

- constitutional law
- conflict of laws
- none of the above
- do not know

Part 4:

- Builders Lien Act
- Divorce Act
- Family Relations Act
- Insurance (Motor Vehicle) Act
- Insurance (Vehicle) Act
- Motor Vehicle Act
- Occupiers Liability Act
- Supreme Court Act
- Wills Variation Act

OR

1. *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2
2. *Privacy Act*, R.S.B.C. 1996, c. 373
3. *Personal Information Protection Act*, S.B.C. 2003, c. 63