Court File No: CV-19-00633194-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N

MICHAEL FELDBERG and DANIEL FELDBERG

Plaintiffs

- and -

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

Defendants

STATEMENT OF CLAIM

(Notice of Action issued December 19, 2019)

Proceeding under the *Class Proceedings Act, 1992*

OVERVIEW

1. LifeLabs is the largest private medical testing company in Canada, providing diagnostic medical testing services to millions of Canadians each year. In the course of its business, LifeLabs collects a significant amount of Personal Information,[1] including very sensitive Personal Health Information,[2] regarding each of those millions of customers.

---

[1] Personal Information is defined in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, as "information about an identifiable individual".

[2] Personal Health Information is defined in the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A, to include identifying information about an individual in oral or recorded form, if the information, *inter alia*:

(a) relates to the physical or mental health of an individual, including information that consists of the health history of the individual's family;
(b) relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual;
(c) relates to payments or eligibility for health care in respect of the individual;
(d) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
(e) is the individual's health number, or;

2. 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 health information that it collects and stores.

3. In reality, LifeLabs employed inadequate and ineffective cybersecurity, with the result that hackers were able to gain access to LifeLabs' computer network. As a result of this access, the hackers were able to access without authorization, and to extract, the Personal Information of approximately 15 million Canadians (the "Breach").

4. After gaining access to LifeLabs' computer network and effecting the Breach, the hackers demanded, and LifeLabs paid, an undisclosed amount of money as ransom in an attempt to secure the data.

5. LifeLabs then proceeded to keep their customers in the dark regarding the Breach for almost two months, only issuing a public notice when compelled to do so by regulatory authorities.

6. The plaintiffs now bring this action on behalf of all persons, excluding the defendants and the defendants' executives, whose Personal Information was collected by a LifeLabs Facility (as defined below) located in Ontario, and then accessed and/or extracted in the Breach (the "Class" or "Class Members").

7. The plaintiffs propose that the Class be divided into two subclasses:

(a) Class Members who provided their Personal Health Information to LifeLabs (the "Direct Subclass"); and

(b) Class Members whose Personal Information was provided to LifeLabs only by a third-party health information custodian (the "Indirect Subclass").

(f) identifies an individual's substitute decision-maker.

RELIEF SOUGHT

8. As a result of the defendants' actions, and in particular the failure to take reasonable actions to protect the extremely sensitive Personal Information, including Personal Health Information, of the plaintiffs and Class Members, the plaintiffs and Class Members have suffered and will continue to suffer damages.

9. The plaintiffs, on their own behalf and on behalf of the Class Members, claim:

(a) an order pursuant to the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 (the "*CPA*"), certifying this action as a class proceeding and appointing them as representative plaintiffs of the Class;

(b) a declaration that the defendants owed a duty of care to the plaintiffs and the Class Members, and breached the standard of care owed to them;

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

(d) a declaration that the defendants breached the confidence of the plaintiffs and the Class Members;

(e) a declaration that the defendants breached the statutory privacy rights of the Class Members, as set out in the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A (the "*PHIPA*");

(f) a declaration that the LifeLabs defendants are liable for breach of contract;

(g) a declaration that the LifeLabs defendants violated the *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Sched. A (the "*Consumer Protection Act*");

(h) damages in an amount to be determined prior to trial;

(i) punitive damages;

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

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

(l) pre-judgment and post-judgment interest, compounded, or pursuant to ss. 128 and 129 of the *Courts of Justice Act*, R.S.O. 1980, c. 43 (the "*CJA*");

(m) costs of this action on a partial indemnity basis, together with applicable taxes thereon;

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

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

THE PARTIES

Michael Feldberg

10. The plaintiff Michael Feldberg ("Michael") is an individual residing in Toronto, Ontario.

11. Michael has attended at LifeLabs for medical testing on numerous occasions over the last ten years, with the result that LifeLabs has collected and retained a significant amount of Michael's Personal Information, including his name, date of birth, address, and telephone numbers, and personal health information, including his health card number and medical test results.

12. Since at least 2016, Michael has maintained a "My Results" account on the LifeLabs website that provides him with online access to view and download his medical test results. In addition to his Personal Health Information which was collected and retained by LifeLabs,

Michael provided LifeLabs with additional Personal Information in order to sign up for an online account, including his email, login information, password, and credit card information.

Daniel Feldberg

13. The plaintiff Daniel Feldberg ("Daniel") is an individual residing in Toronto, Ontario. Daniel has attended at LifeLabs for medical testing on numerous occasions over the last ten years, with the result that LifeLabs has collected and retained a significant amount of Daniel's Personal Information, including his name, date of birth, address, telephone numbers, and email address, and personal health information, including his health card number and medical test results.

Defendants

14. The defendant LifeLabs Inc. is federally incorporated company headquartered in Toronto, Ontario.

15. LifeLabs Inc. is the general partner of the defendant LifeLabs LP, a limited partnership incorporated under the laws of Ontario and headquartered in Toronto, Ontario. LifeLabs Inc. and LifeLabs LP collectively do business under the registered name LifeLabs and are referred to as such herein.

16. LifeLabs' primary business is the conducting of a range of medical testing. LifeLabs is comprised of four corporate divisions:

(a) LifeLabs Medical Laboratory Services, which conducts general diagnostic medical tests;

(b) LifeLabs Genetics, which conducts genetic testing and provides related services;

(c) Rocky Mountain Analytical, which conducts urine and hair element analysis, food sensitivity testing, and saliva hormone testing; and

(d) Excelleris, which is a health information exchange platform.

17. Excelleris provides electronic access to, and storage of, health care information and lab results to customers, healthcare providers, hospitals and health authorities. Essentially, the other three corporate divisions collect and generate Personal Health Information, while Excelleris is the vehicle by which customers' Personal Information, including Personal Health Information, is stored and disclosed.

18. Excelleris is operated by the defendant Excelleris Technologies Inc., a corporation incorporated under the laws of British Columbia and headquartered in Vancouver, British Columbia, with an extra-provincial registration in Ontario. Excelleris Technologies Inc. is a wholly owned subsidiary of LifeLabs Inc. and carries on business in Ontario.

19. At all material times, the defendants functioned as one organized business unit pursuing common objectives. Accordingly, each defendant is vicariously responsible for the acts and omissions of the other defendants, as particularized herein.

20. Both LifeLabs and Excelleris are custodians of customer personal health information pursuant to the *PHIPA*. Every LifeLabs and Excelleris employee with the ability to access customer personal health information is an "agent", pursuant to the *PHIPA*, who acts for or on behalf of the custodian with respect to the personal health information of the Class Members.

FACTS

Background

21. LifeLabs owns and operates a network of medical testing facilities across Canada, including several laboratories and over 220 collection centres (as defined in the *Laboratory and Specimen Collection Centre Licensing Act*, R.S.O. 1990, c. L.1) in Ontario (collectively, the "LifeLabs Facilities").

22. 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.

Class Members who have never had direct dealings with LifeLabs and fall into subcategory (c) above make up the Indirect Subclass.

LifeLabs' collection of Personal Information

23. 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.

24. 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; and

(f) health card number.

25. 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.

26. Most LifeLabs requisition forms contain additional Personal Health Information, such as the name and contact information for the customer's primary care physician. For example: the standard laboratory requisition form also includes a box for "additional clinical information (*e.g. diagnosis*)"; the requisition form for a PULS cardiovascular health test includes additional information about the customer's cardiovascular health history and risk factors, as well as the customer's private health insurance status; the cytology & HPV testing requisition form includes additional information about the customer's pap screening status, menstrual period, cervix, birth control, and pregnancy status; and so on.

27. Because a requisition form must accompany every sample to be tested, regardless of whether the sample is provided directly to LifeLabs or through another medical facility, LifeLabs collects, retains and stores the Personal Information, including Personal Health Information, of many people (*i.e.* the Indirect Subclass Members) who are unaware that their information has been collected by LifeLabs.

28. LifeLabs creates an Excelleris account pertaining to each of the individuals on whose sample(s) it performs testing. This Excelleris account contains the information from the customer's requisition form(s) and test result(s), and is accessible to physicians and medical practitioners through a platform named "Launchpad".

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

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

31. 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.

32. 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.

33. The LifeLabs website states, in its Terms of Use, that the use of the website, which includes use of the "My Results" and/or "Save My Spot" platforms, is governed by the laws of the Province of Ontario.

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

Applicable privacy standards

35. LifeLabs' website states that it has "robust privacy policies, procedures and training in place that are in compliance with applicable privacy laws".

36. One privacy policy (the "LifeLabs Privacy Policy") is posted on LifeLabs' website. It purports to govern all use of the LifeLabs website, which includes the "My Results", "Save My Spot" and "Launchpad" platforms described above and states, *inter alia*:

> **Accountability**: [LifeLabs is] accountable to protect and safeguard [customer] Personal Health Information…
>
> **Limiting Use, Disclosure and Retention**: Personal health information will not be used or disclosed for purposes other than those for which the information is collected or as required or permitted by law.
>
> …
>
> **Safeguards**: LifeLabs takes security measures to ensure [customer] personal health information is protected from loss, theft, unauthorized access, use, copying or disclosure. As a health information custodian, [LifeLabs] review[s] and update[s] security measures to meet industry standards. [LifeLabs has] implemented safeguards to protect [customer] personal information and these include but are not limited to:*Physical safeguards*: locking filing cabinets and restricting access to [LifeLabs] facilities to only authorized employees, vendors or visitors
> *Technical safeguards*: passwords, encryptions and firewalls
> *Administrative safeguards*: role based access, staff training, signing a confidentiality pledge.

37. Excelleris has its own Privacy Statement posted on its website (the "Excelleris Privacy Policy") which states, *inter alia*:

> **Accountability**
>
> - Excelleris is accountable to protect the privacy of the personal information in [its] care.
> - Excelleris trains its employees to follow written privacy policies and operational procedures, and also performs ongoing review of [its] privacy practices.
>
> **Identifying Purposes**
>
> - Excelleris does not collect personal information for its own purposes other than the maintenance of employee records.
> - Personal information is collected only as directed by the customers to whom it is providing services as an agent under a Customer Service Agreement or Information Sharing Agreement
>
> ...

Safeguards

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

38. Pursuant to s. 12 of the *PHIPA*, a health information custodian should takes all steps that are reasonable in the circumstances to ensure that Personal Health Information in the custodian's control is protected against theft, loss, and unauthorized use or disclosure, and to ensure that the records containing the Personal Health Information are protected against unauthorized copying or disposal.

39. Pursuant to s. 29 of the *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.

40. Ontario Regulation 856/93 "Professional Misconduct", made under the *Medicine Act, 1991*, S.O. 1991, c. 30, states that it is an act of professional misconduct for the purposes of clause 51(1)(c) of the *Health Professions Procedural Code* to "[give] information concerning the condition of a patient or any services rendered to a patient".

The Breach

41. On October 28, 2019, LifeLabs informed the British Columbia Ministry of Health that its network and data servers may have been subject to a cyberattack. Several days later, on November 1, 2019, LifeLabs also informed the Office of the Information and Privacy Commissioner of Ontario (the "IPC") and the Office of the Information and Privacy Commissioner for British Columbia (the "OPCBC") that it may have been subject to a cyberattack.

42. Shortly thereafter, LifeLabs confirmed to the IPC and the OPCBC that their computer systems were the subject of a cyberattack in which data had been accessed and extracted without

authorization. LifeLabs advised the IPC and the OPCBC at that time that the servers affected by the cyberattack contained the Personal Information of approximately 15 million customers, including: names, addresses, email addresses, customer logins and passwords, health card numbers, and lab test results.

43. LifeLabs advised further that the unidentified hackers who had penetrated their computer systems were demanding a ransom for the return of the extracted data.

44. None of these particulars of the Breach, or even the fact of the Breach's occurrence, were disclosed to the public or the Class Members until almost two months later, on December 17, 2019.

45. At that time, LifeLabs made a public announcement that the Breach had occurred. In that announcement, LifeLabs disclosed that the Breach had affected the Personal Information of 15 million Canadians, but stated that only approximately 85,000 LifeLabs customers (all based in Ontario) had had their lab test results accessed and extracted without authorization. It also confirmed that a ransom demand had been made and that a payment had been made to "retrieve the data".

46. LifeLabs has provided no information regarding the amount of the ransom demand, what the hackers 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 if there exists any methodology capable of confirming whether the data extracted in the Breach was distributed or copied in any way.

47. To date, some, but not all, LifeLabs customers with "Save My Spot" portal accounts have received email notifications from LifeLabs confirming that their "online appointment booking account was within the systems that were potentially affected".

48. To date, it has not been confirmed whether LifeLabs has provided direct notice of the Breach to any other individuals, including the approximately 85,000 LifeLabs customers who are confirmed to have had their lab test results accessed and extracted without authorization.

49. The IPC and the OPCBC are currently engaged in an ongoing investigation of the circumstances of the Breach.

Significance of the accessed / extracted data

50. Personal Health Information lies near the biographical core of personal information and is one of the most sensitive types of personal information.

51. While Personal Health Information is frequently shared for a variety of legitimate and necessary purposes, the collection, storage, use, retention, and/or disclosure of Personal Health Information is highly regulated in recognition of the fundamental, quasi-constitutional nature of the right to privacy.

52. Hackers who extract large quantities of Personal Information, including Personal Health Information, will often sell the information online, or use it to attempt fraud, or both.

53. Individuals affected by privacy breaches may find themselves the target of attempted identity theft or other fraud. They may end up subject to an increased volume of "phishing" attacks, where hackers pose as trustworthy sources and attempt to obtain even more sensitive information which might lead to attempted identity theft or other fraud in the future.

54. Phishing attacks become more sophisticated and dangerous when hackers have access to more private information to use. For example, a person will be much less likely to suspect that an email is not legitimate if it appears to be coming from their primary care physician. The more information a hacker has, the more difficult it becomes for recipients to distinguish which communications are potentially dangerous.

55. Since the data from the Breach has been stolen and there is likely no way to prevent it from being sold or posted online at a later time, despite the payment of the ransom demand, the risks associated with this privacy breach will continue on as credible threats for years.

56. Finally, individuals frequently recycle usernames and passwords across multiple online accounts. For example, Excelleris permits LifeLabs customers to use the same password for the My Results and Save My Spot platforms. Accordingly, extracting the login information and associated password of any given population of individuals will also provide a hacker with access to other online accounts of a significant proportion of that population.

57. The risk that other online accounts will be compromised is exacerbated where, as here, the cyberattack and ensuing privacy breach are not reported promptly to the individuals who are affected.

RIGHTS OF ACTION

Negligence

58. The defendants owed a duty of care to the Class Members to collect, store, use, retain, and/or disclose their Personal Information only in accordance with legislative, regulatory and professional standards, as well as internal policies. Specifically, the defendants owed a duty of care to the Class Members to take all reasonable steps to ensure that:

a) their Personal Information, including their Personal Health Information, would only be used for the provision of medical testing services;

b) their collected Personal Information, including Personal Health Information, would be kept confidential and secure, including being stored and transported or transferred in compliance with the *PHIPA*, applicable principles from the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

("*PIPEDA*"), any other legislative or regulatory standards, any applicable industry standards, the LifeLabs Privacy Policy, and the Excelleris Privacy Policy; and

c) any of their collected Personal Information, including Personal Health Information, would not be disseminated or disclosed to the public or to any unauthorized individuals without their express consent.

59. The plaintiffs and Class Members plead that the defendants breached their duty of care, particulars of which include:

(a) failing to collect, store, use, retain, and/or disclose the Class Members' Personal Information only in accordance with appropriate legislative, regulatory and industry standards;

(b) failing to collect, store, use, retain, and/or disclose the Class Members' Personal Information only in accordance with the LifeLabs Privacy Policy and Excelleris Privacy Policy;

(c) failing to collect, store, use, retain and/or disclose the Class Members' Personal Information in a manner that ensured that it would not be lost to, disclosed to, accessed by, or used by unauthorized persons;

(d) failing to properly supervise their employees, and/or failing to provide their employees with proper training with regard to the collection, storage, use, retention, and/or disclosure of Personal Information, including Personal Health Information;

(e) failing to establish, maintain and enforce appropriate cybersecurity measures, programs, and/or policies to keep the Class Members' Personal Information

confidential, and to ensure that it would not be lost to, disclosed to, accessed by, or used by unauthorized persons;

(f) failing to properly supervise their employees, and/or failing to provide their employees with proper training with regard to network and cybersecurity management;

a) failing to provide notice of the Breach to the Class Members in a reasonably timely manner;

b) failing to offer sufficient credit monitoring services to the Class Members;

c) with regard to the LifeLabs defendants, relying on Excelleris to keep the Class Members' Personal Information secure without taking reasonable steps to ascertain whether Excelleris' cybersecurity measures were adequate to safeguard the Class Members' Personal Information and were compliant with industry standards; and

d) with regard to the LifeLabs defendants, failing to ensure and/or determine, to the extent that Excelleris was responsible for ensuring that the Class Members' Personal Information remained confidential, that Excelleris had network and cybersecurity management sufficient to ensure that the Class Members' Personal Information remained confidential.

60. As a result of the defendants' negligence, unidentified hackers were able to gain access to the Class Members' Personal Information and Personal Health Information, resulting in the Class Members sustaining damages.

Intrusion upon seclusion

61. The defendants are jointly liable for the tort of intrusion upon seclusion because their reckless conduct facilitated the deliberate intrusion of the unidentified hackers.

62. Specifically, the tort of intrusion upon seclusion is made out because:

(a) the unidentified hackers intentionally invaded the Class Members' privacy;

(b) the defendants' reckless conduct regarding cybersecurity and the protection of Personal Information facilitated the hackers' ability to invade the Class Members' privacy and led directly to the invasion of the Class Members' privacy;

(c) there was no lawful justification for the invasion of the Class Members' privacy; and

(d) a reasonable person would consider the invasion of the Class Members' Personal Information, particularly the Personal Health Information, to be highly offensive.

Breach of confidence

63. The Class Members' Personal Information was confidential information which was conveyed to the defendants in confidence, and in circumstances in which an obligation of confidence arose.

64. The defendants made unauthorized use of the Class Members' Personal Information, in that they:

(a) failed to make reasonable efforts to maintain the confidentiality of the Personal Information;

(b) failed to secure the Personal Information against such risks as theft, loss, and unauthorized use, disclosure, copying or disposal; and

(c) failed to give notice of the Breach for almost two months, thereby subjecting the Class Members to heightened risk of suffering identity theft or fraud.

Waiver of tort

65. In the alternative, the plaintiffs will waive the torts and claim the disgorgement of the defendants' financial gains associated with medical testing services during the time period for which they have maintained inadequate cybersecurity safeguards for customers' Personal Health Information.

Breach of the *PHIPA*

66. In engaging in the wrongful conduct as pleaded herein, the defendants have wilfully or recklessly contravened s. 12 of the *PHIPA*, causing actual harm and mental anguish to the plaintiffs and Class Members. They are therefore liable for awards of damages pursuant to s. 65 of the *PHIPA*.

Breach of contract

67. The plaintiffs and every Direct Subclass Member entered into a standard form contract with the LifeLabs defendants. In exchange for agreeing that LifeLabs could collect the Class Members' Personal Information, including their Personal Health Information, and their sample(s) customers were granted access to LifeLabs' services, including the medical testing services, and the use of LifeLabs' online services (the "Contract").

68. It was an express or implied term of the Contract that the LifeLabs defendants would be responsible for all of the Class Members' Personal Information under its control/possession and would establish, maintain and enforce appropriate cybersecurity measures, programs, and/or policies to keep the Class Members' Personal Information confidential, and to ensure that it would not be lost to, disclosed to, or used by unauthorized persons.

69. All of the provisions in the LifeLabs Privacy Policy are impliedly incorporated in to the Contracts.

70. The LifeLabs defendants are in breach of the terms of their Privacy Policy, including as follows:

(a) LifeLabs failed to take security measures to ensure that the Direct Subclass Members' Personal Health Information was protected from theft, unauthorized access, use, copying or disclosure;

(b) LifeLabs failed to review and update their security measures to meet industry standards; and

(c) LifeLabs failed to implement sufficient technical and administrative safeguards to protect the Direct Subclass Members' Personal Health Information.

71. In addition to breaches of the express Privacy Policy terms of the Contract, the LifeLabs defendants breached their implied contractual obligation to make all reasonable efforts to maintain confidentiality over the Direct Subclass Member's Personal Information.

72. The LifeLabs defendants are also liable to the Indirect Subclass Members for breach of the contracts formed between the LifeLabs defendants and the third-party medical clinicians/practitioners who provide the Subclass Members' Personal Information to LifeLabs (the "Indirect Contracts").

73. The plaintiffs plead that the right of the Indirect Subclass Members to sue on the Indirect Contracts is grounded in the principled exception to the privity principle.

74. While the Indirect Subclass Members are not parties to the Indirect Contracts, the parties intended the Indirect Subclass Members to be the beneficiaries of the Indirect Contracts. More specifically, the plaintiffs plead that the contractual provision which was breached was made with regard to the Indirect Subclass Members' Personal Information, and that a) the benefit of the provision was clearly intended to extend to the Indirect Subclass Members and b) the

Subclass Members therefore are not strangers to the contracts and may rely on them and sue in relation to their breach.

Breach of the *Consumer Protection Act*

75. The plaintiffs and Class Members entered into consumer transactions with the LifeLabs defendants, as defined in the *Consumer Protection Act*.

76. The LifeLabs defendants engaged in unfair practices by making false, misleading or deceptive representations to the Class Members regarding the security and confidentiality of their Personal Information, contrary to the *Consumer Protection Act*.

77. The LifeLabs defendants represented to the plaintiffs and Class Members that they maintained strict cybersecurity measures to safeguard their Personal Information and to prevent unauthorized access or disclosure. As evidenced by the occurrence of the Breach, the LifeLabs defendants, in fact, failed to maintain appropriate or adequate cybersecurity measures.

78. The plaintiffs and the Class Members are entitled to an award of damages in respect of the LifeLabs defendants' unfair practices.

79. It is in the interests of justice that the plaintiffs and Class Members receive a waiver of the notice requirement in s. 18 of the *Consumer Protection Act*

DAMAGES

80. As a result of the defendants' wrongful conduct pleaded herein, the plaintiffs and the Class Members have suffered and/or continue to suffer harms and injuries.

81. The defendants are liable to the Class Members for damages including, but not limited to:

(a) serious and prolonged mental distress;

(b) damages to credit reputation and costs incurred in rectifying identity theft or fraud or, in the alternative, costs incurred in preventing identity theft or fraud; and

(c) out-of-pocket expenses.

82. In addition, the plaintiffs and Class Members seek moral damages for breach of confidence and intrusion upon seclusion.

83. The defendants' deliberate disregard for the confidentiality and security of the Class Members' personal health information constitutes a flagrant betrayal of their trust. This selfish, high-handed and callous conduct warrants condemnation of the Court through an award of punitive damages.

STATUTES

84. The plaintiffs plead and rely upon the *CJA*, the *CPA*, the *PIPEDA*, the *PHIPA*, the *Consumer Protection Act*, the *Negligence Act*, R.S.O. 1990, c. N.1, and the regulations made thereto.

PLACE OF TRIAL

85. The plaintiffs propose that this action be tried at the City of Toronto.

SERVICE OF FOREIGN DEFENDANTS

86. Pursuant to Rule 17.04(1), the plaintiffs 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 defendant Excelleris Technologies Inc. outside of Ontario without a court order.

Date: January 17, 2020

WADDELL PHILLIPS PC
36 Toronto Street, Suite 1120
Toronto, Ontario M5C 2C5
Tel: (647) 261-4486
Fax: (416) 477-1657

Margaret L. Waddell (LSO #29860U)
W. Cory Wanless (LSO #57288M)
Tina Q. Yang (LSO #60010N)

KLEIN & SCHONBLUM, ASSOCIATES
Barristers & Solicitors
2300 Yonge Street, Suite 2901
Toronto, Ontario M4P 1E4
Tel: (416) 480-0221
Fax: (416) 480-0017

David Fogel (LSO #58572A)

Lawyers for the Plaintiffs