COURT FILE NO.: CV-20-006-36642-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

ALITA MARIE CARTER

PLAINTIFF

AND:

LIFELABS INC., LIFELABS BC INC., LIFELABS BC LP, LIFELABS LP, CMH HEALTH CARE INC. and EXCELLERIS TECHNOLOGIES INC.

DEFENDANTS

Proceeding under the *Class Proceeding Act, 1992*

FRESH 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 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: October [ ] 2020
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

AND TO: **CMH HEALTH CARE INC.**
200 Bay St, Royal bank Plaza, South Tower, Suite 2100,
Toronto, ON M5J 2J2.

AND TO: **EXCELLERIS TECHNOLOGIES INC.**
2900-500 Burrard Street
Vancouver, BC V6C 0A3

RELIEF SOUGHT

1. The Plaintiff, on her own behalf and on behalf of the Class Members (as defined herein), seeks the following relief:

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

   b) An order appointing the Plaintiff as the representative plaintiff for the Class, as defined herein;

   c) An order, pursuant to s. 24 of the CPA, for the aggregate assessment of monetary relief and distribution to the Plaintiff and Class Members;

   d) Declarations that:

      i. the Defendants owed a duty of care to the Plaintiff and Class Members in the handling 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 Security Breach was a result of breaches of contracts with the Plaintiff and Class Members;

      iv. the Defendants breached the common law privacy rights and/or intruded upon the seclusion of the Plaintiff and Class Members;

      v. the Defendants breached the statutory privacy and personal information protection rights of the Plaintiff and Class members;

      vi. the Defendants conduct amounted to breaches of confidence of the Plaintiff and Class Members;

vii. the Defendants made negligent misrepresentations to the Plaintiff and the Class Members;

viii. the Defendants are jointly and severally liable for the damages suffered by the Plaintiff and Class Members as set out herein;

ix. the Defendants owed and breached fiduciary duties to the Plaintiff and Class Members to secure their Personal Information, to be by failing to disclose the risks regarding the risks and the lack of safeguards in place, and to provide timely notification of each and every unauthorized access/disclosure of their Personal Information;

x. a declaration that the Defendants violated the *Consumer Protection Act,* 2002, S.O. c. 30;

e) An order for general damages in an amount to be determined at trial;

f) Orders for punitive, exemplary and aggravated damages in amounts to be determined prior to trial;

g) Orders for 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);

h) An order for nominal damages for breach of contract in an amount to be determined prior to trial;

i) In the alternative, in the event that compensation for breach of contract as set out above is inadequate compensation to the Class Members for their loss (by reason that the loss is impossible to calculate or the Class Members' interest in privacy protection is not reflected by a purely economic measure) the Plaintiff seeks an order that the Defendants pay the gains made by the Defendants in costs savings incidental to their failure to implement sufficient protections against unauthorized access and disclosure of the Personal Information during the relevant period;

j) An order that the Defendants disgorge all earned profits commencing from their known failure to implement sufficient safeguards to the point in time when proper safeguards were allegedly implemented, or to the time of judgment;

k) An order pursuant to s. 25 of the CPA directing individual hearings, inquiries, and determinations for Class Members who may have suffered special damages and all necessary directions relating to the procedures to be followed in conducting such hearings, inquiries, and determinations;

l) An order for 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;

m) Cost of this action on a substantial indemnity basis plus HST or in an amount that provides full indemnity, plus the costs of distribution of an award under ss.24 or 25 of the CPA;

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

THE PARTIES

The Plaintiff

2. The Plaintiff, Alita Marie Carter ("Carter"), is an individual residing in Toronto, Ontario.

3. Carter was a long-time customer/patient of the Defendants.

The Defendants

4. 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.

5. LifeLabs LP is a limited partnership established under the laws of Ontario. It has a registered office in Toronto. It is registered as an extraprovincial limited partnership in British Columbia with an office in Vancouver. Lifelabs Inc. is the general partner of Lifelabs LP.

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

7. 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 with in Burnaby, British Columbia. LifeLabs BC Inc. is the general partner of LifeLabs BC LP.

8. LifeLabs Ontario Inc. was an Ontario business corporation with a registered address in Toronto. LifeLabs Ontario Inc. is now merged with the Defendant CMH Health Care Inc., also a corporation incorporated pursuant to the laws of Ontario and having an office at Toronto.

9. LifeLabs Inc., LifeLabs LP, LifeLabs BC Inc., LifeLabs BC LP and LifeLabs CMH Health Care Inc. are in the business of medical testing. The LifeLabs Group performs medical diagnostic tests and makes customers' personal information available online to customers and their healthcare providers.

10. Excelleris Technologies Inc. is a wholly owned subsidiary of LifeLabs Inc. incorporated under the laws of British Columbia. It has a registered office in Vancouver, with an extra-provincial registration in Ontario where it carries on business *inter alia.*

11. Excelleris Technologies Inc. provides information technology services that support Lifelabs' business. While the LifeLabs Group collects and generates personal health information, Excelleris is the vehicle by which that information is stored and disclosed.

12. The Defendants are hereinafter referred to collectively as "LifeLabs".

Affiliates

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

14. By virtue of the conduct described herein, each of the of the Defendants is 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;

    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/or

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

Class Definition

15. The plaintiff brings this action on his own behalf and on behalf of a proposed class defined as:

    All persons who were resident of Canada and customers/patients of

LifeLabs prior to December 17, 2019.

[collectively, the "Class" or the "Class Members"]

FACTS

LifeLabs' Services

16. 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").

17. 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.

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

19. 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.

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

Personal Information

21. In the course of providing the Services, LifeLabs collected, created, used, and stored a vast amount of confidential personal information about its patients, including:.

a) names;
b) addresses;
c) email addresses;
d) user identifications;
e) passwords;
f) dates of birth;
g) health care numbers;
h) health provider names;
i) gender;
j) phone numbers;
k) security questions and answers;
l) Internet Protocol addresses; and
m) information about login attempts.

("Personal Identity Information").

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

23. Personal Identity Information and Personal Health Information are referred to herein collectively as "Personal Information".

Foreseeability

24. 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 increase in cyberattacks upon other custodians of Personal Information, it was foreseeable that LifeLab's 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

25. LifeLabs at all material times held a form of monopoly in Canada with respect to provision of the Services and, as a result, the Plaintiff and Class Members had limited if any choice but to rely on LifeLabs' cybersecurity measures for the protection of their Personal Information.

26. LifeLabs undertook the responsibility of administering restricted access to the Personal Information by patients, healthcare providers, hospitals and health authorities.

27. LifeLabs has acknowledged that:

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

b) it was accountable to protect and safeguard the personal information of its clients.

28. LifeLabs committed itself to:

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

b) take 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, and procedural safeguards.

29. These acknowledgements and commitments were included in LifeLabs' privacy statements and privacy policies. These statements and policies were incorporated into contracts with each Class Member ("the Contracts").

Contractual terms

30. The Contracts contained the following express or implied terms:

a) LifeLabs would comply with all relevant statutory 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 personal information protection 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 making appropriately high, industry-standard security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks; and

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

Fiduciary Position

31. LifeLabs was in a position of fiduciary in relation to the Plaintiff and Class Members who were in a peculiarly vulnerable position and at the mercy of LifeLabs in the exercise of its discretion as to what measures to take to secure their Personal Information. The Plaintiff and Class Members could not have known of LifeLabs' ineffective safeguards and lack of cybersecurity measures to protect their Personal Information.

32. As such, LifeLabs owed the Plaintiff and Class Members a duty to act in the

utmost good faith and the best interests of the Plaintiff and Class Members which required LifeLabs to be transparent and candid, and provide timely disclosure of the state and vulnerability of their cybersecurity measures.

Security Breach

33. LifeLabs used computer systems (the "Computer Systems") to store Personal Information. The Computer Systems were connected to the Internet.

34. LifeLabs implemented security policies and practices that were intended to prevent unauthorized access to the Computer Systems. These policies and practices were inadequate, as particularized herein.

35. In or about November of 2018 or earlier, one or more unknown individuals ("the Cyberattackers") breached the Computer Systems' security by accessing LifeLabs' computer servers situated in Ontario (the "Security Breach").

36. The Security Breach occurred undetected for almost a year (or more) before it was discovered by LifeLabs; or, alternatively, the Security Breach was known to LifeLabs for some time prior to October of 2019 and they failed to take appropriate responsive action.

37. Over this period of time, the Security Breach permitted Cyberattackers to repeatedly access data in the Computer Systems including the Personal

Information of Class Members.

38. Having gained repeated and ongoing access to the Computer Systems, Cyberattackers copied data, including Personal Information, to their own computer systems, and locked LifeLabs out of the same data on the Computer Systems.

39. By way of the Security Breach, up to 15 million LifeLabs customers had their Personal Information exposed, accessed and extracted by Cyberattackers or other third parties.

Defendants' Response to Security Breach

40. At some point in October 2019 or earlier, LifeLabs became aware of the Security Breach.

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

42. Without having had disclosed the Security Breach to those affected, LifeLabs proceeded to pay a ransom to the Cyberattackers to have the data unencrypted on the Computer Systems so as to allow LifeLabs to resume its own access to the data.

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

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

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

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

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

Defendants' Communications about the Security Breach

48. 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.

49. The Open Letter includes 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.

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

51. 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.

52. Beginning in January 2020, LifeLabs notified customers whose email addresses

were stored on the Computer Systems as part of LifeLabs' online appointment booking systems.

53. The statements that LifeLabs made to Class Members in the Open Letter and in direct communications were misleading to Class Members.

54. LifeLabs failed to provided 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.

55. 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.

Deficiencies

56. In January 2013, LifeLabs suffered a previous security breach whereby personal information from 16,000 of its customers in Kamloops, British Columbia was lost.

57. LifeLabs knew or ought to have known:

a) of the inadequacies in technical and procedural safeguards particularized below;

b) that they were particularly vulnerable to being hacked; and

c) that the Personal Information they stored was particularly sensitive/valuable and would be a target to hackers.

58. The Security Breach (and the extent of adverse consequences for LifeLabs' customers/patients) occurred as a result of LifeLabs having inadequate technical and procedural safeguards, inadequate information technology security policies and inadequate information-management practices. In particular, deficiencies included, but are not limited to:

a) failing to implement, manage and/or update the Computer Systems for ongoing monitoring and maintenance to address evolving digital vulnerabilities and threats so as to reasonably protect against breach;

b) storing unencrypted Personal Information on the Computer Systems and/or failing to implement sufficiently strong encryption and security safeguards to prevent the Personal Information from being subject to unauthorized access, collection, use, disclosure and copying;

c) providing greater access rights to users and applications than necessary and failing to restrict access privileges to necessary individual;

d) storing usernames and passwords without salting and hashing;

e) failing to use firewalls, network segmentation and segregation;

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 use up-to-date hardware;

i) failing to act when it had actual or constructive knowledge that its security measures were inadequate to protect against a data breach into the Computer Systems;

j) failing to train employees to deal with phishing and other common attacks;

k) failing to employ or contract personnel with the necessary skills, education, training and expertise in encrypting data and/or securing the Computer Systems against unauthorized access;

l) failing to have in place, implement and/or adhere to a procedural protocol to be adhered to and followed by its personnel in the event of a breach of its Computer Systems;

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

n) failing to address (adequately or at all) the vulnerabilities exposed by previous well-publicized cyber attacks and previous breaches of privacy with respect to the Personal Information;

o) failing to monitor its Computer Systems for evidence of breach and, consequentially, failing to effect a timely identification of the Security Breach once it had occurred;

p) failing to warn customers/patients that its Computer Systems lacked adequate encryption / security and were therefore vulnerable to breach and

unauthorized disclosure of the Personal Information;

q) failing to comply with the minimum standards set out in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, C. 5;

r) negotiating with the Cyberattacker(s) and paying a ransom did not guarantee the Cyberattackers' complete disgorgement of the data - and therefore achieved no security against further improper use or disclosure of that data;

s) failing to notify provincial privacy commissioners and Class Members of the Security Breach adequately and/or in a reasonably timely manner;

t) failing to provide provincial privacy commissioners with relevant particulars, documents and investigations reports undertaken by, or on behalf of, LifeLabs regarding the Security Breach, for the benefit of the Plaintiff and the Class Members;

u) failing to properly investigate the Security Breach; and

v) when providing customers with notice of the Security Breach, failing to provide sufficient or accurate information so that Class Members could take steps to mitigate harm or risk from the Security Breach.

("the Deficiencies")

59. The Personal Information of Class Members remains vulnerable to further cyberattacks and nefarious use/disclosure.

60. LifeLabs paid a ransom to Cyberattackers but has not made any or reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, or modification of the Personal Information by the Cyberattackers or other third parties.

61. In its conduct amounting to the Security Breach, LifeLabs failed to adhere to its own privacy statements, privacy policies and terms of the Contracts.

62. LifeLabs knowingly and intentionally used security systems which were below the industry standards for the protection of Personal Information and in so doing disregarded the known interests of its customers/patients.

63. By way of the Deficiencies, *inter alia*, LifeLabs was reckless and/or intentional in its conduct amounting to the Security Breach.

64. In the alternative, LifeLabs' recklessness amounted to intentional conduct. In particular:

a) LifeLabs knew their Personal Information protection measures were grossly inadequate and also knew that their Computer Systems were particularly

vulnerable to being hacked, given the highly sensitive nature and the volume of Personal Information they stored. Despite this knowledge, LifeLabs continued to store the Personal Information with inadequate technical and procedural safeguards.

b) Prior to the Security Breach, LifeLabs had adverted to the risks of a cyberattack on its Computer Systems and engaged experts in cybersecurity 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 employed inferior staff, equipment, programs, as well as policies and procedures, in order to reduce the operating costs necessarily associated with meeting the industry standard applicable to the custodianship of such highly sensitive and valuable Personal Information.

65. The said reduction in operating costs was deliberate and willful and resulted in a financial gain to LifeLabs at the expense of the Plaintiff's and Class Members' fundamental right to personal privacy and security. It was only after the Security Breach that LifeLabs made a substantial investment in information security.

Harm Suffered

66. As a result of the Security Breach and the disclosure of their Personal Health Information, Class Members are suffering, and will continue to suffer indefinitely, an intrusion upon seclusion and moral damages including

humiliation, injury to dignity, loss of personal security and a highly offensive invasion into their private affairs.

67. As a result of the Security Breach and the disclosure of their Personal Identity Information, Class Members are exposed to a real and substantial risk of identity theft, cybercrime, phishing, extortion, fraud, injury to credit rating and further disclosure of their highly sensitive and valuable Personal Information; including the cost of monitoring and insuring against same.

The Plaintiff's Relationship with the Defendants

68. The plaintiff is a customer of LifeLabs, having obtained medical diagnostic laboratory testing services from LifeLabs on numerous occasions since approximately 1982.

69. LifeLabs collected, used and disclosed the plaintiff's Personal Information.

70. At all material times, the plaintiff's Personal Information was stored on computer systems in the control of LifeLabs when those computer systems were subject to the Security Breach.

71. LifeLabs did notify the plaintiff confirming that she might be affected by the Security Breach until mid-January 2020, over two months after LifeLabs had learned of the breach.

CAUSES OF ACTION

Negligence

72. It was reasonably foreseeable that a failure by LifeLabs to adequately protect Class Members' Personal Information would result in a security breach that would cause harm to the Class Members.

73. LifeLabs owed a duty to the Class Members to collect, create, use, store, and transmit their Personal Information securely. The Plaintiff pleads that LifeLabs breached its duty of care owed to Class Member as a result of its conduct as aforesaid.

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

Breach of Contract and Warranty

75. The Class Members, including the Plaintiff, entered into identical or very similar contracts in using LifeLabs' services ("the Contracts").

76. The Class Members agreed to use LifeLabs to conduct medical diagnostic laboratory testing, which required them to provide LifeLabs with Personal Information and to permit LifeLabs to create Personal Information about them. In exchange, LifeLabs 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 Statement and Privacy Policy.

77. LifeLabs breached the Contracts by failing to perform its contractual obligation to meet the standards set out in its Privacy Statement and Privacy Policy.

Intrusion upon Seclusion

78. LifeLabs committed the tort of Intrusion upon Seclusion against the Class Members. The Security Breach caused an invasion of privacy that a reasonable person would regard as highly offensive, causing distress, humiliation or anguish.

79. By way of the Deficiencies *inter alia*, LifeLabs engaged in conduct that was reckless and/or intentional in its conduct resulting in the Security Breach.

80. LifeLabs' recklessness amounted to intentional conduct. LifeLabs knew their Personal Information protection measures were grossly inadequate and also knew that their Computer Systems were particularly vulnerable to being hacked, given the highly sensitive nature and the volume of Personal Information they stored. Despite this knowledge, LifeLabs continued to store the Personal Information with inadequate technical and procedural safeguards.

81. LifeLabs invaded, without lawful justification, the Class Members' private affairs or concerns, in that its recklessness and negligence resulted in the Security Breach.

82. After the Security Breach, LifeLabs continued its reckless and negligent conduct by failing to take all reasonable steps to protect the Class Members' Personal Information, including immediately engaging experts to isolate and secure the affected Computer Systems.

83. The resulting intrusion upon seclusion was highly offensive, causing distress, humiliation and anguish. The Personal Information, which includes Personal Health Information, is highly sensitive and personal. Unauthorized access and disclosure, and the real and substantial risk of ongoing and future unauthorized access to such information has caused mental distress.

Violation of Personal Information Protection Act

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

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

86. By failing to implement sufficient encryption and security, LifeLabs breached section 34 of PIPA 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.

87. LifeLabs breached section 35 of PIPA BC by failing to destroy the Personal Information as required by that section.

88. The British Columbia Privacy Commissioner has made an order against LifeLabs for violations of the provisions of PIPA BC and LifeLabs is liable for damages pursuant to section 57(1) of PIPA.

89. The plaintiff pleads the comparable provisions of the *Personal Information Protection Act*, SA 2003, c. P-6.5.

Personal Health Information Protection Act, 2004 S.O. 2004, ch. 3 ("PHIPA")

90. Some of the Class Members' Personal Information collected and used by LifeLabs constitutes 'personal health information' as defined by section 4 of PHIPA.

91. 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.

92. 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.

93. In failing to protect Class Members' personal health information as aforesaid, LifeLabs is liable for damages pursuant to section 65 of PHIPA.

Violation of Provincial Privacy Statutes

94. LifeLabs failed to take appropriate steps to guard against unauthorized access to the Personal Information of the plaintiff and Class Members.

95. The aforementioned actions and omissions of LifeLabs were highly offensive and constitute intentional, willful and reckless violations of the plaintiff and the Class Members' privacy, causing the plaintiff and the Class Members to suffer damages as particularized below. As a result, the Defendants breached several provincial statutory provisions as follows.

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

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

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

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

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

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

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

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

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

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

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

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

(2) The nature and degree of privacy to which an individual is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and the relationship, whether domestic or other, between the parties.

100. Articles 35 and 37 of the *Civil Code of Quebec*, L.R.Q., c. C-1991 ("Quebec Civil Code") provide:

35. Every person has a right to the respect of his reputation and privacy. The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.

37. Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

101. Section 10 of *Act Respecting the Protection of Personal Information in the*

Private Sector, R.S.Q., c. P-39.1 ("**ARPPIP**") provides:

> 10. A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

Breach of Confidence

102. The information that the Plaintiff and the Class Members provided to LifeLabs was confidential and was conveyed in confidence. The Personal Information, including Personal Health Information, was highly sensitive in nature. The Plaintiff and the Class Members relied on LifeLabs' commitment to privacy, including as expressed in its Privacy Statement and Privacy Policy, as well as mandated by various legislative and industry standards, and this gave rise to an obligation of confidence. The Plaintiff and the Class Members reasonably expected their Personal Information to be kept in confidence.

103. The Personal Information was misused by LifeLabs to the detriment of the Plaintiff and the Class Members. LifeLabs failed to take all reasonable steps to protect the Class Members' Personal Information in accordance with its own commitments, including in its Privacy Statement and Privacy Policy, and the applicable legislative and industry standards, as set out above.

104. The misuse of the Personal Information resulted in the Security Breach which

has led to damage to the Plaintiff and the Class Members, particularized below.

Breach of Fiduciary Duty and Duty to Act in Good Faith

105. With respect to the protection and custodianship of their Personal Information, LifeLabs owed to the Plaintiff and Class Members a fiduciary duty and a duty to act in good faith and in their best interests ("the Fiduciary Duty").

106. LifeLabs breached their Fiduciary Duty by failing to implement adequate safeguards against unauthorized access and disclosure of the Personal Information and by choosing to withhold disclosure of the fact of this inadequacy and the resulting Security Breach unnecessarily and contrary to law. By its conduct, LifeLabs preferred its own interest to those of Class Members and, as a result, the privacy interests of members of the Class were detrimentally affected.

Negligent Misrepresentation

107. Through Lifelabs' Privacy Statement and Privacy Policy, LifeLabs represented to the Plaintiff and Class Members that their Personal Information would be safeguarded.

108. The representations in the Privacy Statement and Privacy Policy were untrue, inaccurate, and misleading in that LifeLabs did not collect, create, use, store, and transmit Personal Information in accordance with Lifelabs' Privacy Statement or

Privacy Policy. In particular, LifeLabs did not maintain the highest standards of personal information protection, including through data security, and did not review and update its security measures to meet industry standards.

109. LifeLabs acted negligently in making the representations in its Privacy Statement and Privacy Policy.

110. LifeLabs knew that the Plaintiff and Class Members would rely on the representations in its Privacy Statement and Privacy Policy.

111. The Plaintiff and Class Members relied on the representations made in the Privacy Statement and Privacy Policy to their detriment, and suffered damage, particularized below, as a result.

112. The Plaintiff and the Class Members trusted that LifeLabs was in the process of remedying the deficiencies that led to the Security Breach. As a result, Class Members did not take further investigative action on their own and continued to use Lifelabs' services.

113. The Plaintiff and Class Members suffered damage, particularized below, as a result.

Breach of Consumer Protection Act

114. The interactions between the Class Members and LifeLabs constitute a consumer transaction pursuant to the *Consumer Protection Act*, 2002, S.O. 2002, c.30.

115. The Representations were false, misleading or deceptive and constitute unfair practices under the Consumer Protection Act.

116. The plaintiff, on her behalf and on behalf of the Class Members, claims damages for the said unfair practices pursuant to the Consumer Protection Act.

117. A waiver is sought in respect of the notice requirement of section 18 of the *Consumer Protection Act*.

DAMAGES

118. As a result of LifeLabs' negligence, breach of contract, breach of confidence, negligent misrepresentation, intrusion upon seclusion and statutory breaches, the Plaintiff and Class Members suffered damages including, but not limited to:

a) Substantial exposure to the risk of identity theft, cybercrime, phishing, extortion, fraud, injury to credit rating, damage to reputation and/or the wasted time and expense of monitoring and insuring against same;

b) Loss of privacy, injury to dignity and mental distress from having highly sensitive Personal Information disclosed to unknown and unauthorized

persons;

c) Loss of privacy, injury to dignity and mental distress from providing LifeLabs with highly sensitive Personal Information, including Personal Health Information, and/or continuing to allow LifeLabs to store highly sensitive Personal Information, on the assurance that experts were engaged to remedy the procedural and technical deficiencies when in fact such Personal Information remains highly vulnerable to further attack and thus further disclosure and/or use by the Cyberattackers or other third parties;

d) 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 accessed from the Security Breach;

e) Damages as a result of the Personal Information being inaccessible to Class Members and their health care providers between the date of the Security Breach and the date that the data was unencrypted.

f) The costs and expense of credit monitoring, identity theft protection and online security education.

119. Given that its acts and/or omissions amount to recklessness and intentionality, LifeLabs is jointly and severally liable with the Cyberattackers for intentional

and negligent conduct causing the Plaintiff and Class Members harm.

Punitive Damages

120. The Defendants' conduct was high-handed, reckless, without care, deliberate, and in disregard of the rights of the Plaintiff and Class Members.

121. The Defendants prioritized profit over the privacy, security and dignity of the Plaintiff and the Class Members which conduct warrants an award of punitive damages.

STATUTES

122. The Plaintiff relies on the following British Columbia statutes:

a) *Class Proceedings Act*, RSBC 1996, c. 34;

b) *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c. 28 ("CJPTA");

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

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

e) *Negligence Act* [RSBC 1996] chapter 333.

123. The Plaintiff relies on the following Alberta statutes:

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

124. The Plaintiff relies on the following Saskatchewan statutes:

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

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

125. The Plaintiff relies on the following Manitoba statutes:

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

126. The Plaintiff relies on the following Ontario statutes:

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

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

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

d) *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3

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

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

127. The Plaintiff relies on the following Newfoundland and Labrador statute:

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

128. The Plaintiff relies on the following Quebec statute:

a) *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40, and *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1

129. The Plaintiff relies on the following federal statutes:

a) *Personal Information Protection and Electronic Documents Act*, SC 2000, c.

5 ("PIPEDA");

PLACE OF TRIAL

130. The plaintiff proposes that this action be tried at the City of Toronto.

SERVICE OF FOREIGN DEFENDANTS

131. Pursuant to Rule 17.04(1), the plaintiff pleads and relies 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. and Excelleris Technologies Inc. outside of Ontario without a court order.

Dated: October [ ] 2020.

MCPHADDEN SAMAC TUOVI LPP
161 Bay Street, 27th Floor
Toronto, Ontario M5SJ 2S1

Bryan C. McPhadden LSO# 28160K
Tel: (416) 601-1020Fax: (416) 601-1721

Lawyers for the Plaintiff