Electronically issued
Délivré par voie électronique : 27-Dec-2019
Toronto

Court File No.:

ONTARIO
SUPERIOR COURT OF JUSTICE

**CHRISTOPHER SPARLING,
DR. ADRIANO PERSI, AGATINA RICO,
JOAQUIN GUTIERREZ TRUJILLO, and
RYAN SADLER**

Plaintiffs

-and -

**LIFELABS INC., LIFELABS LP, LIFELABS ONTARIO INC.,
LIFELABS BC INC., LIFELABS BC LP,
EXCELLERIS TECHNOLOGIES INC.,
FRANK AMODEO, CHARLES BROWN, ELSA CABRAL,
TOM CLOSSON, BRENDA EATON, GISELE EVERETT,
JOHN KNOWLTON, MICHAEL MA, JOHN MCMANUS,
JON NANTHO, JAMES SCONGACK, GAVIN STUART,
PIERRE BOU-MANSOUR, AKIKO CAMPBELL,
JENNIFER CUDLIPP, and JILL SHARLAND**

Defendants

Proceeding under the *Class Proceedings Act*, 1992, S.0. 1992, c. 6, as amended

STATEMENT OF CLAIM

TO THE DEFENDANTS:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiff. The Claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a Statement of Defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the Plaintiff's lawyer, or where the Plaintiff does not have a lawyer, serve it on the Plaintiff and file it, with proof of service, in this court office, **WITHIN TWENTY DAYS** after this Statement of Claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your Statement of Defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a Statement of Defence, you may serve and file a Notice of Intent to Defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to file your Statement of Defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. If you wish to defend this proceeding but are unable to pay legal fees, legal aid may be available to you by contacting a local Legal Aid office.

IF YOU PAY THE PLAINTIFFS' CLAIM, and $3,000.00 for costs, within the time for serving and filing your Statement of Defence, you may move to have this proceeding dismissed by the court. If you believe the amount claimed for costs is excessive, you may pay the Plaintiffs' claim and $3,000.00 for costs and have the costs assessed by the court.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

DATED: December 27, 2019 Issued by:

LOCAL REGISTRAR
393 University Avenue
10th Floor
Toronto, Ontario
M5G 1E6

TO: **LIFELABS INC.**
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **LIFELABS LP**
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **LIFELABS ONTARIO INC.**
200 BAY ST, ROYAL BANK PLAZA,
SOUTH TOWER, SUITE 2100,
TORONTO, ON M5J 2J2

AND TO: **LIFELABS BC INC.**
90 GILMORE WAY,
BURNABY, BC, V5G 1V8

AND TO: **LIFELABS BC LP**
3680 GILMORE WAY,
BURNABY BC, V5G 4V8

AND TO: **EXCELLERIS TECHNOLOGIES INC.**
2900-550 BURRARD STREET,
VANCOUVER, BRITISH COLUMBIA, V6C 0A3

AND TO: **FRANK AMODEO**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **CHARLES BROWN**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **ELSA CABRAL**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **TOM CLOSSON**
210 WALMER ROAD
TORONTO, ON M5R 3R7

AND TO: **BRENDA EATON**
4012 RAINBOW HILL LANE
VICTORIA, BC V8X 0A6

AND TO: **GISELE EVERETT**
450 PARK AVENUE, 9TH FLOOR
NEW YORK, NY 10022

AND TO: **JOHN KNOWLTON**
900-100 ADELAIDE STREET WEST
TORONTO, ON M5H 0E2

AND TO: **MICHAEL MA**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **JOHN MCMANUS**
900-100 ADELAIDE STREET WEST
TORONTO, ON M5H 0E2

AND TO: **JON HANTHO**
4 GLENDARLING ROAD
TORONTO, ON M9A 4G2

AND TO: **JAMES SCONGACK**
228 TRILLIUM DRIVE
PORT ELGIN, ON N0H 2C2

AND TO: **GAVIN STUART**
2775 LAUREL STREET, 6TH FLOOR
VANCOUVER, BC V5Z 1M9

AND TO: **PIERRE BOU-MANSOUR**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

AND TO: **AKIKO CAMPBELL**
3680 GILMORE WAY
BURNABY BC V5G 4V8
CANADA

AND TO: **JENNIFER CUDLIPP**
3680 GILMORE WAY
BURNABY BC V5G 4V8
CANADA

AND TO: **JILL SHARLAND**
C/O LIFELABS INC.
100 INTERNATIONAL BLVD.
TORONTO, ON M9W 6J6

The Claim

1. The Plaintiffs on their own behalf and on behalf of the Class Members, claim:

(a) an Order that the Plaintiff Christopher Sparling is appointed as a Class Representative and the other Plaintiffs are appointed as alternative class representatives subject to the Court's approval;

(b) an order pursuant to the *Class Proceedings Act, 1992* (the "*CPA*"), certifying this action as a class proceeding;

(c) a declaration that the Defendants owed a duty of care to the Plaintiffs and the Class Members, and breached the standard of care owed to them;

(d) a declaration that the Defendants were negligent and failed in their duty to implement an appropriate standard of care;

(e) a declaration that the Defendants are liable in breach of contract by breaching their contracts with the Plaintiffs and the Class Members;

(f) a declaration that the Defendants breached the confidence of the Plaintiffs and the Class Members;

(g) a declaration that the Defendants intruded upon seclusion of the Plaintiffs and the Class Members or, in the alternative, are jointly and severally liable for intruding upon seclusion of the Plaintiffs and the Class Members;

(h) a declaration that the Defendants committed the tort of public disclosure of private information or, in the alternative, that the Defendants are jointly and severally liable for committing the tort of public disclosure of private information;

(i) a declaration that the Defendants violated the *Consumer Protection Act* ("the *Consumer Protection Act*"), 2002, S.O. 2002, c.30, Sched. A, and other equivalent provincial and territorial consumer protection legislation;

(j) a declaration that the Defendants breached the statutory privacy rights of the Plaintiffs and the Class Members, including those as set out in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000 c. 5, and the *Personal Health Information Protection Act*, 2004, S.O. 2004, c 3, Sched A and other equivalent provincial and territorial information protection legislation and personal health information protection legislation;

(k) a declaration that the Defendants were unjustly enriched, to the deprivation of the Class members;

(l) an Order that the Defendants disgorge to the Class Members, or as directed by the Court, any profits of their services in the period during which the Defendants acted negligently and were in breach of fiduciary duties and obligations to the Class Members or such period, as the Court determines; and the Class Members would rely upon the cause of action of waiver of tort;

(m) an interim or permanent Order requiring that the Defendants fund credit monitoring services and credit insurance for the Plaintiffs and the Class Members;

(n) an Order directing the common issues respecting liability and damages;

(o) an aggregate assessment of damages in the amount of $1,130,000,000.00 for:

i) Negligence;
ii) Breach of contract;
iii) Breach of duties of good faith, honesty and fair dealing;
iv) Breach of confidence;
v) Intrusion upon seclusion;

vi) Public disclosure of private information;

vii) Breach of Directors and Officers Liability; and

viii) Breach of provincial privacy and consumer protection legislation.

(p) $10,000,000.00 for punitive damages or an amount that this Court finds appropriate at the trial of the common issues or at a reference or references;

(q) an Order, pursuant to s. 24 of the *CPA*, directing an aggregate assessment of damages;

(r) an Order directing a reference or giving such other directions as may be necessary to determine any issues not determined at the trial of the common issues;

(s) an Order directing a reference or giving such other directions as may be necessary to determine any issues not determined at the trial of the common issues;

(t) pre-judgment and post-judgment interest, compounded, or pursuant to ss. 128 and 129 of the *Courts of Justice Act*, R.S.O. 1990, c.43;

(u) the costs of this action on a full indemnity basis, or in an amount that provides substantial indemnity, plus the costs of notices and of administering the plan of distribution of the recovery in this action, together with applicable HST or other applicable taxes thereon; and

(v) such further and other relief as this Honourable Court deems just.

Parties and Overview

Plaintiffs

2. This action arises out of a cybersecurity breach that occurred on or about October 28, 2019 wherein unidentified hackers accessed, extracted and/or exfiltrated from the Defendants'

computer systems, personal information and/or health records of around 15 million of the LifeLabs' customers located across Canada.

3. The Plaintiff, Christopher Sparling, is a lawyer that resides in Toronto, Ontario. Christopher Sparling used the services of LifeLabs and is a customer of the Defendants as defined below.

4. The Plaintiff, Dr. Adriano Persi, resides in Hamilton, Ontario. The Plaintiff Dr. Adriano Persi used the services of LifeLabs and is a customer of the Defendants as defined below.

5. The Plaintiff, Agatina Rico, resides in Toronto, Ontario. The Plaintiff Agatina Rico used the services of LifeLabs and is a customer of the Defendants as defined below.

6. The Plaintiff, Joaquin Gutierrez Trujillo, resides in Toronto, Ontario. The Plaintiff Joaquin Gutierrez Trujillo used the services of LifeLabs and is a customer of the Defendants as defined below.

7. The Plaintiff, Ryan Sadler, resides in Toronto, Ontario. The Plaintiff Ryan Sadler used the services of LifeLabs and is a customer of the Defendants as defined below.

Defendants

8. The Defendant, LifeLabs Inc. ("**LifeLabs**") is a Canadian corporation incorporated under the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44 with its head office located at 100 International Blvd., Toronto, Ontario M9W 6J6. LifeLabs is a lab testing company that provides general diagnostic and specialty laboratory testing to customers across Canada. The company has four core divisions – LifeLabs Medical Laboratory Services, LifeLabs Genetics, Rocky Mountain Analytical, and Excelleris.

9. The Defendant, LifeLabs LP ("**LifeLabs LP**") is a limited partnership incorporated under the laws of Ontario and headquartered at 100 International Blvd, Toronto, Ontario M9W

6J6, and carrying out business of diagnostic services under the registered name LifeLabs. LifeLabs is a general partner of LifeLabs LP.

10. The Defendant, LifeLabs Ontario Inc. ("**LifeLabs ON**") is an Ontario business corporation with the address at 200 Bay St, Royal bank Plaza, South Tower, Suite 2100, Toronto, ON M5J 2J2, and carries out business in relation to LifeLabs.

11. The Defendant, LifeLabs BC Inc. ("**LifeLabs BC**") is a company incorporated in British Columbia with a registered office at 90 Gilmore Way, Burnaby, British Columbia, V5G 1V8 and a records office at 2900-550 Burrard Street, Vancouver, BC V6C 03A, and carries out business in relation to LifeLabs.

12. The Defendant, LifeLabs BC LP ("**LifeLabs BC LP**") is a limited partnership incorporated under the laws of Ontario and headquartered at 100 International Blvd, Toronto, Ontario M9W 6J6 and carrying out business of diagnostic services. LifeLabs BC LP has extraprovincial limited partnership registration with business and mailing address at 3680 Gilmore Way, Burnaby BC, V5G 4V8. LifeLabs BC is a general partner of LifeLabs BC LP.

13. The Defendant, Excelleris Technologies Inc. ("**Excelleris**") is a corporation incorporated under the laws of British Columbia and headquartered at 2900-550 Burrard Street, Vancouver, British Columbia V6C 0A3 with an extra-provincial registration in Ontario. Excelleris provides e-health services that are providing electronic access to, retention and storage of personal information relating to health care.

14. The Defendant, Frank Amodeo ("**Amodeo"**), is the Senior Vice-President of Corporate Services of LifeLabs, a signatory of LifeLabs LP and Officer and Manager of Excelleris, and resides in Toronto.

15. The Defendant, Charles Brown ("**Brown**"), is the CEO and President of LifeLabs and resides in Toronto, Ontario.

16. The Defendant, Elsa Cabral ("**Cabral**"), is the Vice-President of Client Services and Logistics of LifeLabs and resides in Toronto, Ontario.

17. The Defendant, Tom Closson ("**Closson**"), is a Director of LifeLabs and resides in Toronto, Ontario.

18. The Defendant, Brenda Eaton ("**Eaton**"), is a Director of LifeLabs and resides in Victoria, British Columbia.

19. The Defendant, Gisele Everett ("**Everett**"), is the Director of LifeLabs and resides in New York, NY, United States.

20. The Defendant, John Knowlton ("**Knowlton**"), is a Director of LifeLabs and a Director and Officer at LifeLabs Ontario Inc., who resides in Toronto, Ontario.

21. The Defendant, Michael Ma ("**Ma**"), is the Chief Information Officer of LifeLabs, who resides in Toronto, Ontario. At all material times, Ma was responsible for information technology and IT systems at LifeLabs Inc.

22. The Defendant, John McManus ("**McManus**"), is a Director of LifeLabs and resides in Toronto, Ontario.

23. The Defendant, Jon Nantho ("**Nantho**"), is a Director of LifeLabs and resides in Toronto, Ontario.

24. The Defendant, James Scongack ("**Scongack**"), is a Director of LifeLabs and resides in Port Elgin, Ontario.

25. The Defendant, Gavin Stuart ("**Stuart**"), is a Director of LifeLabs and resides in Vancouver, British Columbia.

26. The Defendant, Pierre Bou-Mansour, ("**Bou-Mansour**"), is an Officer and a Vice President of Excelleris.

27. The Defendant, Akiko Campbell, ("**Campbell**"), is an Officer and a President of Excelleris and resides in Toronto, Ontario.

28. The Defendant, Jennifer Cudlipp, ("**Cudlipp**"), is a Director of Excelleris and resides in Burnaby, British Columbia.

29. The Defendant, Jill Sharland, ("**Sharland**"), is an Officer and a Treasurer of Excelleris and resides in Toronto, Ontario.

30. The Plaintiffs plead that the Defendants LifeLabs and Excelleris are vicariously liable for the negligence of its servants, agents, employees, officers, and/or members.

Class Definition

31. The proposed class action is brought on behalf of all Canadians who used the services of the Defendants. Alternatively, in the event the Defendants identify the individuals whose information was compromised and notify them, then the class definition shall be all Canadians who were notified their information was compromised in the breach.

32. The Plaintiffs seek to represent the proposed class.

Facts

33. On October 28, 2019, the Defendants informed the Province of British Columbia of a potential cybersecurity breach.

34. On November 1, 2019, the Defendants reported a potential cyberattack on their computer systems to the Office of the Information and Privacy Commissioner of Ontario ("**IPC**") and the Office of the Information and Privacy Commissioner for British Columbia ("**OPIC**").

35. On or shortly after November 1, 2019, the Defendants confirmed they were the subject of an attack affecting the personal information of approximately 15 million customers across Canada, primarily in Ontario and British Columbia. The affected systems contained personal information of the Defendants' customers, including names, addresses, emails, customer logins and passwords, health card numbers, and lab test results ("**the Personal Information**").

36. The Defendants informed the IPC and OPIC that cybercriminals had hacked into the company's systems, extracting data and demanding a ransom.

37. The Defendants' customers are required to provide their health card and the Personal Information including but not limited to name, date of birth and address when attending a lab.

38. Customers can also create an online account to access their lab test results online. Creating an online account requires users to create a login username and password and input the Personal Information including, name, date of birth, address, email and health card number.

39. The Defendant LifeLabs', website outlines its Terms of Service, including a Privacy Policy, which provides:

    a) Accountability: We are accountable to protect and safeguard your personal health information we collect, use and disclose. LifeLabs ensures that current privacy policies and procedures established are compliant with privacy legislation. Our Privacy Office conducts annual privacy training for staff, and conducts ongoing audits of our staff access to your personal health information. Our Privacy Office is available to respond to your privacy questions or concerns.

    b) Identifying Purposes: We will identify the purpose for which personal information is collected at or before the time the information is collected.

c) Consent: LifeLabs operates on the order of your health care provider; therefore, consent may be implied for some defined circumstances. For example, when you visit one of our patient service centres with a test requisition from your physician, we rely on your implied consent not only to carry out those tests but to collect, use and disclose your personal health information in order to share the results with your health care providers. LifeLabs also posts notices in our patient service areas to advise you of the purposes for which we collect, use and disclose your personal health information. In some instances, LifeLabs will obtain your express consent when we collect, use and disclose your personal health information.

d) Limiting Collection: LifeLabs will limit the collection of personal health information to that which is necessary for the authorized purposes identified. Information will be collected by fair and lawful means.

e) 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.

f) Safeguards: LifeLabs takes security measures to ensure your personal health information is protected from loss, theft, unauthorized access, use, copying or disclosure. As a health information custodian, we review and update our security measures to meet industry standards. We have implemented safeguards to protect your personal information and these include but are not limited to:

Physical safeguards: locking filing cabinets and restricting access to our 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.

g) Openness: At LifeLabs, we have communications posted in our patient waiting areas to notify you about our current practices in place to protect your personal health information. To ensure quality of service, we can communicate with you via telephone, in person and e-mail. We are committed to safeguarding your personal health information irrespective of the method through which we communicate with you.

h) Individual Access: We offer our patients online access to their test results. Patients with access to the internet can register free of charge to our *my results*™ portal in Ontario and *my ehealth*™ portal in BC to view their results. Not all test results are available on our portal; specifically, we don't post, those results that are: sensitive in nature; controlled by regulatory requirements; sent to a government lab for analysis; or test results that are required to be reported directly to the ordering physician.

40. The Defendant Excelleris' website outlines its Privacy Statement that provides:

a) Protecting privacy and security of personal information is essential to the Excelleris' values and the way we conduct our business;

b) Excelleris is accountable to protect the privacy of the personal information in our care;

c) Excelleris has appropriate physical, technical and procedural safeguards in place to protect personal information; and

d) Excelleris remains firmly committed to maintaining the privacy and confidentiality of personal information in our care.

41. The data breach affected the Class Members who have used the Defendants' services, including those who physically visited a lab and/or used their online services/portal.

42. The Defendants, contrary to the Terms of Service and the Privacy Policy, failed to encrypt the Personal Information on their servers, exposing and enhancing the vulnerability of the exfiltration of the Class Members' data.

43. The Defendants', contrary to their publicized Terms of Service and the Privacy Policy and contrary to the industry standards ("**the Industry Standards**"), failed to implement adequate safeguards and internal controls to protect the Personal Information and health records of the Class Members from loss, theft, unauthorized access, unauthorized, unauthorized use, unauthorized duplication and/or unauthorized disclosure.

44. As a result of the cybersecurity breach and the access, extraction and/or exfiltration of the Class Members' data, the Plaintiffs' Personal Information has been intentionally accessed on a computer/server without their personal authorization, including their names, dates of birth, addresses, health card information and/or lab test results.

45. Some of such safeguards and internal controls may include, but are not limited to encryption, tokenization, multi-factor authentication, data loss prevention (DLP), identity and access management, intrusion detection, data protection, security risk assessments, least privilege access, asset management, vulnerability management, endpoint protection, malware defences, security monitoring, security incident response, application security, security architecture, penetration testing, vendor/supplier/third-party risk management, and security awareness and training.

46. The Industry Standards include, but are not limited to ISO 27001/27002, NIST SP800-53 Revisions 3 and 4, NIST Cybersecurity Framework, ISF Standard of Good Practice, and Canadian Standards Association's Model Code for the Protection of Personal Information CAN/CSA-Q830-96.

47. The Defendants', contrary to their Terms of Service and the Privacy Policy and contrary to the Industry Standards, failed to test and verify the adequacy and effectiveness of any

safeguards and internal controls, that might have been implemented by the Defendants' to protect the Personal Information and health records of the class members from loss, theft, unauthorized access, unauthorized use, unauthorized duplication and/or unauthorized disclosure.

48. The Defendants', contrary to their Terms of Service and the Privacy Policy and contrary to the Industry Standards, failed to implement adequate measures and controls to detect and respond swiftly to threats and risks to the Personal Information and health records of the class members in storage, in use and during transmission.

49. The Defendants', contrary to their Terms of Service and the Privacy Policy and contrary to the Industry Standards, failed to implement and operationalize adequate cyber defence and security capabilities to detect, deter, and counter hostile and adversarial actions against the Personal Information and health records of the class members in storage, in use and during transmission.

50. The hacker(s) have been in possession of the Plaintiffs' and the Class Members' Personal Information and data since October 28, 2019, or earlier. It is reasonably likely that the hacker(s) have released all or part of the said Personal Information and data online, or sold or distributed it to others who have or will in the future monetize it or release it publicly.

51. The Plaintiffs and the Class Members are therefore obliged to take all reasonable steps necessary to protect their information including hours of wasted time and inconvenience involved in applying for identity theft protection services, changing passwords, notifying financial institutions and applying for new social insurance numbers from Service Canada, as well as the humiliation and mental distress of having lab tests results released without their consent.

52. To the extent criminals rely on the Plaintiffs' and the Class Members' Personal Information and data to secure credit cards and/or conduct fraudulent financial transactions, the Class Members will experience damage to their credit reputation and wasted time and inconvenience responding to the losses.

53. The Defendants retained outside cybersecurity consultants to investigate the breach and assist with restoring the security of the exposed data. The Defendants paid the ransom to the cybercriminals responsible for the hack.

54. In or about December 2019, CEO and President of LifeLabs, Charles Brown, issued an apology statement titled "An Open Letter to LifeLabs Customers", offering concerned customers one free year of protection that includes dark web monitoring and identity theft insurance.

55. To date, the Defendants have not directly notified the Class Members of the breach or arranged for the Class Members to receive protection services including identity theft insurance.

Causes of Action

56. In pleading all causes of action, the Plaintiffs rely on the common law of Ontario. The Plaintiffs also rely on the laws of other provinces in respect of the Class Members who provided personal and confidential information in those provinces. For the purposes of the causes of action pleaded herein, the Plaintiff and the Class Members plead that those laws are the same as the law of Ontario and will be assumed by the Plaintiff and the Class Members to be the same at trial except where otherwise stated herein.

Directors and Officers Liability

57. The directors and officers are personally liable since in their direct supervisory roles they breached their duty to safeguard and protect the Personal Information of the Defendants' customers and monitor the operations of LifeLabs.

58. The directors and officers failed to adequately oversee the cybersecurity of LifeLabs before a breach and/or failed to appropriately oversee the organization's disclosure, investigation, and remediation efforts after the breach.

59. Given the nature of the business of the Defendants, the danger or risk of loss of data to Canadians was or should have been readily apparent to the directors and officers, including and not limited to the length of time not having the data encrypted that was or should have been apparent to the directors and officers, who had the authority and ability to control the situation and had ready access to the means in order to rectify the danger.

60. The directors and officers also had a fiduciary duty to the Class Members, who were vulnerable, and the Defendants failed to honour such fiduciary duty. The directors and officers breached their fiduciary duties including their duty to exercise the care, diligence, and skill of a reasonably prudent person in comparable circumstances.

Negligence

61. The Defendants owed a duty of care to the Class Members in their collection, use and storage of the Personal Information, to keep the Personal Information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons.

62. Specifically, the Defendants owed a duty of care to the Class Members to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and to limit the exposure of the said Personal Information in the event of a successful cyberattack.

63. There was a sufficient degree of proximity between the Class Members and the Defendants to establish a duty of care:

a) it was reasonable for the Plaintiffs and other the Class Members to expect that the Defendants had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their Personal Information in case of a cyberattack;

b) it was reasonably foreseeable that, if a cyberattack resulted in the extraction, theft or exfiltration of the Class Members' Personal Information, the Class Members would sustain damages;

c) it was reasonably foreseeable to the Defendants that, if they failed to take appropriate security measures to protect the Personal Information, there was a risk that the Class Members' privacy would be breached, because of the sensitive nature of the data stored and the increasing number of cyberattacks targeted toward companies which collect and store such sensitive information;

d) it was reasonably foreseeable, and the Defendants knew or ought to have known of the great risks to the Plaintiffs and the Class Members because of the numerous major data breaches in the past: 21st Century Oncology, 2016; Accendo Insurance Co., 2011; Adobe Inc., 2019; Adobe Systems, 2013; Advocate Medical Group, 2013; AerServ (subsidiary of InMobi), 2018; Affinity Health Plan, Inc., 2009; Air Canada, 2018; Amazon Japan G.K., 2019; Ameritrade, 2005; Ancestry.com, 2015; Ankle & Foot Center of Tampa Bay, Inc., 2010; Anthem Inc., 2015; AOL, 2004, 2006, 2014; Apple Health Medicaid, 2016; Apple, 2013; Apple, Inc./BlueToad, 2012; Ashley Madison, 2015; AT&T, 2008, 2010; Auction.co.kr, 2008; Australian Immigration Department, 2015; Australian National University, 2019; Automatic Data Processing, 2005; AvMed, Inc., 2009; Bailey's Inc., 2015; Bank of America, 2005; Barnes & Noble, 2012; Bell Canada, 2017, 2018; Betfair, 2010; Bethesda Game Studios, 2011, 2018; Blank Media Games, 2018; Blizzard Entertainment, 2012; BlueCross BlueShield of Tennessee, 2009; BMO and Simplii, 2018; British Airways, 2015, 2018; Bulgarian Revenue Agency 2019, 2019; California Department of Child Support Services, 2012; Canva, 2019; Capital One, 2019; CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express), 2005; CareFirst BlueCross Blue Shield - Maryland, 2015; Cathay

Pacific Airways, 2018; Centers for Medicare & Medicaid Services, 2018; Central Coast Credit Union, 2016; Central Hudson Gas & Electric, 2013; CheckFree Corporation, 2009; China Software Developer Network, 2011; Chinese gaming websites (Duowan, 7K7K, 178.com), 2011; Citigroup, 2005, 2011, 2013; City and Hackney Teaching Primary Care Trust, 2007; Colorado Government, 2010; Community Health Systems, 2014; Compass Bank, 2007; Countrywide Financial Corp, 2006, 2011; Cox Communications, 2016; Crescent Health Inc., Walgreens, 2013; CVS (PNI Digital Media), 2015; Dai Nippon Printing, 2007; Data Processors International (MasterCard, Visa, Discover Financial Services and American Express), 2008; Defense Integrated Data Center (South Korea), 2017; Deloitte, 2017; Democratic National Committee, 2016; Desjardins, 2019; Domino's Pizza (France), 2014; DoorDash, 2019; Dropbox, 2012; Drupal, 2013; DSW Inc., 2005; Dun & Bradstreet, 2013; Earl Enterprises (Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy, Mixology, Tequila Taqueria), 2018; eBay, 2014; Educational Credit Management Corporation, 2010; Eisenhower Medical Center, 2011; Embassy Cables, 2010; Emergency Healthcare Physicians, Ltd., 2010; Emory Healthcare, 2012; Equifax, 2017; European Central Bank, 2014; Evernote, 2013; Excellus BlueCross BlueShield, 2015; Experian - T-Mobile US, 2015; EyeWire, 2016; Facebook three times in 2019, also in 2018 and 2013; Federal Reserve Bank of Cleveland, 2010; Fidelity National Information Services, 2007; First American Corporation, 2019; Florida Department of Juvenile Justice, 2013; Formspring, 2012; Friend Finder Networks, 2016; Gamigo, 2012; Gap Inc., 2007; Gawker, 2010; Global Payments, 2012; Gmail, 2014; Google Plus, 2018; Greek Government, 2012; Grozio Chirurgija, 2017; GS Caltex, 2008; Gyft, 2016; Hannaford Brothers Supermarket Chain, 2007; HauteLook, 2018; Health Net - IBM, 2011, 2009; Health Sciences Authority (Singapore), 2019; Heartland, 2009; Heathrow Airport, 2017; Hewlett Packard, 2006; Hilton Hotels, 2014; Home Depot, 2014; Honda Canada, 2011; Hyatt Hotels, 2015; Internal Revenue Service, 2015; Inuvik hospital, 2016; Iranian banks (Saderat, Eghtesad Novin, and Saman), 2012; Jefferson County, West Virginia, 2008; JP Morgan Chase, 2010, 2014; Justdial, 2019; KDDI, 2006; Kirkwood Community College, 2013; KM.RU, 2016; Korea Credit Bureau, 2014; Kroll Background America, 2013; KT Corporation, 2012; Landry's, Inc., 2015; LexisNexis, 2014; Lincoln Medical & Mental Health Center, 2010; LinkedIn, eHarmony,

Last.fm, 2012; Living Social, 2013; MacRumors.com, 2014; Mandarin Oriental Hotels, 2014; Marriott International, 2018; Massachusetts Government, 2011; Massive American business hack including 7-Eleven and Nasdaq, 2012; Medical Informatics Engineering, 2015; Memorial Healthcare System, 2011; Michaels, 2014; Militarysingles.com, 2012; Ministry of Education (Chile), 2008; Ministry of Health (Singapore), 2019; Mobile TeleSystems (MTS), 2019; Monster.com, 2007; Morgan Stanley Smith Barney, 2011; Mozilla, 2014; MyHeritage, 2018; NASDAQ, 2014; National Archives and Records Administration (U.S. military veterans records), 2009; National Guard of the United States, 2009; Natural Grocers, 2015; Neiman Marcus, 2014; Nemours Foundation, 2011; Network Solutions, 2009; New York City Health & Hospitals Corp., 2010; New York State Electric & Gas, 2012; New York Taxis, 2014; Nexon Korea Corp, 2011; NHS, 2011; Nintendo, 2013; Nival Networks, 2016; Norwegian Tax Administration, 2008; Ofcom, 2016; Office of the Texas Attorney General, 2012; Ohio State University, 2010; Orbitz, 2018; Oregon Department of Transportation, 2011; OVH, 2013; Patreon, 2015; Philippines Commission on Elections, 2016; Popsugar, 2018; Premera, 2015; Puerto Rico Department of Health, 2010; Quest Diagnostics, 2019; Quora, 2018; Rambler.ru, 2012; RBS Worldpay, 2008; Reddit, 2018; Restaurant Depot, 2011; RockYou!, 2009; Rosen Hotels, 2016; San Francisco Public Utilities Commission, 2011; Scottrade, 2015; Scribd, 2013; Seacoast Radiology, PA, 2010; Sega, 2011; Service Personnel and Veterans Agency (UK), 2008; SingHealth, 2018; Slack, 2015; SnapChat, 2013; Sony Online Entertainment, 2011; Sony Pictures, 2011, 2014; Sony PlayStation Network, 2011; South Africa Police, 2013; South Carolina Government, 2012; South Shore Hospital, Massachusetts, 2010; Southern California Medical-Legal Consultants, 2011; Spartanburg Regional Healthcare System, 2011; Stanford University, 2008; Starbucks, 2008; Starwood Hotels including Westin Hotels and Sheraton Hotels, 2015; State of Texas, 2011; Steam, 2011; StockX, 2019; Stratfor, 2011; Supervalu, 2014; Sutter Medical Center, 2011; Syrian government (Syria Files), 2012; Taobao, 2016; Target Corporation, 2013; Taringa!, 2017; TaxSlayer.com, 2016; TD Ameritrade, 2007; TD Bank, 2012; TerraCom & YourTel, 2013; Texas Lottery, 2007; The Bank of New York Mellon, 2008; Tianya Club, 2011; Ticketfly (subsidiary of Eventbrite), 2018; TK / TJ Maxx, 2007; T-Mobile, Deutsche Telekom, 2006; Tricare, 2011; Triple-S Salud, Inc., 2010; Truecaller,

2019; Trump Hotels, 2014; Tumblr, 2013; Twitch, 2015; Twitter, 2013; Typeform, 2018; U.S. Army, 2010, 2011; U.S. Department of Defense, 2009; U.S. Department of Veteran Affairs, 2006; U.S. Government (United States diplomatic cables leak), 2010; U.S. law enforcement (70 different agencies), 2011; Uber, 2014, 2016; Ubisoft, 2013; Ubuntu, 2013; UCLA Medical Center, Santa Monica, 2015; UK Driving Standards Agency, 2007; UK Home Office, 2008; UK Ministry of Defence, 2008; UK Revenue & Customs, 2007; Under Armour, 2018; United States Postal Service, 2018; Universiti Teknologi MARA, 2019; University of California, Berkeley, 2009, 2016; University of Central Florida, 2016; University of Maryland, College Park, 2014; University of Miami, 2008; University of Utah Hospital & Clinics, 2008; University of Wisconsin–Milwaukee, 2011; UPS, 2014; US Department of Homeland Security, 2016; US Medicaid, 2012; US Office of Personnel Management, 2015; Verizon Communications, 2016; Virginia Department of Health, 2009; Virginia Prescription Monitoring Program, 2009; Vodafone, 2013; VTech, 2015; Walmart Canada (PNI Digita Media), 2015; Washington Post, 2011; Washington State court system, 2013; Weebly, 2016; Wendy's, 2015; Westpac, 2019; Woodruff Arts Center, 2019; WordPress, 2018; Writerspace.com, 2011; Xat.com, 2015; Yahoo Japan, 2013; Yahoo! Voices, 2012; Yahoo, 2013, 2014; Yale University, 2010; Zappos, 2012; and Zynga, 2019;

e) the Class Members were vulnerable to the Defendants, and relied on them to take appropriate security measures to protect their Personal Information;

f) the Defendants, through their Terms of Service and their Privacy Policy, promised to take appropriate measures to protect the Class Members' Personal Information;

g) there is a sufficient degree of proximity between the Class Members and the Defendants because the Class Members are, or were, customers of the Defendants and received diagnostic testing services from the Defendants;

h) the Defendants were required by sections 4.1, 4.5 and 4.7 of Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (the "**PIPEDA**"),

to implement safeguards appropriate to the sensitivity of the information stored on their network;

i) the Defendants were required by section 12 of the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A to take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal; and

j) there was a contractual relationship between the Class Members and the Defendants.

64. The Defendants were negligent and failed in their duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, and/or securing the Class Members' Personal Information. Without limiting the generality of the foregoing, the particulars of gross negligence include:

a) failing to handle the collection, retention, security and disclosure of the Class Members' Personal Information in accordance with the Privacy Policy;

b) failing to designate, hire and/or properly train and/or supervise individuals responsible and accountable for network security management, including compliance internal policies and legislation in its collection, storage, protection and destruction of the Personal Information, contrary to s. 4.1 of Schedule 1 to the PIPEDA;

c) allowing the Personal Information to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to the PIPEDA;

d) failing to implement appropriate physical, organizational and technological safeguards to protect the Personal Information against loss, theft, unauthorized access, disclosure,

copying, use, and/or modification, as particularized in contrary to s. 4.7 of Schedule 1 to the PIPEDA;

e) failing to keep the Class Members' Personal Information secure and confidential;

f) storing the Class Members' Personal Information on an unsecured network and server(s);

g) failing to encrypt the Personal Information on their servers, exposing and enhancing the vulnerability of the exfiltration of the Class Members' data;

h) failing to implement any, or adequate, cyber-security measures, programs, safeguards and internal controls to protect the Personal Information and health records of the Class Members from loss, theft, unauthorized access, unauthorized use, unauthorized duplication and/or unauthorized disclosure,

i) failing to protect the Class Members' Personal Information from compromise, disclosure, and/or theft;

j) failing to take steps to prevent the Class Members' Personal Information from being disseminated or disclosed to the public;

k) failing to notify the Class Members of the breach and failing to provide sufficient information to allow the Class Members to understand the significance of the breach to them and to take steps, if any are possible, to reduce the risk of harm or mitigate the harm that could result from the breach. At the time of pleading there has been no program implemented to provide direct notice to the Class Members of the breach.

65. As a result of these Defendants' negligence, the hacker(s) were able to gain access to the Class Members' Personal Information, resulting in the Class Members sustaining damages.

66. The Plaintiffs state that as a result of the Defendants' negligence, the Defendants are jointly and severally liable with the hacker for the intentional privacy torts as pleaded below. The Plaintiffs pleads and relies on the *Negligence Act,* R.S.O. 1990, c.N.1 section 1 and the *Negligence Act* [RSBC 1996] Chapter 333 section 4(2)(a).

Breach of Contract/Warrant

67. The Plaintiffs and the Class Member entered into identical or very similar contracts with the Defendants when using the Defendants' services.

68. In exchange for agreeing that the Defendants collected, used and stored the Class Member's Personal Information, customers were provided with diagnostic medical lab testing services and online access to their test results.

69. The provisions of the Privacy Policy in LifeLabs Terms of Service are pleaded in the Fact Section of the Claim.

70. The Defendants had a contractual obligation to maintain confidentiality over the Personal Information they collected from the Plaintiffs and the Class Members, which they stored on their internal computer network, to secure the aforesaid Personal Information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated customer Personal Information, in accordance with their own privacy policies, applicable laws and the Industry Standards. The Defendants breached their contracts with the Plaintiffs and the Class Members by failing to comply with the terms of service and privacy policy resulting in unauthorized access.

71. The Defendants warranted to the Plaintiffs and the Class Members, through its Privacy Policy that it was committed to protecting their privacy. The Defendants breached their warranty by failing to make reasonable efforts to protect the Class Members' Personal Information, resulting in unauthorized access.

72. The Defendants had an express or alternatively implied contractual obligation to comply with applicable privacy legislation including PIPEDA and to manage private information in a manner that was consistent with the principles that are reflected in such legislation. By promising to comply with the applicable privacy legislation in its Privacy Policy and Terms of Service the Defendants also incorporated the legislation into the contract and have therefore breached its contract with the Class Members by failing to comply with the applicable privacy legislation.

Breach of Contractual Duties of Honesty, Good Faith & Fair Dealing

73. The Defendants had a contractual duty to act honestly and in good faith. At a minimum, the Defendants were required to make reasonable efforts to maintain confidentiality over the Personal Information they collected from the Plaintiffs and the Class Members and stored on their internal computer network and to secure said information against risks of unauthorized access, collection, use, disclosure and copying.

74. The Defendants represented through the Privacy Policy that it had established reasonable security safeguards for the Personal Information of the Plaintiffs and the Class Members. The Defendants knew or ought to have known that the Personal Information provided by the Class Members was highly sensitive and that the Class Members relied on the Defendants to secure said information.

75. The Defendants breached their duties of honesty, and good faith and fair dealing by failing to take reasonable steps to secure the information stored on its network when it promised and made assurances that it had done so.

Breach of Confidence

76. The Class Members were required to provide the Personal Information to the Defendants in exchange for services, which was then stored electronically on its internal network.

77. The Class Members' Personal Information was confidential, sensitive and not public knowledge, exhibiting the necessary qualities to require confidence.

78. The Class Members' Personal Information was imparted to the Defendants in circumstances in which an obligation of confidence arose, and in which the Plaintiffs and the Class Members could have reasonably expected their sensitive information to be protected and secured.

79. The Defendants made unauthorized use of the Class Members' Personal Information by failing to make reasonable efforts to maintain its confidentiality, secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated information, in accordance with the Defendants' own privacy policies, applicable laws and the Industry Standards. The Defendants' aforesaid unauthorized use violated the PIPEDA, including sections 4.1, 4.5 and 4.7 of Schedule 1 to that legislation.

80. The Defendants' misuse resulted in unauthorized access and public disclosure of the private information to the detriment of the Class Members. The Defendants are therefore liable for the tort of breach of confidence.

Intrusion Upon Seclusion

81. The Defendants were responsible for collecting, managing, storing and/or securing the Class Members' private information.

82. The Defendants failed to take appropriate measures to safeguard the Class Members' Personal Information as detailed in the particulars of negligence plead above, and as such are, together with the hacker(s), liable for intrusion upon seclusion.

83. The hacker(s) intentionally invaded the Class Members' privacy. The Defendants' tortious conduct or alternatively, recklessness, facilitated the hacker(s)' ability to invade the Class Members' privacy.

84. The Class Members' privacy was invaded without lawful jurisdiction of the Class Members' private affairs or concerns.

85. The Personal Information invaded is of highly sensitive and personal natures that a reasonable person would consider its invasion to be highly offensive, causing anguish, humiliation or distress.

Public disclosure of private information

86. By their decision to utilize inadequate security measures to safeguard the Class Members' private information, the Defendants, in effect, publicized private aspects of the Class Members' private life, by making the private information available to hackers and others;

87. The Plaintiffs and the Class Members did not consent to having the private information accessible and publicized by the Defendants;

88. The publication of the private information by the Defendants that the hackers accessed would be highly offensive to a reasonable person.

89. The publication of the private information of the Plaintiffs and the Class Members by the Defendants was not of a legitimate concern to the public.

Breach of Provincial Privacy Statutes

90. The Plaintiffs rely on the following statutory claims on behalf of the Class Members who are domiciled in or are residents of the Provinces of British Columbia that the Defendants without a claim of right, willfully violated the privacy of the British Columbia Class Members, violating the *Privacy Act*, RSBC 1996, c. 373, as amended (section 1).

91. The Plaintiffs rely on the following statutory claims on behalf of the Class Members who are domiciled in or are residents of other provinces in Canada that the Defendants without a claim of right, willfully violated the privacy of these provinces' Class Members, violating the *Privacy Act*, CCSM c.P125, as amended (section 2) for Manitoba, *Privacy Act*, RSS 1978, c. P-24, as amended 1996; (section 2) for Saskatchewan; *Privacy Act*, RSNL 1990, c. P-22, as amended; (section 3) for Newfoundland & Labrador; articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c. CCQ-1991, as amended, and section 5 of the *Charter of Human Rights and Freedoms*, CQLR C. C-12, as amended for Quebec.

92. The Plaintiffs plead that 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. and rely on *Privacy Act*, RSBC 1996, c. 373, as amended (section 1) for British Columbia; *Privacy Act*, CCSM c.P125, as amended (section 2) for Manitoba; *Privacy Act*, RSNL 1990, c. P-22, as amended; (section 3) for Newfoundland & Labrador; and *Privacy Act*, RSS 1978, c. P-24, as amended 1996; (section 2) for Saskatchewan.

Breach of Applicable Consumer Protection Legislation

93. The Defendants are subject to the provisions of the Ontario *Consumer Protection Act* because it entered into consumer contracts with individuals resident in Ontario. By misrepresenting to the Plaintiffs and the Class Members that their Personal Information would be secure, the Defendants breached the Ontario *Consumer Protection Act*.

94. The Defendants are also subject to the provisions of the *British Columbia Business Practices and Consumer Protection Act*, [SBC 2004] because it entered into consumer contracts with individuals resident in British Columbia. The Plaintiffs and the British Columbia Class Members each entered into consumer agreements or conducted consumer transactions with the Defendants.

95. Similarly, the Class Members residents in other provinces entered into consumer contracts with the Defendants pursuant to the consumer protection legislation in their provinces.

96. The Defendants are subject to the obligations of the Applicable Consumer Protection Legislation, which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices. The Defendants' failure to take reasonable measures to secure the Personal Information and data constitutes a prohibited practice because the Defendants made false and misleading representations to the Class Members in relation to their security measures. Without limiting the generality of the foregoing, the particulars of which are as follows:

    (a) at the times that the Class Members used the Defendants' services, the Defendants represented that they would comply with their own privacy policy and the PIPEDA, and protect the Class Members' privacy, including their Personal Information and the information contained in their Accounts; and

    (b) the Defendants failed to disclose to the Class Members that their security measures were inadequate to secure the privacy of their Personal Information.

Unjust Enrichment by Wrongdoing – Waiver of Tort

97. The Plaintiffs and the Class Members claim unjust enrichment by wrongdoing *per se*, a form of claim that has been referred to as " waiver of tort". A claim for unjust enrichment is made without reliance on proof of loss or damages to class members, but on the basis of wrongdoing by the Defendants that have been unjustly enriched by operating their business without establishing adequate security safeguards in collecting, managing, storing, and/or securing the Class Members' Personal Information.

98. Given the conduct of the Defendants as outlined above, this is an appropriate case for disgorgement of profits, which the Defendants obtained by employing the methods of

collection, usage, retention, storage and disclosure of the Personal Information of their customers, by the way of waiver of tort and fiduciary obligations.

Damages

99. The Plaintiffs on their behalf of the Class Members claim non-pecuniary damages on an aggregate basis in the amount of $1,130,000,000.00.

100. The Plaintiffs also claim compensatory damages on behalf of each Class Member who has suffered an actual loss as a result of the privacy breach.

101. Additionally, the Class Members have suffered or will likely suffer further damages from identity theft and/or fraud in the event that the Personal Information was or becomes publicly available on the internet and may be downloaded and used for criminal purposes. There is a real and substantial risk that the Personal Information may be released on the internet or used in the future for criminal purposes, thereby causing the Class Members to suffer damages.

Punitive Damages

102. The Defendants were, at all times, aware that their actions would have a significant adverse impact on the Class Members. The Defendants' conduct was negligent, highhanded, reckless, without care, deliberate, and in disregard of the Class Members' rights and interests.

103. The Plaintiffs seek substantial punitive damages in light of the grave harm and risk that the Defendants caused and the conduct of the Defendants.

Symbolic or Moral Damages to Be Assessed in Aggregate

104. Every Class Member's privacy was breached in the same way: the Personal Information was exfiltrated from the Defendants' servers and the Defendants are liable for the breach that occurred.

105. The Plaintiffs seek to assess symbolic or moral damages in whole or in part in the aggregate as a common base amount to be awarded to every class member relating to exfiltration of the Plaintiffs' Personal Information from the Defendants' servers.

Common Issues

106. The Plaintiffs seek that the following common issues be certified:

a) the Defendants are liable for breach of fiduciary duty to the Plaintiffs and the Class members;

b) the Defendants are liable for breach of the duty and standard of care;

c) the Defendants are liable for negligence;

d) the Defendants are liable for gross negligence;

e) the Defendants are liable for breach of contract with the Plaintiffs and the Class Members;

f) the Defendants intruded upon seclusion of the Plaintiffs and the Class Members or, in the alternative, are jointly and severally liable for intruding upon seclusion of the Plaintiffs and the Class Members;

g) the Defendants are liable for the breach of the confidence of the Plaintiffs and the Class Members;

h) the Defendants are liable for the violation of provincial and territorial consumer protection legislation;

i) the Defendants are liable for the breach of statutory privacy rights of the Plaintiffs and the Class Members;

j) the Defendants are liable for the unjust enrichment, waiver of tort as a cause of action;

k) assessment of symbolic or moral damages in whole or in part in the aggregate;

l) entitlement to punitive damages; and

m) such further and other common issues as counsel may advise and this Honourable Court may permit.

Relevant Statutes

107. The Plaintiffs plead and rely upon the *CPA*, the *PIPEDA*, the *Personal Health Information Protection Act*, the *Negligence Act*, R.S.O. 1990, c.N.1, Ontario *Consumer Protection Act S.O. 2002 c.30*, the British Columbia *Business Practices and Consumer Protection Act* SBC 2004 Chapter 2, the British Columbia *Privacy Act* RSBC 1996, c. 373, and the applicable consumer protection and privacy legislation of the Provinces.

Service Outside of Ontario

108. The Plaintiffs plead that the Statement of Claim may be served on Defendants outside of Ontario without a court order pursuant to Rule 17.02 of the *Ontario Rules of Civil Procedure*. The Plaintiffs plead that the proceedings have a real and substantial connection with Ontario because:

a) the Plaintiffs are residents of Ontario;

b) the Defendants carry on business in Ontario;

c) the Defendants have corporate headquarters in Ontario;

d) contracts relating to the subject matter of this action were made in Ontario;

e) the torts pleaded in the sections above were committed in Ontario;

f) the Class Members' Personal Information was transmitted in and through Ontario; and

g) a significant number of the Class Members reside in Ontario.

Place of Trial

109. The Plaintiffs propose that this action be tried at the City of Toronto.

December 27, 2019

Peter I. Waldmann Professional Corporation
183 Augusta Avenue
Toronto, Ontario M5T 2L4

Peter I Waldmann (LSO #23289M)
Tel: (416) 921-3185
Fax: (416) 921-3183
Email: peter@peteriwaldmann.com

Stein Law Office
1400-330 Bay Street
Toronto, Ontario M5H 2S8

Andrew Stein (LSO #32065K)
Tel: (416) 642-2020
Fax: (416) 203-9456
Email: astein@andrewsteinlaw.com

Lawyers for the Plaintiffs