AMENDED THIS February 9/22 PURSUANT TO
MODIFIÉ CE CONFORMÉMENT À
☐ RULE/LA RÈGLE 26.02 (_____)
☒ THE ORDER OF Justice Belobaba
L'ORDONNANCE DU
DATED / FAIT LE February 3, 2022
RL GISTRAR GREFFIER
SUPERIOR COURT OF JUSTICE COUR SUPÉRIEURE OF JUSTICE

Court File No: CV-20-006-36642-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

ALITA MARIE CARTER,
ANNA BELLE THARANI, and ALBERT OTOTÉ

Plaintiffs

-and-

LIFELABS INC., LIFELABS BC INC.,
LIFELABS BC LP, and LIFELABS LP

Defendants

FRESH AS AMENDED STATEMENT OF CLAIM

Proceeding under the *Class Proceedings Act, 1992*

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 THE 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 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 serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGEMENT 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 FEEDS, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

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 this court.

~~Date: February 20, 2020~~
Date: February 24, 2021

Issued by:_____

Local Registrar
330 University Avenue, 8th Floor
Toronto, Ontario M5G 1R8

TO: **LIFELABS INC.**
100 International Boulevard
Toronto, ON M9W 6J6

AND TO: **LIFELABS BC INC.**
3680 Gilmore Way
Burnaby, BC V5G 4V8
Canada

AND TO: **LIFELABS LP**
100 International Boulevard
Toronto, Ontario M9W 6J6

AND TO: **LIFELABS BC LP**
100 International Boulevard
Toronto, Ontario M9W 6J6

RELIEF SOUGHT

1. The Plaintiffs, on their own behalf and on behalf of the Class Members, seek the following relief:

   (a) An order certifying this action as a class proceeding pursuant to the *Class Proceeding Act, 1992*, S.O. 1992, c. 6, as amended ("*CPA*");

   (b) An order appointing the Plaintiffs as representative plaintiffs for the Class;

   (c) Declarations that:

      (i) the Defendants owed a duty of care to the Plaintiffs and Class Members in the handling, storage, and protection of their Personal Information, as defined herein;

      (ii) the Security Breach, as defined herein, was a result of the Defendants breaching the standard of care required of them;

      (iii) the Defendants breached their contracts with the Plaintiffs and Class Members and breached contracts to which the Plaintiffs and the Class Members were third party beneficiaries, which resulted in the Security Breach;

      (iv) the Defendants breached the common law privacy rights and intruded upon the seclusion of the Plaintiffs and Class Members;

      (v) the Defendants breached the statutory privacy and personal information protection rights of the Plaintiffs and Class Members;

      (vi) the Defendants were unjustly enriched, to the deprivation of the Plaintiffs and the Class Members;

      (vii) the Defendants are jointly and severally liable with each other and with the Cyberattackers for the damages suffered by the Plaintiffs and Class Members;

(viii) the Defendants violated the *Consumer Protection Act, 2002*, SO 2002, c 30, Sch. A; the *Business Practices and Consumer Protection Act*, SBC 2004, c 2; the *Consumer Protection Act*, RSA 2000, c. C-26.3, the *Consumer Protection and Business Practices Act*, SS 2013, c C-30.2; the *Consumer Protection Act*, CQLR c P-40.1; the *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1; *Consumer Product Warranty and Liability Act*, S.N.B. 1978, c. C-18.1; *Sale of Goods Act*, R.S.N.B. 2016, c. 110; *Business Practices Act*, R.S.P.E.I. 1988, c. B-7; and the *Consumer Protection Act*, R.S.P.E.I. 1988, c. C-19 (the "Applicable Consumer Protection Legislation")

(d) pursuant to s. 24 of the *CPA*, an aggregate assessment of monetary relief, including nominal damages, and directions for distribution of the aggregate damages to the Plaintiffs and Class Members;

(e) general and special damages in an amount to be fixed by the Court;

(f) punitive and aggravated damages;

(g) disgorgement of the Defendants' profits;

(h) damages pursuant to section 65 of *Personal Health Information Protection Act*, 2004 S.O. 2004, c.3, section 57(1) of the *Personal Information Protection Act* SBC 2003 c. 63; section 60(1) of the *Personal Information Protection Act*, SA 2003, c. P-6.5; and section 16(c) of the *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5);

(i) pursuant to s. 25 of the *CPA,* a direction for individual hearings, inquiries, and determinations for any issues not determined at the trial of the common issues;

(j) 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. C. 43, as amended;

(k) costs of this action on a substantial indemnity basis plus HST or in an amount that provides full indemnity to the Plaintiffs;

(l) the costs of administering the plan of distribution of the recovery in this action; and,

(m) Such further and other relief as this Honourable Court may deem just.

OVERVIEW

2. LifeLabs is Canada's largest provider of medical laboratory testing and analytic and diagnostic services, including medical information and digital health connectivity services ("the Services").

3. LifeLabs provides the Services at a high volume, each year conducting over 100 million laboratory tests in the course of approximately 20 million patient visits facilitated by approximately 5700 employees and leading edge testing, analytic and diagnostic technologies.

4. The Services are provided with the objective of enabling patients and their health care providers to diagnose, treat, monitor and prevent disease.

5. In providing the Services, LifeLabs operates Canada's largest online health portal, with more than 2.3 million customers accessing their laboratory tests results online annually.

6. Through its provision of the Services, LifeLabs generates substantial revenue and profit, the bulk of which is publicly funded.

7. In the course of providing the Services, LifeLabs collected, created, used, and stored a vast amount of confidential personal information about its customers, including names, addresses, email addresses, user identification, passwords,

dates of birth, health care numbers, health provider names, gender, phone numbers, security questions and answers, Internet Protocol addresses, and information about login attempts ("Personal Identity Information").

8. In the course of providing the Services, LifeLabs also collected, created, used, and stored a vast amount of confidential personal health information about its customers' physical health, including requisitions for and results of laboratory testing, information about diseases, and past and current medical conditions, syndromes or disabilities ("Personal Health Information").

9. Personal Identity Information and Personal Health Information are referred to collectively in this statement of claim as "Personal Information".

10. As a large medical company operating in today's digital world, LifeLabs should have had effective, updated cybersecurity in place to secure the nearly unprecedented amount of Personal Information in its possession.

11. In fact, under its contracts with the British Columbia Ministry of Health, LifeLabs agreed that privacy is critically important, that its services to the BC class members would be delivered with the utmost care for confidential and personal information, and that LifeLabs would comply with all Provincial privacy, security and confidentiality standards. Dr. Ototé, Ms. Tharani, and any class members who received services from LifeLabs that were paid for by the British Columbia Ministry of Health are third party beneficiaries to these agreements, which were made for the benefit of these class members.

12. In reality, LifeLabs employed inadequate and ineffective cybersecurity, and it did not deliver its services with the utmost care for confidential and personal information, which resulted in criminal hackers (the "Cyberattackers") gaining access to LifeLabs' computer network (the "Computer Systems"). The Cyberattackers were able to gain access to the Computer Systems because the defendants knowingly or recklessly failed to take steps to protect Personal Information in its electronic systems, failed to have adequate IT securities policies

in place, and collected more Personal Information than was reasonably necessary. As a result, in 2019, the Cyberattackers were able to access without authorization, and to extract, the Personal Information of as many as 15 million Canadians (the "Security Breach"), giving rise to a breach of the proposed Class Members' privacy rights.

Class Definition

13. The Plaintiffs bring this action on behalf of:

    (a) all Canadian resident customers or patients of LifeLabs whose Personal Information was stored on computer systems in the control of LifeLabs that were compromised or accessed by unauthorized persons in the Security Breach announced by LifeLabs on December 17, 2019; and,

    (b) a subclass of all customers or patients of LifeLabs whose test requisitions or test results were accessed by unauthorized persons in the Security Breach.

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

Plaintiffs

14. Alita Marie Carter is an individual residing in Toronto, Ontario. Ms. Carter is a customer of LifeLabs, having obtained medical diagnostic laboratory testing services from LifeLabs on numerous occasions since approximately 1982.

15. LifeLabs collected, used and disclosed Ms. Carter's Personal Information.

16. At all material times, Ms. Carter's Personal Information was stored on the Computer Systems and her Personal Information was affected by the Security Breach.

17. LifeLabs did not notify Ms. Carter of the Security Breach until mid-January 2020, some two months after LifeLabs first reported the Security Breach to the Office of the Information and Privacy Commissioner of Ontario ("OIC") and the Privacy

Commissioner for British Columbia ("OIPC"), and other provincial privacy commissioners.

18. Anna Belle Tharani is a care aide residing in British Columbia. Ms. Tharani has been a patient of LifeLabs for years.

19. LifeLabs collected, used, and disclosed Ms. Tharani's Personal Information.

20. At all material times, Ms. Tharani's Personal Information was stored on the Computer Systems and they were affected by the Security Breach.

21. Albert Ototé is an individual residing in London, Ontario. Dr. Ototé has been a customer of LifeLabs since 2015. He registered with LifeLabs' online appointment booking system in 2015.

22. Dr. Ototé received services from LifeLabs paid for by the Ontario Health Insurance Plan. He also received services from LifeLabs that he paid for himself.

23. LifeLabs collected, used, and disclosed Dr. Ototé's Personal Information.

24. At all material times, Dr. Ototé's Personal Information was stored on the Computer Systems and they were affected by the Security Breach.

Defendants

25. LifeLabs Inc. is a corporation incorporated under the *Canada Business Corporations Act*. It has a registered office in Toronto. In addition to operating under its own name, LifeLabs does business as Rocky Mountain Analytical and LifeLabs Genetics.

26. LifeLabs LP is a limited partnership established under the laws of Ontario. It has a registered office in Toronto. LifeLabs Inc. is the general partner of LifeLabs LP.

27. LifeLabs BC Inc. is a corporation incorporated in British Columbia with a registered office in Vancouver.

28. LifeLabs BC LP is a limited partnership established under the laws of Ontario. It has registered office in Toronto. It is registered as an extra-provincial limited partnership in British Columbia. LifeLabs BC Inc. is the general partner of LifeLabs BC LP.

29. LifeLabs Inc., LifeLabs LP, LifeLabs BC Inc., LifeLabs BC LP (collectively "LifeLabs"), are in the business of medical testing. LifeLabs performs medical diagnostic tests and makes customers' Personal Information available online to customers and their healthcare providers.

30. Excelleris Technologies Inc. was a wholly owned subsidiary of LifeLabs Inc. incorporated under the laws of British Columbia. It had a registered office in Vancouver, with an extra-provincial registration in Ontario.

31. In January 2021, LifeLabs BC Inc. and Excelleris Technologies Inc. amalgamated into one company under the name LifeLabs BC Inc. LifeLabs BC Inc. is liable for any acts, omissions, or contractual obligations of Excelleris Technologies Inc.

32. Excelleris Technologies Inc. provided information technology services that supported LifeLabs. While LifeLabs collected and generated personal health information, Excelleris was the vehicle by which that information was stored and disclosed.

33. Excelleris Technologies LP was a limited partnership established under the laws of British Columbia that was dissolved in January 2021. Excelleris Technologies Inc. was the general partner in Excelleris Technologies LP. LifeLabs BC Inc. is liable for any actions, omissions, or contractual obligations of Excelleris Technologies LP. Excelleris Technologies Inc. and Excelleris Technologies LP are collectively described as "Excelleris".

34. Each of the Defendants are affiliated in that they are directly or indirectly owned in common.

35. Each of the Defendants is jointly liable and/or vicariously liable for the acts and/or omissions of the others for the following reasons:

(a) each was the agent of the other;

(b) each Defendant's business was operated so that it was inextricably interwoven with the business of the other as one corporate enterprise;

(c) each defendant entered into a common advertising and promotion plan with the other;

(d) each defendant operated pursuant to a common business plan; and,

(e) each defendant intended that the business appear to be operated, and in fact was operated, as one common business organization.

FACTS

Background

36. LifeLabs owns and operates a network of medical testing facilities across Canada, including laboratories and collection centres (collectively, the "LifeLabs Facilities").

37. There are several ways in which a customer or a customer's biomedical sample can come into contact with LifeLabs:

(a) a customer can attend at a collection centre and provide a sample in person;

(b) a customer can provide a sample to LifeLabs' in-home mobile service; or

(c) a customer can provide a sample at a hospital or health clinic, which is then sent to a LifeLabs testing facility.

38. In order for LifeLabs to collect a sample and/or conduct testing, a requisition form must be completed and signed by a medical clinician or practitioner.

39. There are different requisition forms for different types of tests, but each requisition form contains, at a minimum, the following customer Personal Information:

(a) full name;

(b) sex;

(c) address;

(d) phone number(s);

(e) date of birth;

(f) credit card information in some cases; and

(g) health card number.

40. If a customer is attending at a LifeLabs Facility, or is using LifeLabs' mobile service, they are asked to confirm their full name, date of birth, address, and health card number to a LifeLabs employee directly before sample collection.

41. Most LifeLabs requisition forms contain additional Personal Health Information, such as the following:

(a) the name and contact information for the customer's primary care physician;

(b) medical diagnosis information;

(c) health history and risk factors; and

(d) health insurance information.

42. When LifeLabs conducts tests on biomedical samples like blood or urine, the requisition form containing the above information must accompany every sample to be tested, regardless of whether the sample is provided directly to LifeLabs or through another medical facility. Accordingly, LifeLabs collects, retains and stores large amounts of Personal Information of many people who are unaware that their information has been collected and stored by LifeLabs.

43. An account was created by Excelleris for each individual who needed tests to be performed on a biomedical sample. This account contains the information from the customer's requisition form(s) and test result(s), which contains Personal Information, and is accessible to physicians and medical practitioners through a platform named "Launchpad".

44. Launchpad permits practitioners to complete requisition forms electronically, to access patient test results in real time, sort through test content, print reports, etc.

45. Customers could also access their Excelleris accounts through a number of different platforms. For customers who use Ontario- or Saskatchewan-based LifeLabs Facilities, test results could be accessed and reports could be downloaded through the "My Results" platform. In addition, appointments can be booked or confirmed through the "Save My Spot" platform.

46. The "My Results" and "Save My Spot" platforms operate separately—meaning that a customer must set up and access their "My Results" and "Save My Spot" accounts separately—but both platforms operate using and accessing data from one unified underlying Excelleris account per customer.

47. Each of the many access points into the Computer Systems referenced above, along with LifeLab's office management systems was protected inadequately, and each was vulnerable to cyber-breaches. One or more of these access points was used by the Cyberattackers to gain access to the Computer Systems.

48. Most of the tests offered by LifeLabs at their Ontario Facilities are covered by the Ontario Health Insurance Plan, but LifeLabs also offers additional tests which may be covered by private health insurance or are billed to customers directly. Thus, some customers' Excelleris accounts also include credit card payment information.

49. The LifeLabs' website states, in its Terms of Use, that the use of the website is governed by the laws of the Province of Ontario.

50. For customers who use BC-based LifeLabs Facilities, test results could be accessed and appointments could be booked through "my ehealth".

51. All the Personal Information that was collected by LifeLabs was stored in the Computer Systems that were infiltrated by the Cyberattackers in breach of the privacy of all of the Class Members.

52. The defendants were, and are, responsible for safeguarding the Class Members' Personal Information, which was stored electronically on the Computer Systems. To the extent that LifeLabs delegated responsibility for collecting, managing, storing, securing and/or deleting the Class Members' Personal Information to Excelleris, and/or to any other party or parties, LifeLabs is directly or vicariously liable for any resultant damages because LifeLabs has a non-delegable duty to secure the Class Members' Personal Information.

53. As a result of its collection, creation, use, storage, and transmission of Personal Information; and given the sensitivity and value of that data, and the known increase in cyberattacks upon other custodians of personal information, and particularly cyberattacks on healthcare providers, LifeLabs knew or ought to have known that its Computer Systems would be a prime target for criminal activity, including attempts to extract or hold the Personal Information for ransom.

LifeLabs' Commitment to Privacy and Security

54. LifeLabs was responsible for protecting the privacy of the Class Members' Personal Information, including restricting access to the Personal Information to only those within each Class Members' circle of care, and limiting the amount of such information that it retained in the Computer Systems.

55. LifeLabs represented to the public that:

    (a) protecting the privacy and security of personal information is essential to its values and the way it does business; and

(b) it is accountable to protect and safeguard the Personal Information of its clients.

These representations are implied terms of its service contracts with each Class Member.

56. LifeLabs represented to the public that it would:

(a) maintain the highest standards of privacy, confidentiality, and data security;

(b) take strict security measures to ensure that Personal Information was protected from loss, theft, unauthorized access, use, copying, or disclosure; and

(c) implement security measures that met industry standards, including appropriate physical, technical, administrative, and procedural safeguards.

These representations are implied terms of its service contracts with each Class Member.

57. These representations were included in LifeLabs' privacy statements and privacy policies. These statements and policies were incorporated into LifeLab's contracts with each Class Member ("the Contracts"). The Contracts purported to govern the use of LifeLabs' services and websites, including the "My Results", "Save My Spot", "my ehealth", and "Launchpad" platforms.

58. LifeLabs was required to have in place practices that comply with all provincial privacy statutes for each Province in which it operates. Meeting these requirements was an implied term of the Contracts, and LifeLab's duty of care owed to the class included compliance with the privacy legislation of every Province in which it operated.

59. LifeLabs was also required to meet the terms of its contractual arrangements with health care providers and with each Provincial health ministry, including but not limited to its contractual obligations enumerated in its agreements with the British

Columbia Ministry of Health to deliver its services with the utmost care for confidential and personal information, and in compliance with all Provincial privacy, security and confidentiality standards. The Plaintiffs and the Class are third party beneficiaries to LifeLab's agreements with the Provincial health ministries, and LifeLab's duty of care owed to the class included compliance with these contracts.

The Security Breach

60. LifeLabs used its Computer Systems to store the Class Members' Personal Information. The Computer Systems were connected to the Internet.

61. LifeLabs knew that its security policies and practices were inadequate, out of date, and did not meet industry standards applicable to a custodian of Personal Information in particular.

62. In approximately November of 2018, and possibly earlier, the Cyberattackers breached the Computer Systems' security and gained widespread access to the information stored on the Computer Systems, including accessing the Class Members' Personal Information (the "Security Breach").

63. The Security Breach continued undetected for at least a year before LifeLabs discovered it in or about late October 2019. Alternatively, LifeLabs knew of the Security Breach for some time prior to October of 2019 and it failed to take appropriate responsive action, or any action at all. LifeLabs was reckless in failing to have appropriate security procedures in place to detect the Cyberattackers, who roamed undetected throughout the Computer Systems for many months.

64. During this time, the Cyberattackers repeatedly accessed data and exfiltrated data in the Computer Systems including the Personal Information of Class Members, thereby continuously or repeatedly breaching the Class Members' privacy. Both the accessing of the Personal Information, and the exfiltration of the Personal Information by the cyberattackers, which was permitted by LifeLabs, were breaches of the Class Members' privacy, causing them harm.

65. As a result of the Security Breach, up to 15 million LifeLabs customers had their Personal Information exposed, accessed and/or extracted by the Cyberattackers, and they were put at risk of having their Personal Information accessed and used by other criminal actors.

66. The Security Breach occurred because LifeLabs had inadequate technical and procedural safeguards over its Computer Systems. Deficiencies included, but are not limited to:

(a) storing unencrypted, or weakly encrypted, Personal Information on the Computer Systems;

(b) providing greater access rights to users and applications than necessary;

(c) storing usernames and passwords without salting and hashing;

(d) failing to use network segmentation and segregation;

(e) collecting and storing more Personal Health Information than was necessary;

(f) failing to make regular back-ups that were segregated from the Computer Systems;

(g) failing to install security patches and other software updates;

(h) failing to maintain adequate or any surveillance and systems checks over the Computer Systems;

(i) failing to train employees to identify and respond appropriately to phishing and other common attacks; and

(j) failing to delete and destroy stored Personal Information after there was no longer a legitimate purpose for retaining it.

(the "Deficiencies")

67. LifeLabs knew about the Deficiencies but failed to take any or appropriate steps to address them. LifeLabs knew it was particularly vulnerable to being hacked, knew the Personal Information that it stored was particularly sensitive and that it would be a prime target for hackers, and it was aware of the importance of encrypting data as a means of protecting the data.

68. LifeLabs knew that it had inadequate technical and procedural safeguards before it discovered the Security Breach. It deliberately and wilfully or recklessly chose not to implement appropriate IT security to protect the Personal Information of Class Members. As a result, the defendants negligently, or recklessly, or intentionally exposed the Class Members to the risks of the Security Breach, and to the intrusion upon their privacy rights, in order to reduce its operating costs and increase its profits.

69. Because of the Security Breach, Class Members are vulnerable to, and have a real, substantial and imminent risk of being subjected to future privacy breaches, identity theft and other forms of fraud, phishing attacks, and other unauthorized uses of their Personal Information by malicious actors, including but not limited to the Cyberattackers exploiting the Personal Information acquired from the Security Breach.

Reckless and/or Intentional Conduct

70. At all material times, LifeLabs willfully and deliberately chose not to put into effect any policy related to the security of its Computer Systems. In particular, while the Security Breach was underway, LifeLabs had in its possession draft IT security documents (dated January 2019) that had never been signed, finalized or brought into effect.

71. One of the most fundamental safeguards that a trustee of Personal Information should have in place is continually updated and formally approved privacy and security policies and procedures. LifeLabs knew these safeguards were fundamental and knew these safeguards were not in place at the time of the

Security Breach. Lifelabs knew its delay in implementing these safeguards meant its cyber security was at a high risk of being breached and that this would cause harm to the class, but decided not to do anything about it. This fundamental safeguard was not addressed as a prevention measure until May 27, 2020 - months after the discovery of the Security Breach.

72. As a result of its intentional and deliberate omission to have key written and approved privacy and security policies in place, LifeLabs failed to provide its employees with enough guidance to protect the Personal Information. LifeLabs' security personnel could not and did not plan and implement enterprise IT system defenses against security breaches and vulnerability issues, audit existing procedures, or put in place security policies, procedures and standards.

73. LifeLabs' decision not to have key written and approved privacy and security policies in place was a breach of applicable personal information protection statutes, including subsection 16(c) of Saskatchewan's HIPA, subsection 12(1) of Ontario's PHIPA and subsection 34 of British Columbia's Personal Information Protection Act.

74. Prior to the Security Breach, LifeLabs knew its security systems were below industry standards for custodians of Personal Information but, for the sake of reducing costs and increasing profits, decided not to do anything about it.

75. In the alternative, LifeLabs was reckless, which amounted to intentional conduct. In particular:

a) Prior to the Security Breach, LifeLabs knew its Personal Information protection measures were grossly inadequate and also knew that its Computer Systems were particularly vulnerable to being hacked, given the highly sensitive nature and the volume of Personal Information that it stored. Despite this knowledge of the consequences of inadequate security measures, LifeLabs continued to store the Personal Information with inadequate technical and procedural safeguards.

b) Prior to the Security Breach, LifeLabs had considered the risks of a cyberattack on its Computer Systems and even engaged experts in cybersecurity to review its systems and to provide advice as to the industry standard policies and procedures required to safeguard the Personal Information. Despite these initial efforts, LifeLabs deliberately and willfully elected not to prioritize cyber security. For example, it utilized staff who were untrained and inexperienced in cyber security best practices, outdated cyber security computer equipment and programs, outdate privacy and security policies or no policies - all to avoid increases in its operating costs. These decisions to prioritize profits over cyber security were made at the highest level of the company.

76. It was only after the Security Breach that LifeLabs made a $50 million investment into information security.

77. At all material times, LifeLabs held a dominant position, and in some provinces it had a monopolistic agreement with the Ministry of Health, for provision of the Services. As a result, the Plaintiffs and Class Members had limited, if any, choice but to use LifeLabs to obtain the Services, and consequently limited, if any, choice but to rely on LifeLabs' cyber security measures for the protection of their Personal Information.

78. Because of Lifelabs' dominant position, it was not subject to market forces that would otherwise have made the timely implementation of sufficient cyber security safeguards a company priority. As a result, there existed at LifeLabs a culture of reckless indifference to customer privacy and security. The existence of that culture negligent, and was a causal factor in the occurrence of the Security Breach.

Defendants' Response to the Security Breach

79. At some point before the end of October 2019, LifeLabs became aware of the Security Breach.

80. LifeLabs failed to disclose the Security Breach to its customers/patients for over two months, only issuing a public notice when compelled to do so by regulatory

authorities. LifeLabs failed to directly notify most Class Members at all, and failed to notify those Class Members whose test results were impacted in a timely manner. It failed to provide sufficient or accurate information in their notices so that Class Members could take steps to mitigate harm arising from the Security Breach.

81. Without having disclosed the Security Breach to those affected, LifeLabs paid a ransom to the Cyberattackers. The ransom payment reflects the minimum monetary value to the Cyberattackers of the extracted data, prior to any resale to third parties.

82. Although LifeLabs alleges that the ransom payment will protect Class Members, the Cyberattackers are anonymous and are not subject to the authority of Canadian courts. LifeLabs had no objective assurances that payment of the ransom would result in a return of all exfiltrated data to it, without copies having been made, and without copies being sold to third party malicious actors.

83. Irrespective of the return of the exfiltrated data, Class Members' privacy rights were breached by the Cyberattackers' intrusion into their Personal Information for over one year.

84. Between the date of the Security Breach and the date the data was unencrypted or restored, Class Members and their health care providers were unable to access their Personal Information on the Computer Systems.

85. On October 28, 2019, LifeLabs reported the Security Breach to the British Columbia Ministry of Health.

86. On November 1, 2019, LifeLabs reported the Security Breach to the Information and Privacy Commissioner of Ontario.

87. On November 5, 2019, LifeLabs reported the Security Breach to the Information and Privacy Commissioner of British Columbia.

88. On December 13, 2019, LifeLabs reported the Security Breach to the Information and Privacy Commissioner of Saskatchewan.

89. On December 17, 2019, LifeLabs posted "An Open Letter to LifeLabs Customers" on its website (the "Open Letter"). The Open Letter stated that information relating to approximately 15 million customers was stored on the computer systems that were accessed in the Security Breach.

90. The Open Letter included the following statements:

> Through proactive surveillance, LifeLabs recently identified a cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results.
>
> ...
>
> There is information relating to approximately 15 million customers on the computer systems that were potentially accessed in this breach. The vast majority of these customers are in B.C. and Ontario, with relatively few customers in other locations. In the case of lab test results, our investigations to date of these systems indicate that there are 85,000 impacted customers from 2016 or earlier located in Ontario; we will be working to notify these customers directly. Our investigation to date indicates any instance of health card information was from 2016 or earlier.

91. The Open Letter stated that LifeLabs would contact the 85,000 Ontario customers whose lab test results were disclosed, but LifeLabs failed to make this contact in a timely manner, adequately, or at all.

92. At no material time has LifeLabs offered adequate information so as to enable its customers/patients to fully and properly assess whether they were impacted by the Security Breach, and to take responsive measures.

93. Beginning in January 2020, LifeLabs emailed customers whose email addresses were stored on the Computer Systems as part of LifeLabs' online appointment booking systems. LifeLabs advised Ontario and Saskatchewan customers to create a new password the next time they logged into their LifeLabs account. LifeLabs advised British Columbia customers that they "are not required to take

any action because this system is no longer used to book appointments in the province."

94. The statements that LifeLabs made to Class Members in the Open Letter and in direct communications were misleading to Class Members. LifeLabs sought to persuade Class Members that it was taking all reasonable steps to protect their Personal Information.

95. However, LifeLabs has failed to disclose adequate information to enable the Class Members to fully and properly assess how they were impacted by the Security Breach, and to take responsive measures. To the contrary, LifeLabs has consistently refused to provide or disclose any information about the adequacy of its IT security and has denied responsibility for the IT breach, and attempted to downplay the consequences of the Security Breach.

96. LifeLabs has provided no information regarding the amount of the ransom demand, what the Cyberattackers promised in return for the payment of the ransom, the scope or nature of the data retrieved, whether LifeLabs had any way to confirm with reasonable certainty that the terms of the ransom exchange were met, nor whether any methodology capable of confirming whether the data extracted in the Breach was distributed or copied in any way exists. In fact, there is no way for LifeLabs to confirm with reasonable certainty that the terms of the ransom exchange were met, and that the data was fully returned to LifeLabs without having been copied or sold.

97. After having conducted an investigation into the Security Breach, the Saskatchewan Privacy Commissioner issued a report stating:

> 150 In this case, seven months after the discovery of the breach, I have concluded that LifeLabs has not done enough to properly notify affected individuals, investigate the breach, prevent future breaches or create a comprehensive investigation report. I have also identified several ways in which LifeLabs was not in compliance with HIPA at the time of the cyberattack. I have had to make these conclusions based on the limited information provided by LifeLabs.

151 Overall, I am disappointed with the lack of information about the breach provided by LifeLabs, the delay in notifying my office and affected individuals and its assessment of the risk to affected individuals.

152 LifeLabs has missed its opportunity to demonstrate to my office that it has responded adequately to this breach.

98. Similarly, the Ontario IPC and BC OIPC found that LifeLabs failed to protect personal information in the 2019 breach. The joint investigation revealed that the company's failure to implement reasonable safeguards to protect the personal health information of millions of Canadians violated Ontario's health privacy law and BC's personal information protection law. The IPC and OIPC determined that LifeLabs (1) failed to take reasonable steps to protect the personal health information in its electronic systems, (2) failed to have adequate information technology securities in place, and (3) collected more personal health information than was reasonably necessary. The results of the joint investigation have not been published, due to LifeLabs' claims that the information it provided was privileged or otherwise confidential.

CAUSES OF ACTION

Negligence

99. It was reasonably foreseeable that a failure by LifeLabs to adequately protect the Class Members' Personal Information would result in a security breach that would cause harm to the Class Members, including the inherent personal harm arising from a breach of their privacy and consequential harm following the extraction and criminal use of their Personal Information from the Computer Systems, and/or the damages arising from Class Members taking reasonable steps to mitigate or prevent the real, substantial and/or imminent risk of harm arising from the Security Breach.

100. LifeLabs owed a duty to the Class Members to collect, create, use, store, and transmit their Personal Information securely and with reasonable care because of:

(a) its close and direct relationship with each Class Member arising out of the Contracts and its collection, creation, use, storage, and transmission of the Class Members' Personal Information; and,

(b) LifeLabs' acknowledgements and commitments regarding the need to protect the Personal Information, including LifeLabs' own privacy policies and privacy statement.

101. The standard of care LifeLabs was required to meet with respect to the collection and storage of Personal Information is heightened given the highly sensitive nature of the Personal Information that LifeLabs was entrusted with. The required standard is informed by, but not limited to, industry practice, the common law, and privacy legislation. LifeLabs was and is mandated by statute and common law to have in place effective, updated, state of the art cybersecurity to protect the nearly unprecedented amount of Personal Information that it collects and stores.

102. LifeLabs' conduct did not meet the requisite standard of care. Particulars of LifeLabs' breaches of the standard of care include, but are not limited to, the Deficiencies.

103. LifeLabs' negligent conduct caused the Plaintiff and Class Members to suffer harm, as particularized below.

Breach of Contract

104. The Class Members, including the Plaintiffs, entered into identical or very similar contracts when using LifeLabs' services.

Service Contracts

105. The Class Members agreed to use LifeLabs' services to obtain medical diagnostic laboratory testing, which required the Class Members to provide LifeLabs with Personal Information and to permit LifeLabs to store Personal Health Information about them in the Computer Systems. In exchange, LifeLabs agreed, represented and warranted that it would protect the Personal Information of Class Members by

keeping it confidential and secure from risks such as the Security Breach, as provided in its privacy statements and privacy policies, and in its service agreements with the provincial health ministries.

106. LifeLabs entered into a series of contracts with the BC Ministry of Health to provide laboratory services to individuals in British Columbia. Those class members who received LifeLab's services while in British Columbia and which were paid for by the Ministry of Health are third party beneficiaries to these contracts. Under its agreement with the BC Ministry of Health, LifeLabs acknowledged that patients' privacy was of critical importance, and agreed that it would deliver its services with the utmost care for confidential and personal information, and that it would comply with all Provincial privacy, security and confidentiality standards.

107. LifeLabs entered into similar agreements with other Provincial health ministries, to which the Class Members in those provinces are third party beneficiaries.

108. In particular, LifeLabs is bound by the *Agreement for the Provision of Community Laboratory Services* between the Saskatchewan Health Authority [SHA] and LifeLabs LP ("the SHA Agreement") which states:

> 12. Security and Segregation of [Personal Health Information]
>
> [LifeLabs] shall have in place reasonable policies, procedures and safeguards to protect the confidentiality and security of [personal health information].

109. By judgment of June 9, 2020, The Saskatchewan Information and Privacy Commissioner held (para. 105) that LifeLabs had breached the SHA Agreement because it did not have reasonable policies and procedures in place at the time of the Security Breach.

110. The SHA Agreement also states, at Appendix E, that LifeLabs "must have in place, privacy breach management protocols that have been approved by [the SHA] in accordance with the Governance Process in Schedule G." Prior to the Security Breach, the SHA had not approved LifeLabs' privacy breach protocol as required

by the SHA Agreement. On this basis, *inter alia*, the Saskatchewan Information and Privacy Commissioner found LifeLabs to have breached the Saskatchewan Health Information Protection Act.

111. The Class Members were the intended beneficiaries of the contracts between LifeLabs and health service providers or ministries of health. As a result, the Class may rely on these contracts and sue in relation to their breach.

112. Further, or in the alternative, while LifeLabs customers do not typically sign a written contract for laboratory testing funded by the Provinces, LifeLabs is a service provider, so a common law unwritten contract for laboratory services exists between LifeLabs and the Class members. These common law contracts are included in the Contracts. The implied terms of these Contracts include that LifeLabs would ensure that it had appropriate security safeguards in place to prevent a cyberattack and to limit the exposure of the Class Members' Personal Information in the event of a successful cyberattack.

113. LifeLabs had a duty to perform its Contracts and the contracts with the Provincial health ministries honestly and in good faith.

Online Contracts

114. Class Members who used LifeLabs' online services, including "My Results", "Save My Spot", "my ehealth", and "Launchpad" entered into standard form contracts with LifeLabs or Excelleris. These contracts incorporated as terms of the contract LifeLabs' privacy statements and privacy policies.

115. LifeLabs committed to keep the Class Members' Personal Information safe and secure from third parties in its privacy statements and privacy policies.

116. It was an implied term of LifeLabs' contracts with all its patients and customers that it would meet the commitments to privacy included in the privacy statements and privacy policies, and that it would comply with all statutory privacy obligations.

117. The Contracts and the contracts with Provincial health ministries contained the following express or implied terms:

(a) LifeLabs would comply with all relevant statutory privacy obligations regarding the collection, use, retention, and disclosure of each customer/patient's personal information;

(b) LifeLabs would not collect, use, retain, or disclose the Personal Information except in the manner and for the purposes expressly authorized by the Contract or applicable privacy legislation;

(c) LifeLabs would keep the Personal Information secure and confidential;

(d) LifeLabs would not disclose the Personal Information without consent;

(e) LifeLabs would protect the Personal Information by using high security arrangements to prevent unauthorized access, unauthorized copying or collection, use, disclosure, copying, modification or disposal of Personal Information, or similar risks; and

(f) LifeLabs would delete, destroy, or not retain the Personal Information as soon as it was reasonable to assume that (i) the purpose for which that Personal Information was collected was no longer being served by retention of the Personal Information, and (ii) retention was no longer necessary for legal or business purposes.

118. LifeLabs breached the Contracts and the contracts with the Provincial health ministries by failing to perform these contractual obligations, and by failing to perform these contracts honestly and in good faith. It intentionally failed to comply with the privacy terms by failing to maintain the highest standards of privacy, confidentiality and data security including safeguarding the Personal Information of its patients and failed to secure the Class Members' data as it had agreed to do. It did so to reduce its expenses and increase its profits. Accordingly, the Class are

entitled to disgorgement of the improper profits that LifeLabs gained at the expense of the Class arising from its intentional breach of the contracts.

119. As a result of LifeLabs' breach of the Contracts and the contracts with the Provincial health ministries, the Class Members have been harmed. They have suffered a breach of their privacy by the Cyberattackers accessing and reviewing their personal information, and then extracting it. Their Personal Information has been compromised, and used by malicious actors for fraudulent or criminal purposes.

120. The Class Members have incurred damages in taking reasonable steps to mitigate their losses or the risk of loss to which they were exposed by the Security Breach.

121. The Class have also suffered mental injuries arising from their anxiety and distress upon being advised of the Security Breach. Such mental injuries were within the reasonable contemplation of the parties at the time that the Contracts were formed, and they are serious and prolonged and rise above the ordinary annoyances, anxieties and fears that come with living in civil society.

122. The Class Members have a legitimate contract interest in LifeLabs complying with its contractual obligations to protect unauthorized access to its Computer Systems, to keep private and confidential the Class Members' Personal Information, and to limit the storage of this information.

123. The Class Members' contract interest is for protection of their privacy rights. This cannot be vindicated or quantified on a pure economic loss measure, which fails to remedy or compensate for the loss of control of personal private information, including the Personal Health Information.

124. In all the circumstances, other remedies will not adequately protect or vindicate the breach of the Class Members' contractual right to prevent the unauthorized access and dissemination of their Personal Information, including:

(a) Conventional contract damages alone would fail to deter LifeLabs, who misrepresented to Class Members how it would protect their privacy, and LifeLabs thereby increased its profits at the expense of the security of the Class Members' Personal Information;

(b) The representations made to the Class Members encouraged them to trust LifeLabs would protect their Personal Information, putting the Class Members in a position of confidence, reliance and trust. The Class Members were entirely vulnerable to LifeLab's failure to protect Class Members' privacy, since the Class Members had no control over how LifeLabs actually went about protecting their privacy;

(c) The Class Members have a legitimate interest in preventing LifeLab's profit-making activity when it related to failing to put in place adequate cyber-security measures to meet its contractual obligations to the Class;

(d) LifeLabs expressly contracted not to do the particular thing that permitted the Security Breach; the purpose of the contract provision was breached; Class Members' rights were quasi-proprietary; and the Personal Information should have been protected.

125. Therefore, the Class Members seek nominal damages for breach of contract, as well as disgorgement of profits or revenues generated from LifeLabs' failure to obtain, implement and follow adequate cyber-security measures. It would be unconscionable for LifeLabs to retain these profits, which were taken at the expense of the Class Members' privacy rights, and in breach of Class Members' confidence and privacy rights, and any other wrongdoing as set out herein.

Intrusion upon Seclusion

126. LifeLabs was responsible for collecting, managing, storing, securing and/or deleting the Personal Information. It was reasonable for Class Members to expect that LifeLabs would collect only Personal Health Information that was reasonably

necessary, store it for no longer than reasonably necessary, and use adequate security measures to protect it given its highly sensitive nature.

127. The Personal Information that was invaded, including Personal Health Information, is highly sensitive and personal, and a reasonable person would consider the invasion to be highly offensive causing anguish, humiliation or distress.

128. LifeLabs intentionally or recklessly:

(a) collected more Personal Information from Class Members than reasonably necessary;

(b) stored Personal Information for longer than reasonably necessary in its Computer Systems; and,

(c) chose not to use adequate security measures to protect the Personal Information, when it knew that the Personal Information would be a highly desirable acquisition target for cyber criminals, but instead LifeLabs recklessly or intentionally created the Computer Systems in a manner that invited and allowed cyber criminals to access the Personal Information.

129. LifeLabs was reckless in storing the Class Members' Personal Information in the Computer Systems, which it knew were insecure and vulnerable to malicious cyberattacks. It recklessly failed to engage in up to date cybersecurity protocols or apply current software to protect against cyberattacks, all while knowing and callously disregarding the fact that the Class Members' Personal Information was a high-value and easy target for cybercriminals to access, exfiltrated and monetize, and thereby cause harm to the Class.

130. LifeLabs' conduct would be highly offensive to a reasonable person. Its intentional or reckless conduct facilitated and enabled the Cyberattackers to access and copy sensitive Personal Information, including information that LifeLabs should not have stored in its Computer Systems. As a result, LifeLabs intruded upon the seclusion of the Class Members without lawful justification.

131. In the alternative, by recklessly or negligently failing to take appropriate security safeguards, and thereby facilitating the cyber-breach, the Defendants are jointly and severally liable for the tort of intrusion upon seclusion with the Cyberattackers who intentionally invaded the Class Members' privacy, and intruded upon the Class Members' seclusion.

132. The tort of intrusion upon seclusion is made out because:

(a) the Cyberattackers intentionally invaded the Class Members' privacy;

(b) the Defendants' tortious conduct facilitated the Cyberattackers' ability to invade the Class Members' privacy;

(c) the Personal Information was invaded the Class Members' private affairs or concerns without lawful justification; and

(d) the Personal Information that was invaded, including personal health information, is highly sensitive and personal, and a reasonable person would consider the invasion to be highly offensive causing anguish, humiliation or distress.

133. LifeLabs is liable for the deliberate and significant invasions of the Class Members' privacy. LifeLabs knew that its inadequate IT security facilitated the breach by the Cyberattackers. The Security Breach fell within the ambit of risk that LifeLabs' enterprise created or exacerbated through failing to implement appropriate security measures. LifeLabs introduced the risk of the wrongs by collecting the Personal Information and therefore should have managed and minimized the risk. A fair allocation of the consequences justifies imposition of liability on LifeLabs because there is a sufficient nexus between its wrongful acts and the Security Breach.

134. LifeLabs acted with reckless indifference to the consequences of failing to maintain appropriate security measures on their Computer Systems and knew that it was

consequently placing the Class Members at significant risk of having their privacy breached through a cyberattack on LifeLabs' Computer Systems.

135. LifeLabs' actions and omissions constituted either conscious wrongdoing or a marked departure from the standards applicable to responsible and competent institutions in charge of large quantities of sensitive Personal Information, and in particular, personal health information, so as to govern themselves in the collection, management, storage, securing and/or deleting of such data.

136. Class Members of all provinces can advance a claim for intrusion upon seclusion because LifeLabs' head office is in Ontario and the Security Breach occurred in Ontario. LifeLabs' procedures for the collection and safeguarding of Personal Information are implemented in Toronto, as information is collected and safeguarded on Computer Systems located in Ontario.

137. The Class Members are entitled to moral damages for the intrusion upon their seclusion facilitated by LifeLabs.

Breach of Privacy Legislation

Ontario – Personal Health Information

138. The Personal Health Information collected and used by LifeLabs is "personal health information" as defined by section 4 of the *Personal Health Information Protection Act*, 2004 S.O. 2004, ch.3 ("PHIPA").

139. By virtue of section 12 of PHIPA, LifeLabs had a duty to ensure that the personal health information in its custody and control was protected against theft, loss and unauthorized use, disclosure, modification or copying.

140. Pursuant to s. 29 of PHIPA, a health information custodian shall not disclose personal health information about an individual unless it is done with the individual's consent and is necessary for a lawful purpose.

141. By failing to implement sufficient encryption and security, LifeLabs breached sections 12, 13, and 17(3) of PHIPA, which requires that 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.

142. The Ontario Privacy Commissioner has made a final order against LifeLabs for violations of PHIPA. The Plaintiffs, on their own behalf and on behalf of the Class Members assert a claim for damages for the actual harms they have suffered because of LifeLabs' wilful and reckless contravention of PHIPA, including mental anguish, pursuant to s. 65 of PHIPA.

British Columbia – Personal Information

143. The Personal Information is "personal information" as defined in section 1 of the *Personal Information Protection Act* [SBC 2003] c. 63 ("PIPA BC").

144. LifeLabs is an "organization" as defined in section 1 of PIPA BC.

145. By intentionally or recklessly failing to implement sufficient encryption and security, LifeLabs breached section 34 of PIPA BC which requires that 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.

146. LifeLabs breached section 35 of PIPA BC by intentionally or recklessly failing to destroy the Personal Information as required by that section.

147. The British Columbia Privacy Commissioner has made a final order against LifeLabs for violations of the provisions of PIPA BC. The Plaintiffs, on their own behalf and on behalf of the Class Members assert a claim for damages for the actual harms they have suffered because of LifeLabs' contravention of PIPA BC, including mental anguish, pursuant to s. 57(1) of PIPA BC.

Statutory Privacy Torts

148. LifeLabs wilfully, knowingly and recklessly failed to take appropriate steps to guard against unauthorized access to the Personal Information of the Class Members,

and facilitated access by the Cyberattackers, causing a violation of the Class Members' privacy. As a result, LifeLabs is liable for breach of privacy under the following statutes:

(a) Section 1 of the *Privacy Act*, R.S.B.C. 1996, C. 373 ("BC Privacy Act");

(b) Section 2 of the *Privacy Act*, C.C.S.M., c. P125 ("Manitoba Privacy Act");

(c) Section 2 of the *Privacy Act*, R.S.S. 1978, C. P-24 ("Saskatchewan Privacy Act");

(d) Sections 5, 6, 10, 13 of the Act respecting the protection of personal information in the private sector, C. P-39.1 ("Quebec Privacy Act"); and

(e) Section 3 of the *Privacy Act*, R.S.N.L. 1990, c. P-22 ("Newfoundland and Labrador Privacy Act").

Quebec

149. The Defendants breached articles 35, 36, and/or 37 of the CCQ by failing to obtain consent of those Class Members to disclose their Personal Information and failing to maintain adequate cybersecurity to safeguard the Class Members' Personal Information from unauthorized access.

150. More particularly, the Defendants breached arts. 35, 36, and 37 of the CCQ because:

(a) they allowed unauthorized access to the Personal Information of the Class Members resident in Quebec without their consent and without the invasion being authorized by law;

(b) they allowed unauthorized access to the personal documents of Class Members resident in Quebec; and

(c) they communicated the Personal Information of Class Members resident in Québec to unauthorized persons.

151. As a result of the breaches of the CCQ, the Class Members resident in Quebec are entitled to moral and material damages pursuant to arts.1457 and 1463-1464 of the CCQ.

152. With respect to Class Members resident in Québec, LifeLabs is subject to the obligations of the *Consumer Protection Act*, which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices. LifeLab's failure to take reasonable measures to secure the Personal Information constitutes a prohibited practice because the representations that it made to the Class Members in relation to its security measures were false and misleading contrary to section 219, the particulars of which are as follows:

(a) LifeLabs represented through the Contract that it would comply with their own privacy policy, PIPEDA and PPIPS and protect the Class Members' privacy, including their Personal Information and the information contained in their Accounts; and

(b) LifeLabs failed to disclose to the Class Members that its security measures were inadequate to secure the Class Members' privacy.

153. As a result of the breaches of the *Consumer Protection Act*, the Class Members resident in Québec have suffered damages for the false and misleading representations made to them by LifeLabs. In addition, Class Members resident in Québec are entitled to punitive damages pursuant to s. 272 of the *Consumer Protection Act.*

154. In addition, Class Members resident in Quebec are entitled to punitive damages pursuant to art. 49 of the Quebec *Charter of Human Rights and Freedoms*.

Breach of Consumer Protection Legislation

155. The Class Members are consumers within the meaning of the Applicable Consumer Protection Legislation because they entered into a consumer agreement with LifeLabs where LifeLabs agreed to provide goods or services for

payment. In some instances, Class Members paid directly for laboratory testing services that were not eligible for coverage under the applicable provincial publicly funded health care insurance plan. In other instances, LifeLabs supplied the services to the class member but the payment was made on behalf of the Class Member by the province in which the transaction occurred. Nevertheless, in the case where the payment was made by the province, the Class Members were parties to the service agreement, or were third party beneficiaries to them.

156. LifeLabs' failure to take reasonable measures to secure the Personal Information constitutes an unfair practice under the Applicable Consumer Protection Legislation because LifeLabs' security measures did not meet the standards LifeLabs described in its representations regarding its commitment to privacy and security, as detailed above.

157. LifeLabs' failure to notify customers that it was continuing to collect and store their Personal Information long after it was necessary is a misrepresentation by omission that constitutes an unfair practice.

158. By making the false, misleading or deceptive representations about the state of its cyber-security and its ability the maintain the Class Members' privacy, LifeLabs engaged in unfair practices, contrary to sections 14(1)-(2) of the Ontario *Consumer Protection Act* and contrary to parallel provisions of the Applicable Consumer Protection Legislation. LifeLabs is liable to the Class for the damages suffered as a result of the false, misleading and deceptive representations made by it.

159. It is not in the interests of justice to require that notice be given pursuant to section 18(15) of the Ontario *Consumer Protection Act*, and pursuant to parallel provisions of the Applicable Consumer Protection Legislation, and therefore this condition should be waived.

160. With respect to Class Members resident in Québec, LifeLabs is subject to the obligations of the *Consumer Protection Act*, CQLR c P-40.1, which prohibits persons who enter into agreements or conduct transactions with consumers from

engaging in prohibited practices. LifeLabs' failure to take reasonable measures to secure the Personal Information constitutes a prohibited practice because the representations that LifeLabs made to the Class Members in relation to its security measures were false and misleading, contrary to section 219.

161. As a result of the breaches of the *Consumer Protection Act*, CQLR c P-40.1, the Class Members resident in Québec have suffered damages for the false and misleading representations made to them by LifeLabs. In addition, Class Members resident in Québec are entitled to punitive damages pursuant to s. 272 of the *Consumer Protection Act*, CQLR c P-40.1.

Unjust Enrichment

162. Class Members are entitled to recover under restitutionary principles including disgorgement of profits.

163. LifeLabs has been unjustly enriched by receipt of fees in exchange for services that it represented it would provide to Class Members.

164. Class Members paid more for the services provided to them by LifeLabs than they should have, and/or LifeLabs profited more than it should have, because LifeLabs did not make necessary expenditures on security measures needed to protect the Personal Information.

165. Because the money and profits that LifeLabs received were generated by their wrongful acts, including breach of contract and the torts pleaded above, there is no juristic reason justifying the retention of overpayments received by LifeLabs from Class Members.

DAMAGES

166. As a result of LifeLabs' wrongful conduct, the Plaintiff and Class Members suffered damages including, but not limited to:

(a) loss of their right to privacy in respect of their Personal Information;

(b) serious and prolonged mental distress;

(c) loss of privacy and injury to dignity;

(d) harm to credit reputation;

(e) costs incurred in preventing, rectifying, or insuring against identity theft, fraud, and other misuse of Personal Information;

(f) out-of-pocket expenses;

(g) wasted time, expense, and inconvenience associated with attempting to obtain more information about the Security Breach and taking precautionary measures to safeguard the Personal Information, and addressing increased phishing attacks;

(h) damages as a result of the Personal Information being inaccessible to Class Members and their health care providers from the time of the Security Breach until the data was unencrypted or restored.

167. The BC *Privacy Act*, Saskatchewan *Privacy Act*, Manitoba *Privacy Act*, and Newfoundland and Labrador *Privacy Act* mandate that violation of a person's privacy is actionable without proof of damage. Proof of actual pecuniary loss is not an element of the tort of intrusion upon seclusion, or of breach of ss. 35, 36 and 37 of the CCQ. Therefore, LifeLabs' breach of the Class members' privacy is actionable per se and damages for all Class Members is presumed.

168. Punitive damages are justified in these circumstances as such an award is rationally connected to the goals of denunciation, deterrence and retribution:

(a) LifeLabs knew or ought to have known that their actions and omissions would have a significant adverse effect on all Class Members.

(b) LifeLabs' conduct was high-handed, reckless, without care, deliberate, and in disregard of the rights of the Plaintiff and Class Members.

(c) LifeLabs prioritized profit over the privacy, security and dignity of the Plaintiffs and the Class Members.

STATUTES

169. The Plaintiffs rely on the following Ontario statutes:

(a) *Personal Health Information Protection Act, 2004*, SO 2004, c. 3;

(b) *Courts of Justice Act*, R.S.O. 1990, c. C. 43;

(c) *Negligence Act*, R.S.O. 1990, c. N-1;

(d) *Consumer Protection Act, 2002*, S.O. 2002, c.30; and

(e) *Class Proceedings Act, 1992*, S.O. 1992, c. 6.

170. The Plaintiffs rely on the following British Columbia statutes:

(a) *Business Practices and Consumer Protection Act*, SBC 2004, c 2

(b) *Personal Information Protection Act*, SBC 2003, c. 63 ("PIPA BC");

(c) *Privacy Act*, R.S.B.C, 1996, c. 373; and

(d) *Negligence Act* [RSBC 1996] chapter 333.

171. The Plaintiffs rely on the following Alberta statutes:

(a) *Consumer Protection Act*, RSA 2000, c. C-26.3

(b) *Personal Information Protection Act*, SA 2003, c. P-6.5 ("PIPA Alberta").

172. The Plaintiffs rely on the following Saskatchewan statutes:

a) *Health Information Protection Act*, SS 1999, c. H-0.021 ("HIPA Saskatchewan");

b) *Consumer Protection and Business Practices Act*, SS 2013, c C-30.2and

c) *Privacy Act*, R.S.S. 1978, c. P-24.

173. The Plaintiffs rely on the following Manitoba statute:

(a) *Privacy Act*, C.C.S.M., c. P125.

174. The Plaintiffs rely on the following Prince Edward Island statute:

(a) *Consumer Protection Act*, R.S.P.E.I. 1988, c. C-19.

175. The Plaintiffs rely on the following New Brunswick statutes:

(a) *Consumer Product Warranty and Liability Act*, S.N.B. 1978, c. C-18.1;

(b) *Sale of Goods Act*, R.S.N.B. 2016, c. 110.

176. The Plaintiffs rely on the following Newfoundland and Labrador statute:

(a) *Privacy Act*, R.S.N.L. 1990, c. p-22.

177. The Plaintiffs rely on the following Quebec statutes:

(a) *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40; and

(b) *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1

178. The Plaintiffs rely on the following federal statute:

(a) *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 ("PIPEDA");

PLACE OF TRIAL

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

SERVICE OF FOREIGN DEFENDANTS

180. Pursuant to Rule 17.04(1), the Plaintiff plead and rely upon Rules 17.02(f), 17.02(g), and 17.02(p) of the Rules of Civil Procedure, R.R.O. 1990, Reg. 194, in support of service of the Notice of Action and this Statement of Claim upon the Defendants, LifeLabs BC Inc. outside of Ontario without a court order.

Dated: February 24, 2020

MCPHADDEN SAMAC TUOVI LLP
161 Bay Street, 27th Floor
Toronto, ON M5J 2S1

Bryan McPhadden (LSO# 28160K)
bryan@mcphadden.com
Tel: (416) 601-1020

CHARNEY LAWYERS PC
151 Bloor Street West, Suite 602
Toronto, ON M5S 1P7

Theodore P. Charney (LSO #26853E)
tcharney@charneylawyers.com
Tel: (416) 964-7950

Toronto ON M5C 2C5

WADDELL PHILLIPS PC
36 TORONTO STREET, SUITE 1120

Margaret L. Waddell (LSO #29860U)
marg@waddellphillips.ca
Tina Q. Yang (LSO #60010N)
tina@waddellphillips.ca
Tel: 647-261-4486

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

Jean-Marc Leclerc (LSO # 43974F)
jleclerc@sottosllp.com
Tassia Poynter (LSO # 70722F)
TPoynter@sotosllp.com
Tel: 416-977-0007

PETER I. WALDMANN PROFESSIONAL CORPORATION
183 Augusta Avenue
Toronto, ON M5T 2L4

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

STEIN LAW OFFICE
330 Bay Street, Suite 1400
Toronto ON M5H 2S8

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

OV COUNSEL
1030 West Georgia
Suite 1915
Vancouver, BC V6E 2Y3

Brent B. Olthuis
bolthuis@ovcounsel.com
Tel: 604-649-7966

COLLETTE PARSONS CORRIN LLP
1750 – 700 West Georgia Street
Vancouver, BC V7Y 1B6

Guy J. Collette
gcollette@braininjurylaw.ca
Richard Parsons
rparsons@braininjurylaw.ca
Venessa Vuia (LSO #69499L)
vvuia@cphlaw.ca
Tel: (604) 662-7777

ARSENAULT AARON LAWYERS
#302 – 543 Granville Street
Vancouver, BC V6C 1X8

David M. Aaron
david@legalmind.ca
Tel: (604) 788-8860

ROSENBERG LAW
671D Market Hill
Vancouver, BC V5Z 4B5

David Rosenberg Q.C.
david@rosenberglaw.ca
John David Ankenman
john@rosenberglaw.ca
Tel: 604-879-4505

Boughton Law Corporation
700- 595 Burrard Street
Vancouver, BC V7X 1S8

Mark Canofari
mcanofari@boughtonlaw.com
Tel: (604) 687-6789

Lawyers for the Plaintiffs

TO: **MCCARTHY TÉTRAULT LLP**
66 Wellington Street West, Suite 5300
TD Bank Tower Box 48
Toronto, ON M5K 1E6

Dana M. Peebles (LSO #30820V)
Tel: (416) 362-1812
Fax: (416) 868-0673

Lawyers for the Defendants

ALITA MARIE CARTER et al. Plaintiffs	-and-	LIFELABS INC., et al. Defendants	Court File No.: CV-20-00636642-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

PROCEEDING COMMENCED AT TORONTO

FRESH AS AMENDED STATEMENT OF CLAIM

MCPHADDEN SAMAC TUOVI LLP
161 Bay Street, 27th Floor
Toronto, ON M5J 2S1

Bryan McPhadden (LSO No.: 28160K)
bryan@mcphadden.com

Tel: 416.601.1020

CHARNEY LAWYERS PC
151 Bloor St. West, Suite 602
Toronto, ON M5S 1P7

Theodore P. Charney (LSO No.: 26853E)
tcharney@charneylawyers.com
Caleb Edwards (LSO No.: 65132P)
cedwards@charneylawyers.com

WADDELL PHILLIPS PC
36 Toronto Street, Suite 1120
Toronto, ON M5C 2C5

Margaret L. Waddell (LSO No.: 29860U)
marg@waddellphillips.ca
Tina Q. Yang (LSO No.: 60010N)
tina@waddellphillips.ca

Tel: 647.261.4486

SOTOS LLP
180 Dundas St. West, Suite 1200
Toronto, ON M5G 1Z8

Jean-Marc Leclerc (LSO No.: 43974F)
jleclerc@sotos.ca
Tassia Poynter (LSO No.: 70722F)
tpoynter@sotos.ca

Tel: 416.977.0007

PETER I. WALDMANN PC
183 Augusta Avenue
Toronto, ON M5T 2L4

Peter I. Waldmann (LSO No.: 23289M)
peter@peteriwaldmann.com

Tel: 416.921.3185

STEIN LAW OFFICE
330 Bay Street, Suite 1400
Toronto, ON M5H 2S8

Andrew Stein (LSO No.: 32065K)
astein@andrewsteinlaw.com

Tel: 416.642.2020

Lawyers for the Plaintiffs

OLTHUIS VAN ERT
1915-1030 West Georgia Street
Vancouver, BC V6E 2Y3

Brent B. Olthuis
bolthuis@ovcounsel.com

Tel: 604.649.7966

COLLETTE PARSONS CORRIN LLP
1750-700 West Georgia Street
Vancouver, BC V7Y 1B6

Guy J. Colette
gcollette@cpclegal.ca
Richard Parsons
acrp@cphlaw.ca
Venessa Vuia (LSO No.: 69499L)
vvuia@cphlaw.ca

Tel: 604.662.7777

BOUGHTON LAW CORPORATION
700-595 Burrard Street
Vancouver, BC V7X 1S8

Mark Canofari
mcanofari@boughtonlaw.com

Tel: 604.687.6789

ARSENAULT AARON LAWYERS
302-543 Granville Street
Vancouver, BC V6C 1X8

David M. Aaron
david@legalmind.ca

Tel: 604.788.8860

ROSENBERG LAW
671D Market Hill
Vancouver, BC V5Z 4B5

David Rosenberg Q.C.
david@rosenberglaw.ca
John David Ankenman
john@rosenberglaw.ca

Tel: 604.879.4505

CAMP FIORANTE MATTHEWS MOGERMAN
400-856 Homer Street
Vancouver, BC V6B 2W5

Jamie Thornback
jthornback@cfmlawyers.ca

Tel: 604.331.9529

Lawyers for the Plaintiffs