Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

K.L.

Plaintiff

- and -

8303193 CANADA INC., ORGANIZATIONAL HEALTH (ONTARIO) INC., 8974012 CANADA INC., HOMEWOOD HUMAN SOLUTIONS CANADA INC., HOMEWOOD HUMAN SOLUTIONS INTERNATIONAL INC., 8824665 CANADA LTD., 7586787 CANADA INC., 4167546 CANADA INC., 7824092 CANADA LTD. and 7824076 CANADA INC. a.k.a. HOMEWOOD HEALTH INC.

Defendants

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

TO THE DEFENDANTS:

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

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

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

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

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

IF YOU PAY THE PLAINTIFF'S CLAIM, and costs, within the time for serving and filing your statement of defence you may move to have this proceeding dismissed by the Court. If you believe the amount claimed for costs is excessive, you may pay the plaintiff's claim and $400 for costs and have the costs assessed by the Court.

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

Date: February 7, 2023 Issued by .....
Local registrar

Ottawa Courthouse
161 Elgin Street, 2nd floor
Ottawa, ON K2P 2K1

TO: **HOMEWOOD HEALTH INC.**
150 Delhi Street
Guelph, ON N1E 6K9

Defendant

CLAIM

1. The plaintiff, on his own behalf and on behalf of the Class Members (as defined below) claims the following relief:

(a) An Order certifying this action as a class proceeding pursuant to the *Class Proceedings Act, 1992*, and appointing K.L. (a pseudonym) as representative plaintiff for the Class;

(b) A declaration that the defendant owed a non-delegable duty of care to the plaintiff and the Class Members with respect to the collection, use and storage of the plaintiff and Class Members' personal information, including a duty to keep it confidential and secure, and to ensure it would not be lost, disseminated, or disclosed to unauthorized persons.

(c) A declaration that the defendant owed a non-delegable fiduciary duty of care to the plaintiff and the Class Members with respect to the collection, use and storage of the plaintiff and Class Members' personal information, including a duty to keep it confidential and secure, and to ensure it would not be lost, disseminated, or disclosed to unauthorized persons.

(d) A declaration that the defendant breached the confidentiality and/or trust of the plaintiff and the Class Members with respect to the collection, use and storage of the plaintiff and Class Members' personal information, including a duty to keep it confidential and secure, and to ensure it would not be lost, disseminated, or disclosed to unauthorized persons.

(e) A declaration that the defendant breached a contract with the plaintiff and the Class Members in which it was required by the terms of the contract to collect, use, and

store the plaintiff and Class Members' personal information, including a contractual duty to keep it confidential and secure, and to ensure it would not be lost, disseminated or disclosed to unauthorized persons.

(f) A declaration that the defendant breached the Provincial statutory privacy rights of the plaintiff and Class Members as set out in the *Personal Health Information Protection Act, 2004*, SO 2004, c 3 Sch A (the "*PHIPA"),* and similar legislation applicable in Provinces and Territories outside of Ontario;

(g) A declaration that the defendant breached the Federal statutory privacy rights of the plaintiff and Class Members as set out in the *Personal Information Protection and Electronic Documents Act* S.C. 2000, c. 5 (the "*PIPEDA");*

(h) Damages in the amount of $100,000,000 or such other amount as may be fixed by the court on an aggregate or individual basis;

(i) Punitive, aggravated and exemplary damages in the amount of $25,000,000 or such other amount as may be fixed by the Court;

(j) 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;

(k) Pre-judgment and post-judgment interest pursuant to ss. 128 and 129 of the *Courts of Justice Act*, RSO 1980, c 43 (the "*CJA*");

(l) Costs of this action, together with applicable taxes thereon;

(m) The costs of providing notice to the class of certification, resolution of the action, results of the common issues trial, and administering the plan of distribution of the recovery in this action; and

(n) Such further and other relief as this Honourable Court deems just.

THE PARTIES

Homewood Health Inc.

2. The defendant, Homewood Health Inc., is a federally incorporated corporation with its registered head office located in Guelph, Ontario.

3. The defendant reports that it has been providing mental health and addiction services since 1883. The defendant as it is currently known has a long history of incorporations and amalgamations.

4. Throughout the 2000s, a number of companies existed by the names of Homewood Human Solutions International Inc., 4167546 Canada Inc., Proact Human Solutions Inc., Homewood Human Solutions Canada Inc., Wilson, Banwell Assoc. Ltd., Wilson Banwell Human Solutions Inc., Human Solutions Canada Inc., 7824092 Canada Ltd., and 7824076 Canada Inc.

5. On April 1, 2011, by amalgamation certificate, the former companies referred to above were amalgamated to create Homewood Human Solutions International Inc.

6. On May 6, 2011, this corporation changed its name to Homewood Human Solutions Canada Inc.

7. On September 13, 2011, by amalgamation certificate, Homewood Human Solutions Canada Inc. and another corporation named 7586787 Canada Inc. amalgamated to form Homewood Human Solutions Canada Inc.

8. On December 21, 2013, this corporation changed its name to Homewood Health Inc.

9. On April 1, 2014, by amalgamation certificate, Homewood Health Inc. and 8824665 Canada Ltd. amalgamated to form Homewood Health Inc.

10. On December 1, 2014, Homewood Health Inc., Organizational Health (Ontario) Inc. and 8974012 Canada Inc. all amalgamated to form Homewood Health Inc.

11. On April 1, 2021, Homewood Health Inc., as it is currently known and named, was formed federally under the *Business Corporations Act* by amalgamation of Homewood Health Inc. and 8303191 Canada Inc.

12. The corporate entity, 8303191 Canada Inc. was previously registered in Quebec and was incorporated on September 24, 2012.

13. As of June 23, 2021, Homewood Health Inc. is registered to operate in all provinces and territories across Canada.

14. Homewood Health operates a Homewood Health Centre that provides mental health and addiction services to individuals across Canada, with its national network of over 4,500 employees and clinical experts. Homewood Health’s services includes organizational wellness, employee and family assistance programs, assessments, outpatient and inpatient treatment, recovery management, and return to work and family support services.

15. As part of its services, Homewood Health offers its services through an "Employee and Family Assistance Program" ("EFAP") for participating businesses and organizations. Businesses and organizations participating through the EFAP include, but are not limited to: BC Housing, TransLink, BC Provincial Health Services Authority, University of Waterloo, University of Alberta, Workers' Compensation Board of Alberta, the City of Spruce Grove, Construction Labour Relations, Fortis Alberta, Alberta Motor Association, the University of Lethbridge and Bow Valley College, Alberta Health Services, National Energy Board, Canada Revenue Agency, Wellness Together Canada, HSBC, the Law Society of Ontario, the Law Society of Newfoundland and Labrador, Peel District School Board, Ontario Shores Centre for Mental Health Sciences, International Associate of Machinists and Aerospace Workers, and the Halifax Public Libraries.

K.L as the Proposed Representative Plaintiff

16. The plaintiff, K.L., is an individual residing in Alberta. He was a patient of Homewood Health for approximately seven (7) years. He accessed mental healthcare services from Homewood in 2015 and again in 2019.

17. The plaintiff was specifically advised by Homewood Health that his confidential health records were included in the Breach as described below.

18. K.L. seeks to be appointed as the representative plaintiff on behalf of a class of individuals whose personal information and personal health information was exfiltrated from Homewood's computer network in the March 2021 Data Breach (the "Breach", as defined below).

The Class

19. K.L. brings this action on behalf of all persons who are or were patients of Homewood Health from January 1, 2015 to August 5, 2021, excluding the defendant's senior executives, officers and directors, and unionized personnel (the "Class" or "Class Members").

20. The Class comprises all individuals whose Personal Information and/or Personal Health Information was accessed in the Breach, where:

(a) "Personal Information" means information about an identifiable individual;

(a) "Personal Health Information" has the same meaning as from s. 4(1) of the *PHIPA*;

(b) "Personal Health Information" has the same meaning as from s. 2(1) of the *PIPEDA;*

(c) The "Breach" is the event or series of events, culminating in or around March 2021, which has been confirmed by the defendant as having occurred, whereby unknown third-party hackers gained access to Homewood Health's computer network, and collected and exfiltrated data containing the Personal Information and Personal Health Information of the Class Members, and put the exfiltrated data up for bidding on a Dark Website called "Marketo".

FACTS IN SUPPORT OF ALL CAUSES OF ACTION

The plaintiff K.L. was a Homewood Health patient

21. In 2015, K.L. failed a drug and alcohol test while working as a member of a union in Alberta. His employer was a participant of Homewood Health's EFAP program. His employer required him to undergo rehabilitation as a result of his failed drug and alcohol test. As such,

K.L. participated in Homewood Health's EFAP program as it was made available through his employer.

22. K.L. attended one of Homewood Health's facilities in 2015 for about 28 days. He attended individual and group counselling sessions as well as "Alcoholics Anonymous" meetings. Homewood Health's treatment providers kept handwritten and/or electronically documented notes of K.L.'s sessions.

23. In 2019, K.L. failed a test for cannabis use while working as a member of a union in Alberta. His employer was a participant of Homewood Health's EFAP program. His employer required him to undergo rehabilitation as a result of his failed Cannabis use test. As such, K.L. participated in Homewood Health's EFAP program as it was made available through his employer.

24. K.L. participated in 12 one-on-one counselling sessions beginning in 2019 to address his cannabis use. Homewood Health's treatment providers kept handwritten and/or electronically documented notes of K.L.'s sessions.

25. To provide its patients with healthcare services, Homewood Health collects and retains Personal Information, including Personal Health Information, from patients and in some cases, their family members. To that end, Homewood Health collected Personal Information and Personal Health Information about K.L. while he was under their care. The information was recorded in hard copy paper form and in electronic form, which was stored on Homewood Health's computer network.

26. In advance of providing any services, Homewood Health also requested and received additional information from K.L. regarding his medical history, including particulars of his

medical condition, post-accident recovery and medications, as well as detailed information about his personal care abilities and habits, his eating habits, and his daily routine.

27. In K.L.'s case, Homewood Health collected highly sensitive information about K.L. throughout his addiction counselling services provided in 2015 and 2019.

28. K.L. understood that, at all material times, he had entered into a contractual agreement with Homewood for valuable consideration, as well as a doctor and patient relationship with Homewood. K.L. expected that, as a consequence of his contractual agreement, and as a consequence of the doctor-patient relationship, Homewood would collect, use and store his personal information, would keep it confidential and secure, and ensure it would not be lost, disseminated, or disclosed to unauthorized persons.

Homewood collected Personal Information and Personal Health Information from the Class

29. Homewood collected Personal Information from all Class Members. For those patients who paid out-of-pocket for Homewood Health services, Homewood Health also collected and retained their payment information, such as credit card or banking details.

30. The Class Members understood that, at all material times, they had entered into a contractual agreement with Homewood for valuable consideration, as well as a doctor and patient relationship with Homewood. The Class Members expected that, as a consequence of the contractual agreement, and as a consequence of the doctor-patient relationship, Homewood would collect, use and store their personal information, would keep it confidential and secure, and ensure it would not be lost, disseminated, or disclosed to unauthorized persons.

31. At the time of the Breach, Homewood Health provided services to tens of thousands of patients, and had collected, used, modified, and retained substantial amounts of sensitive Personal Health Information and Personal Information for each of those patients, both in hard copy and by electronic means. As such, Homewood Health is a health information custodian as that term is defined in s 3 of the *PHIPA*.

32. Homewood Health was, and is, obliged to secure and safeguard the employee and patient Personal Information in its custody or control, much of which was stored electronically on Homewood Health's computer networks. It was, and is, obliged to take reasonable steps to ensure that Personal Health Information in its custody or control is not access or disclosed without authority, including being protected against theft or loss, and to ensure that records containing Personal Health Information are protected against unauthorized copying, modification or disposal.

33. To the extent that Homewood Health delegated any responsibility for collecting, managing, storing, disclosing, securing, and/or deleting the Class Members' Personal Information to any other party or parties, Homewood Health is directly liable for resultant damages, because it held a non-delegable duty to secure the Class Members' Personal Information.

34. At all times, Homewood Health was obliged to have effective, current and robust cyber security protective measures in place to secure all of the patient and employee Personal Information which it collects and stores, including protection for attack by malicious third parties intent on exfiltration of the Personal Information for improper purposes.

35. Homewood Heath failed to do so. Its cyber security protective measures, if any, were antiquated, inadequate, unreasonable, and readily penetrable by third parties. Homewood

Health failed to encrypt the Personal Information stored on its computer network, which was a patent breach of the relevant standard of care that it was obliged to meet to protect Class Members' privacy.

Privacy Representations

36. At all material times, Homewood Health represented to its patients that it collects, uses, stores, and discloses patient Personal Information in accordance with the Ten Privacy Principles as defined by the Canadian Standards Association and through compliance with *PIPEDA* and substantially similar provincial legislation.

37. At all material times, Homewood Health's website contained the following representations about the security of its patients' personal information:

(a) Personal information is kept secure and protected, and it is only viewed by trained and authorized people involved in delivering your health care services;

(b) We take steps to protect your personal information from theft, loss, unauthorized access, copying, modification, use, disclosure, and disposal;

(c) We conduct audits and complete investigations to monitor and manage our privacy compliance. Any suspected breach or unauthorized access is investigated. Individuals are notified at the first reasonable opportunity when a breach presents a risk of significant harm; and

(d) We take steps to ensure that everyone who performs services for us protects your privacy and only uses your personal information for the purposes to which you have consented.

The Breach

38. In or around March 2021, a group of hackers contacted Homewood Health to advise that they breached the Homewood Health network and extracted data from its servers. The hackers alleged that they extracted 183 gigabytes of data from patients who accessed Homewood Health's services through the EFAP program before April 1, 2021. The compromised information included, *inter alia*, databases containing personal information of users of the defendant's services, as well as agreements, amendments, accruals, and projects.

39. The hackers provided a sample to the defendant that contained the personal identifying and health information of patients, including their name, date of birth, organization, job title, phone number, home address, and the patients' "situation". The "situation" describes the patients' specific mental health history and issues. This was presumably intended to demonstrate to the defendant the veracity of the hackers' claims.

40. Homewood Health allegedly commenced an investigation into the Breach but did not immediately notify the public, or even the individuals whose Personal Information was contained in the data sample provided by the hackers, that the Breach had occurred. Further, the defendant failed to immediately advise the appropriate Federal and Provincial Privacy Commissioners.

41. On July 19, 2021, the group of hackers published the exfiltrated data obtained from Homewood Health to a Dark Website called "Marketo", a self-described leaked data marketplace. Marketo can be accessed by anyone with an internet connection. The data was posted for sale.

42. In or around July 2021, the group of hackers provided Homewood Health with further evidence of the leaked data to pressure Homewood Health into paying a ransom.

43. In or around July 2021, Homewood Health began to notify its clients of the breach via an email blast. Homewood Health's notification to its clients did not include any particulars of the scope of the Breach. Homewood Health did not contact its clients via mail or phone to ensure that they were notified of the breach. As a result, most Class Members, including K.L., remained unaware that the Breach had occurred.

44. On July 27, 2021, CTV News reported that Homewood Health suffered a major data breach. CTV News reported that Homewood Health refused to estimate how many people's information was compromised.

45. CTV News contacted the Marketo site. A representative of the Marketo site named Mannus Gott informed CTV News that if the company [Homewood Health] understands and is willing to accept responsibility for the leak, there [would] be no publication.

46. Homewood Health began negotiating with Marketo on August 5, 2021 to purchase the leaked data. However, the leaked data exfiltrated through the Breach had already been available for sale on Marketo for at least 3 weeks prior to the negotiations.

47. The plaintiff and Class Members do not know the result of Homewood Health's negotiations with Marketo, nor if Homewood Health has paid the ransom to date.

48. The plaintiff and Class Members do not know if the leaked data was purchased by or sold to anyone.

49. The plaintiff and Class Members do not know if the leaked data continues to be available for sale by the original hackers or by any person or group that may have purchased the leaked data from the original hackers.

50. There is likely no way to know if the stolen data has been or will be reproduced, sold, or posted online at any time. The risks associated with this privacy breach will continue on as credible threats indefinitely.

Aftermath of the Breach

51. To date, Homewood Health has not disclosed what specific steps it has taken to remediate the Breach, and to update its cyber-security systems to avoid any future privacy breaches.

52. Homewood's response to the Breach has been entirely inadequate and unresponsive to the risks, embarrassment, humiliation, distress, anxiety, financial and reputation damage and expenses to which it has exposed the Class.

53. Rather than provide the affected individuals with timely disclosure of the relevant facts of the Breach, Homewood Health did not notify the Class of the Breach until sometime in or around July 2021 after the Breach occurred, and not until after portions of the Breach data, including the plaintiff's medical records, were leaked to the public. The failure to provide timely notice of the Breach to the Class exacerbated the risks and dangers to the Class arising from them having been the victims of a privacy breach.

54. The notice ultimately given to the Class or some portion thereof was wholly deficient and failed to adequately disclose to the Class Members the extent of the Breach, and the risk to the Class Members arising therefrom. Instead, Homewood Health downplayed the extent of the Breach and the risks to which they exposed the Class because of their negligence in

protecting the Class Members' sensitive Personal Information and Personal Health Information.

55. On February 24, 2022, Homewood Health sent K.L. an email advising him that his personal information was included in the Breach. They advised that the following information was included in the breach: name and contact information (for example, information such as email address, phone number, postal code, city, province), date of birth, employer, type of service provided or issue addressed, as well as health information related to the services provided. They did not call him or follow up with him in any other manner.

56. K.L. became aware of the Breach in 2022 after being notified of it via social media.

57. On February 23, 2022, K.L. contacted Homewood Health to ask if his personal information was compromised as a result of the Breach. Homewood Health confirmed that it was.

58. K.L. was shocked, embarrassed, and distressed to learn that the Breach occurred, and that, even 3 months after the fact, Homewood Health had not taken steps to inform him that his Personal Information had been accessed and stolen as part of the Breach.

59. The employees and members of numerous companies and organizations were compromised as a result of the leak, including but not limited to: University of Waterloo; Halifax Public Library; Workers Compensation Board of Alberta; University of Alberta; Dassault; Garda World Cash Services; Grupo Antolin; Eastlink; HSBC; National Energy Board; Seastar Solutions; Toronto Central; Translink; City of Spruce Grove; Construction Labour Relations; Fortis Alberta; Alberta Motor Association; University Lethbridge; Bow Valley College; and Iamaw 2323.

60. 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.

61. Personal Health Information lies at the core of individual privacy, and therefore demands enhanced and special protection.

62. 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. In addition to the inherently high privacy value to the individual, Personal Health Information is also accorded high value when trafficked on the black market. It has a high value because it is largely immutable, unlike passwords and credit card information which can be changed – with the result that compromised Personal Health Information has potentially very serious and long-lasting impacts. For these reasons, it is well-known that companies that collect Personal Health Information are highly attractive targets for cyber attackers, and they therefore are obliged to ensure that the Personal Health Information they store is safe from hacking, by employing state-of-the-art and current cyber security processes and software.

63. Companies like Homewood that choose to operate in the healthcare industry, and to collect customer data that includes Personal Health Information, therefore take on commensurate heightened responsibility to safeguard and protect patient privacy.

64. Individuals affected by privacy breaches may find themselves the target of attempted or actual 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 that might lead to further cyber security breaches, identity theft or

other fraud in the future. Phishing attacks become more sophisticated and dangerous when hackers have access to more private information. 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.

Personal Information and Personal Health Information

65. “Personal Health Information” is a defined term under the *PHIPA* and has the same meaning herein. It includes 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,

(f) Identifies an individual’s substitute decision-maker.

66. "Personal Information" is a defined term under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (the "*PIPEDA*") meaning "information about an "identifiable individual" and has that meaning herein.

Applicable privacy and cyber security standards

67. Pursuant to s 12 of the *PHIPA*, a health information custodian should take 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.

68. 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.

69. Homewood Health should have had multiple, redundant, overlapping and consistently updated cyber security measures in place, including the use of encryption, to ensure the protection of the Class Members' Personal Information, and to ensure that, even in the event of any breach, data containing Personal Information would be inaccessible and useless to hackers.

70. At a minimum, among other things, Homewood Health should have had the following protections in place to prevent the Personal Information of the Class Members from being exfiltrated:

(a) Personal Information should have been encrypted in storage and in transmission throughout the Homewood Health network;

(b) Encrypted Personal Information should have been accessible on a record-by-record basis only, to limit the scope of potential breaches;

(c) Encrypted databases should have been further protected by use of a master password accessible to only a limited number of trusted and well-trained users;

(d) Appropriate network segmentation should have been implemented, to limit access to sensitive Personal Information even if a network breach occurred;

(e) Proactive network monitoring processes should have been implemented, including activity logs and system alerts using next-generation persistent threat monitoring, to flag and stop the unauthorized exfiltration of sensitive information; and

(f) Advanced endpoint detection and response tools should have been in place to stop breaches before they occurred.

71. At a minimum, among other things, Homewood Health should have provided the Class Members with timely, fulsome notice of the nature and scope of the Breach.

CAUSES OF ACTION

72. The defendant is liable to the Class Members for negligence (breach of a duty of care), breach of contract, breach of a fiduciary duty of care, breach of *PHIPA* and other Provincial and Territorial privacy legislation, and breach of *PIPEDA*.

Negligence

73. The defendant 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 defendant owed a duty of care to the Class Members to take all reasonable steps to ensure that:

(a) The Class Members' Personal information, including their Personal Health Information, would only be used for the provision of healthcare services;

(b) Any of the Class Members' 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;

(c) Their collected Personal Information, including Personal Health Information, would be kept confidential and secure, including being stored in compliance with the PHIPA, applicable principles from the PIPEDA, any other legislative or regulatory standards, any applicable industry standards, and the Homewood Health Privacy Policies; and

(d) The Class Members' collected Personal Information, including Personal Health Information, would be subject to appropriate safeguards to protect against a cyber-attack and to limit the exposure of the Class Members' Personal Information even in the case of a successful cyber-attack.

74. The defendant breached its duty of care, particulars of which include:

(a) Failing to collect, store, use, retain, and/or disclose the Class Members' Personal Information, including Personal Health 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, including Personal Health Information, only in accordance with the Homewood Health Privacy Policies;

(c) Failing to collect, store, use, retain and/or disclose the Class Members' Personal Information, including Personal Health 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 supervise their employees properly, 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 cyber security measures, programs, and/or policies to keep the Class Members' Personal Information, including Personal Health Information, confidential, and to ensure that it would not be lost to, disclosed to, accessed by, or used by unauthorized persons;

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

(g) Failing to provide notice of the Breach to the Class Members in a reasonably timely manner;

(h) Failing to provide sufficient information about the Breach to the Class Members to allow them to understand the significance of the Breach and to take any possible steps to reduce the risk of harm or mitigate the harm that could result from the Breach;

(i) Relying on a third-party company to keep the Class Members' Personal Information secure without taking reasonable steps to ascertain whether the third-party company's

cyber security measures were adequate to safeguard the Class Members' Personal Information and were compliant with industry standards; and

(j) Failing to ensure and/or determine, to the extent that Homewood Health was responsible for ensuring that the Class Members' Personal Information remained confidential, that Homewood Health had network and cyber security management sufficient to ensure that the Class Members' Personal Information remained confidential.

75. Homewood Health knew or ought to have known that, because it was a healthcare provider, it was a valuable target for hackers including both those who would employ ransomware and those who would attempt to steal the stored Personal Information and Personal Health Information and sell or ransom it for gain. Homewood Health also knew or ought to have known that its cyber security was grossly inadequate and vulnerable to hackers, rendering their customers' Personal Information and Personal Health Information vulnerable to theft or compromise. Nevertheless, Homewood Health negligently, willfully and/or recklessly failed to have proper cyber security protections in place to protect the Personal Information of the Class Members.

76. As a result of the defendant's negligence, the Hackers took to the Class Members' Personal Information and Personal Health Information, resulting in the Class Members sustaining damages which is particularized below.

Breach of Contract

77. The plaintiff and Class Members entered into a standard form contract with the defendant for the provision of healthcare services (the "Patient Contract"). All of the terms in the Homewood Health Privacy Policies and Privacy Representations are impliedly incorporated into the Patient Contract.

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

79. The defendant breached its express and/or implied contractual obligation to make all reasonable efforts to maintain confidentiality over the plaintiff and Class Members' Personal Information, including as follows:

(a) It failed to take security measures to ensure that their Personal Information was protected from theft, unauthorized access, use, copying or disclosure;

(b) It failed to review and update its security measures to meet industry standards;

(c) It failed to implement sufficient technical and administrative safeguards to protect their Personal Information; and

(d) It failed to notify them of the Breach at the first reasonable opportunity to do so.

Breach of Fiduciary Duty

80. The defendant owed a fiduciary duty to the Class Members to collect, store, use, retain, and/or disclose their Personal Information, including Personal Health Information, only in accordance with legislative, regulatory and professional standards, as well as internal policies. This fiduciary duty arises by virtue of the fact that the Class Members, either on their own behalf or through the EFAP funded by contributions made by participating businesses

and organizations on behalf of their employees, were in a fiduciary relationship with the defendant.

81. In exchange for funds provided either by the plaintiff and Class Members or on their behalf through the EFAP, the defendant owed a fiduciary duty to the plaintiff and Class Members to act honestly, in good faith and in the best interests of the Class Members.

82. The defendant breached its fiduciary duty, particulars of which include:

(a) Failing to collect, store, use, retain, and/or disclose the Class Members' Personal Information, including Personal Health Information, only in accordance with the Patient Contract;

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

(c) Failing to supervise their employees properly, 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;

(d) Failing to supervise their employees properly, and/or failing to provide their employees with proper training with regard to network and cyber security management;

(e) Relying on a third-party company to keep the Class Members' Personal Information secure without taking reasonable steps to ascertain whether the third-party company's cyber security measures were adequate to safeguard the Class Members' Personal Information and were compliant with industry standards; and

(f) Failing to ensure and/or determine, to the extent that Homewood Health was responsible for ensuring that the Class Members' Personal Information remained confidential, that Homewood Health had network and cyber security management sufficient to ensure that the Class Members' Personal Information remained confidential.

83. As a result of the defendant's negligence, the defendant breached its fiduciary duty to act in the best interest of the plaintiff and the Class Members and in accordance with the Patient Contract.

BREACHES OF PROVINCIAL PRIVACY LEGISLATION

84. In addition, or in the alternative to the above, as applicable, on behalf of the Class, the plaintiff pleads as follows:

85. **Residents of the Province of British Columbia**: On behalf of the Class Members resident in the Province of British Columbia, the plaintiff pleads that the Defendant violated the Privacy Act, RSBC, c 373, as amended and Personal Information Protection Act [SBC 2003] CHAPTER 63.

86. **Residents of the Province of Manitoba**: On behalf of the Class Members resident in the Province of Manitoba, the plaintiff pleads that the Defendant violated The Privacy Act, CCSM c P125, as amended and The Personal Information Protection and Identity Theft Prevention Act, SM 2013, c 17.

87. **Residents of the Province of Newfoundland and Labrador**: On behalf of the Class Members resident in the Province of Newfoundland and Labrador, the plaintiff pleads that the Defendant violated the Privacy Act, RSNL 1990, c P-22, as amended and Personal Health Information Act, SNL 2008, c P-7.01.

88. **Residents of the Province of Saskatchewan**: On behalf of the Class Members resident in the Province of Saskatchewan, the plaintiff pleads that the Defendant violated The Privacy Act, RSS 1978, c P-24, as amended and The Health Information Protection Act, SS 1999, c H-0.021.

89. **Residents of the Province of Alberta**: On behalf of the Class Members resident in the Province of Alberta, the plaintiff pleads that the Defendant violated Personal Information Protection Act, SA 2003, c P-6.5 and the Health Information Act, RSA 2000, c H-5.

90. **Residents of the Province of New Brunswick**: On behalf of the Class Members resident in the Province of New Brunswick, the plaintiff pleads that the Defendant violated the Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05.

91. **Residents of the Province of Nova Scotia**: On behalf of the Class Members resident in the Province of Nova Scotia, the plaintiff pleads that the Defendant violated the Personal Health Information Act, SNS 2010, c 41.

92. **Residents of the Province of Ontario**: On behalf of the Class Members resident in the Province of Ontario, the plaintiff pleads that the Defendant violated the Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A.

93. **Residents of the Northwest Territories**: On behalf of the Class Members resident in the Northwest Territories, the plaintiff pleads that the Defendant violated the Health Information Act, SNWT 2014, c 2.

94. **Residents of the Territory of Yukon**: On behalf of the Class Members resident in the Territory of Yukon, the plaintiff pleads that the Defendant violated the Health Information Privacy And Management Act, SY 2013, c 16.

95. **Residents of the Province of Quebec**: On behalf of the Class Members resident in the Province of Quebec, the plaintiff pleads that the Defendant violated the Act respecting the protection of personal information in the private sector, CQLR c P-39.1.

DAMAGES

96. As a result of the defendant's actions, and in particular the defendant's failure to take reasonable actions to protect the extremely sensitive Personal Information and Personal Health Information of the plaintiff and Class Members, the plaintiff and Class Members have suffered and will continue to suffer damages.

97. The defendant is liable to the Class Members for damages including, but not limited to:

(a) Serious and prolonged mental distress and anguish;

(b) Damages to personal and credit reputation;

(c) Costs incurred in rectifying identity theft or fraud or, in the alternative, costs incurred in preventing identity theft or fraud;

(d) Out-of-pocket expenses;

(e) General damages to be assessed in the aggregate; and

(f) Special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable to Homewood's breaches as alleged herein.

98. The defendant's deliberate disregard for the confidentiality and security of the Class Members' Personal Information constitutes a flagrant betrayal of their trust. Homewood

Health knew that medical service providers, such as itself, are at a particularly elevated risk of being targeted by hacking efforts, that they were particularly vulnerable to being hacked, and that the data in their network would be a valuable treasure trove for hackers. Homewood Health knew or ought to have known that its actions would have a significant adverse effect on all Class Members. This selfish, high-handed and callous conduct warrants condemnation of the Court through an award of punitive damages.

99. Moreover, subsequent to learning of the existence of an extensive privacy breach affecting many of its patients and employees, Homewood Health failed to implement a timely, comprehensive notice program to inform affected individuals about the Breach. This conduct was further high-handed, reckless, without care, deliberate, and offensive to moral standards of the community.

STATUTES RELIED UPON

100. The plaintiff pleads and relies upon the *CJA*, the *CPA*, the *PHIPA*, the *PIPEDA,* and associated regulations.

PLACE OF TRIAL

101. The Plaintiff proposes that the trial of this action take place in Ottawa.

Date: February 7, 2023

FLAHERTY McCARTHY LLP
The Origin Building
179 Enterprise Blvd.
2nd Floor, Suite 200
Markham, ON
L6G 0A2

SEAN BROWN
LSO No.: 42202W
sbrown@fmlaw.ca

LAURA BASSETT
LSO No.: 79264H
lbassett@fmlaw.ca

CHRISTOPHER LUPIS
LSO No.: 79074V
clupis@fmlaw.ca

Tel: 416-368-0231
Fax: 416-368-9229

Lawyers for the Plaintiff and Putative Class Members

Electronically issued / Délivré par voie électronique : 08-Feb-2023
Ottawa Superior Court of Justice / Cour supérieure de justice

Court File No./N° du dossier du greffe : CV-23-00091324-00CP

K.L.
Plaintiff

and

HOMEWOOD HEALTH
Defendant

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding under the *Class Proceedings Act, 1992*, SO 1992, c 6, as amended

Proceeding commenced at OTTAWA

STATEMENT OF CLAIM

FLAHERTY McCARTHY LLP
The Origin Building
179 Enterprise Blvd.
2nd Floor, Suite 200
Markham, ON L6G 0A2

SEAN BROWN (sbrown@fmlaw.ca)
LSO No. 42202W

LAURA BASSETT (lbassett@fmlaw.ca)
LSO No. 79264H

CHRISTOPHER LUPIS (clupis@fmlaw.ca)
LSO No. 79074V

Lawyers for the Plaintiff and Putative Class Members