Court File No.:

ONTARIO
SUPERIOR COURT OF JUSTICE

Electronically issued
Délivré par voie électronique : 11-Sep-2020
Toronto

ARTHUR REDUBLO

Plaintiff

- and -

CAREPARTNERS/COMMUNITY NURSING SERVICES FOUNDATION

Defendant

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF CLAIM

TO THE DEFENDANT:

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: September 11, 2020

Issued by: _____
(Local Registrar)

Address of Court Office: Superior Court of Justice
330 University Avenue
Toronto, ON M5G 1R7

TO: **CAREPARTNERS/COMMUNITY NURSING SERVICES FOUNDATION**
139 Washburn Drive
Kitchener, ON N2R 1S1

CLAIM

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

(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 him as the representative plaintiff;

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

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

(d) a declaration that the defendant breached the statutory privacy rights of the plaintiff and the Patient Subclass Members (as defined below), as set out in the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A (the "*PHIPA*");

(e) a declaration that the defendant is liable to the Patient Subclass Members for breach of contract;

(f) a declaration that the defendant violated the *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Sched. A (the "*Consumer Protection Act*") with regard to the Patient Subclass Members;

(g) 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;

(h) punitive and exemplary damages in the amount of $10,000,000 or such other amount as may be fixed by the court;

(i) 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;

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

(k) costs of this action, together with applicable taxes thereon;

(l) 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

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

THE PARTIES

Arthur Redublo

2. The plaintiff, Arthur Redublo ("Arthur"), is an individual residing in Pickering, Ontario, with his wife and two young children. Arthur was a patient of CarePartners/Community Nursing Services Foundation ("CarePartners") for approximately two months in 2013, while he was convalescing from an injury.

3. Arthur 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 CarePartners's computer network in the 2018 Breach (as defined below).

The Class

4. Arthur brings this action on behalf of all persons, excluding the defendant's senior executives, officers and directors, whose Personal Information and/or Personal Health Information was accessed in the Breach (the "Class" or "Class Members"), where:

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

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

(c) the "Breach" is the event or series of events, culminating in or around June 11, 2018, whereby unknown third-party hackers gained access to CarePartners' computer network, and collected and exfiltrated data containing the Personal Information and Personal Health Information of the Class Members, which was confirmed by CarePartners on or about June 18, 2018.

5. The plaintiff proposes that the Class be divided into two subclasses:

(a) Class Members who were employees, dependent contractors, or independent contractors of CarePartners at the time of the Breach (the "Employee Subclass"); and

(b) Class Members who were patients of CarePartners at the time of the Breach (the "Patient Subclass").

Personal Information and Personal Health Information

6. "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.

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

CarePartners

8. The defendant, CarePartners, is an Ontario corporation, which is headquartered in the Township of Woolwich, Ontario.

9. CarePartners is one of Ontario's largest private healthcare services providers. It specializes in providing out-of-hospital care to patients at their homes, schools, or workplaces throughout Ontario, including personal support care, nursing care, rehabilitation care, caregiver support, palliative care, and healthcare information.

10. CarePartners has over 4,500 staff and contract workers who are included in the Employee Subclass.

11. CarePartners is a service provider partner of the fourteen Ontario Local Health Integration Networks ("LHIN"). CarePartners also provides staff for some LHIN clinics.

12. In addition to providing staff for LHIN operations, CarePartners operates its own network of clinics, which are located throughout the province. It also operates some clinics that are joint CarePartners/LHIN facilities.

13. At the time of the Breach, CarePartners had provided services to approximately 237,000 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, CarePartners is a health information custodian as that term is defined in s. 3 of the *PHIPA*.

14. CarePartners 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 CarePartners' computer network. It was, and is, obliged to take reasonable steps to ensure that Personal Health Information in its custody or control is not accessed 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.

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

16. At all times, CarePartners 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 from attack by malicious third parties intent on exfiltration of the Personal Information for improper purposes.

17. CarePartners failed to do so. Its cyber security protective measures, if any, were antiquated, inadequate, unreasonable, and readily penetrable by third parties. CarePartners even 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 the Class Members' privacy.

18. As a result of CarePartners' cyber security failures, in breach of its duty of care owed to the Class, at some time in or about 2018, the Breach occurred, wherein hackers gained unauthorized access to CarePartners' computer network, and exfiltrated data containing the Personal Information and Personal Health Information of hundreds of thousands of CarePartners patients and employees. The hackers demanded undisclosed amounts of money from CarePartners as a ransom in exchange for the hackers not posting or selling the Breach data online.

19. CarePartners declined to pay the ransom, with the result that the hackers did, in fact, disclose the Class Members' Personal Information and Personal Health Information to third parties, as detailed below.

20. Rather than provide the affected individuals with timely disclosure of the relevant facts of the Breach, CarePartners did not notify the Class of the Breach until months after the Breach occurred, and not until after portions of the Breach data, including the plaintiff's medical records, were leaked to the media. 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.

21. 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, CarePartners 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.

FACTS

The plaintiff was a CarePartners patient

22. In 2013, Arthur was involved in a serious accident. He was hospitalized for several weeks. When he was discharged from hospital, Arthur's medical team directed that he receive at-home nursing care to support his recovery.

23. The Central East LHIN arranged for CarePartners to provide at-home nursing care to Arthur for approximately two months following his discharge from hospital. Later in his recovery,

Arthur also travelled several times to a Central East LHIN nursing clinic in Scarborough to receive care.

24. In order to provide its patients with healthcare services, CarePartners collects and retains Personal Information, including a wealth of Personal Health Information, from patients and their family members. To that end, CarePartners collected Personal Information and Personal Health Information about Arthur while he was under their care. The information was recorded in hard copy paper form and also in electronic form, which was stored on CarePartners' computer network.

25. In Arthur's case, the Central East LHIN provided CarePartners with clinical notes and records from Arthur's hospitalization. These clinical notes and records included his contact information, provincial health insurance information including his Ontario Health Insurance Plan ("OHIP")/health card number, date of birth, detailed medical information, and pictures of his body.

26. In advance of providing any services, CarePartners also requested and received additional information from Arthur 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. Because CarePartners provided nursing care primarily at Arthur's house, CarePartners also requested and received additional Personal Information from Arthur, including: his wife's contact information; information about his wife and children's daily routine; information pertaining to Arthur's employment, his wife's employment, and their children's school; and information about the family house and property, including security details such as codes for the home alarm system.

28. CarePartners collected additional Personal Information from Arthur and his family, in the same categories as those described above, in the course of providing care to him.

CarePartners collected Personal Information and Personal Health Information from the Class

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

30. CarePartners also collected a wide variety of Personal Information from its approximately 4,500 employees and contractors, including: contact information, dates of birth, social insurance numbers, payroll data including bank account information, and performance data including performance reviews and incident reports.

Privacy representations

31. At all material times, CarePartners represented to its patients that it collects, uses, stores, and discloses patient Personal Information in accordance with its Privacy Pledge, which states as follows:

> At CarePartners, we are dedicated to protecting patient privacy. We adhere to all applicable legislation, including the Ontario Personal Health Information Protection Act. To keep patient information safe, our practices are guided by the principals of our Privacy Pledge:
>
> - We pledge to keep the information patients/service partners share with us safe and secure at all times.
>
> - We collect and use patient information only for purposes that have been consented to – to assist us in providing appropriate, safe, high quality care.

- We minimize access to patient information within our organization by only granting access to those employees involved in the administration and delivery of the patient's care.

- We follow our policies and procedures and all applicable legislative requirements to ensure that patient information is kept current, accurate and secure.

- We educate our staff in strong privacy management practices, and have each employee sign a Pledge of Confidentiality to demonstrate their commitment to keeping patient information safe.

- We hold our staff accountable for their behavior. If a privacy breach does occur, it will always be managed promptly and patients will be notified if their information is ever at risk.

- We respect patient consent directives. No information will be disclosed to a third party unless the patient provides prior consent, OR in extenuating circumstances in which discourse is a legal requirement.

- If we contract another organization or Health Care Provider to provide care to our patients, we will hold them accountable to our standards of information protection.

We have a dedicated privacy representative who is available to respond to concerns or answer questions about how CarePartners protects patient information. …

The Breach

32. On or about June 11, 2018, a group of hackers emailed CarePartners to advise that they had breached the CarePartners network and extracted data from its servers. The hackers' email attached a sample of CarePartners patient and employee data, which CarePartners verified to be authentic data that had resided on its servers.

33. CarePartners 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.

34. One week later, on June 18, 2018, CarePartners, in conjunction with the LHINs, issued a press release stating that a "cyber-attack breached CarePartners' computer system and as a result patient and employee information held in that system, including personal health and financial information…was inappropriately accessed by the [hackers]".

35. CarePartners' press release did not include any particulars of the scope of the Breach, and it was not distributed directly to the Class Members. As a result, most Class Members, including Arthur, remained unaware that the Breach had occurred.

36. Arthur did not receive timely notice of the Breach. Eventually, he received a standard form notice from CarePartners, similar to the form of the June 18, 2018, press release, which stated that his Personal Information "may" have been impacted by the Breach. Arthur received no other communications from CarePartners regarding the Breach either before or after that notice.

37. CarePartners never confirmed to Arthur that his Personal Health Information had been impacted by the Breach.

38. Arthur did not receive the notice from CarePartners until after he received a surprising call from a CBC News reporter. The reporter told Arthur that Arthur had been a victim of the Breach, and—shockingly—that Arthur's Personal Health Information, along with other Class Members' Personal Health Information, had been disclosed to CBC by the hackers. The reporter advised that he had identified Arthur's phone number from records which were part of the Breach data sample provided to CBC by the hackers. After speaking with the reporter, Arthur was able to confirm that the records in the Breach data sample were his authentic medical records containing his Personal Information.

39. On July 17, 2018, CBC News reported that it had been in communication with the hackers, and that the hackers had provided CBC News reporters with a sample of the Breach data. The Breach data sample contained the Personal Information of over 80,000 CarePartners patients, including phone numbers and addresses, dates of birth, and health card numbers, detailed medical histories including past conditions, diagnoses, surgical procedures, care plans and medication information, as well as approximately 140 active patient credit card numbers and expiry dates, many with security codes. It also contained CarePartners employee T4 tax slips, social insurance numbers, bank account details, and plaintext passwords.

40. CBC News reported that the hackers had informed it that the data sample was only a subset of hundreds of thousands of patient records and related materials, dating back to 2010, which they had exfiltrated in the Breach. They advised that they were able to exploit weak passwords and vulnerabilities in the software used by CarePartners, which had not been updated in two years, to remove hundreds of gigabytes of unencrypted data without detection. The hackers also advised that they had demanded a ransom payment in exchange for not leaking the Breach data online, and telling CarePartners how to fix their cyber security vulnerabilities.

41. CarePartners had not paid the ransom as of the date of the CBC News article.

42. After the publication of the July 17, 2018, CBC News report, CarePartners issued a statement confirming that the ransom demand had been made, but providing no further details regarding the ransom.

43. CarePartners claimed in its July 17, 2018, statement that it had proactively notified patients whose records were inappropriately accessed. This was patently untrue. Arthur received no notice of the Breach until he received the phone call from the CBC News reporter.

44. Arthur was shocked, embarrassed, and distressed to learn that the Breach had occurred, and that, even a month after the fact, CarePartners had not informed him that his Personal Information had been accessed and stolen as part of the Breach.

45. In February 2019, the hackers notified a well-known data breach blogger that they would be posting the Breach data online because CarePartners refused to pay their ransom demands. The hackers released links to two "dumps" of the Breach data: a 2.2 GB archive containing 12,971 files of CarePartners financial data, including sensitive employee financial information; and a 7 GB archive containing tens of thousands of patient files, as well patient database/tables listing Personal Information of tens of thousands of patients.

46. To date, CarePartners has not acknowledged publicly that Breach data was provided to the blogger. CarePartners also has not provided any additional information regarding how the Breach occurred, the scope of the Breach, the nature of the data involved in the Breach, the amount of the ransom demand, or what the hackers promised in return for the payment of the ransom. Arthur has received no communication confirming that his own Personal Information and Personal Health Information was affected.

47. Nor has CarePartners disclosed what steps it has taken to remediate the Breach, and to update its cyber security systems to avoid any future privacy breaches. CarePartners' response to

the Breach has been entirely inadequate and unresponsive to the risks, embarrassment, humiliation, distress, anxiety, financial damage and expenses to which it has exposed the Class.

Significance of the accessed/exfiltrated data

48. 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.

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

50. 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.

51. Companies like CarePartners 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.

52. 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.

53. Immediately after learning about the Breach, Arthur spent several hours changing passwords for his online accounts and his family's online accounts.

54. Since the Breach, both Arthur and his wife have noticed an increase in the number of fraudulent phone calls and phishing/spam emails that they receive, as well as the number of unauthorized access attempts on their online accounts.

55. 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.

56. 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 any time, the risks associated with this privacy breach will continue on as credible threats for years.

57. CarePartners made a limited offer of one year of free credit protection services to individuals whose personal data may have been breached, which was only made available for a limited period of time after the Breach. This credit protection service provides no short-term or long-term protection or remedies to the plaintiff and Class Members.

Applicable privacy & cyber security standards

58. 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.

59. 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.

60. CarePartners 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.

61. At a minimum, among other things, CarePartners 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 CarePartners 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.

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

RIGHTS OF ACTION

63. The defendant is liable to the Patient Subclass Members for negligence, intrusion upon seclusion, breach of the *PHIPA*, breach of contract, and breach of the *Consumer Protection Act*.

64. The defendant is liable to the Employee Subclass Members for negligence, intrusion upon seclusion, and breach of contract.

Negligence

65. 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 Patient Subclass Members' Personal information, including their Personal Information, would only be used for the provision of healthcare services;

(b) the Employee Subclass Members' Personal Information, including their Personal Information, would only be used for the purposes of their employment relationship;

(c) 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;

(d) 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 CarePartners Privacy Pledge; and

(e) 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.

66. 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 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 CarePartners 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 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 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) failing to offer sufficient credit monitoring and identity theft insurance services to the Class Members;

(j) 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

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

67. CarePartners 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. CarePartners 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, CarePartners negligently, wilfully and/or recklessly failed to have proper cyber security protections in place to protect the Personal Information of the Class Members.

68. 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.

Intrusion upon seclusion

69. The defendant is liable for the tort of intrusion upon seclusion because its reckless conduct facilitated the deliberate intrusion of the unidentified hackers.

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

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

(b) the defendant's reckless conduct regarding cyber security 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 or CarePartners' dilatory conduct in allowing the Breach; and

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

Breach of the *PHIPA*

71. In engaging in the wrongful conduct as pleaded herein, the defendant has wilfully or recklessly contravened s. 12 of the *PHIPA* with regard to the Patient Subclass Members, causing them actual harm and mental anguish. It is therefore liable for awards of damages pursuant to s. 65 of the *PHIPA*.

Breach of contract

72. The Patient Subclass 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 CarePartners Privacy Pledge are impliedly incorporated in to the Patient Contract.

73. The Employee Subclass Members entered into standard form contracts with the defendant that govern the terms of their relationship with the defendant (the "Employment Contracts").

74. It was an express or implied term of the Patient Contract and the Employment Contracts (collectively, the "Contracts") that the defendant would be responsible for all of the 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 Class Members' Personal Information confidential, and to ensure that it would not be lost to, disclosed to, or used by unauthorized persons.

75. The defendant breached its implied contractual obligation to make all reasonable efforts to maintain confidentiality over the Class Members' Personal Information, including as follows:

(a) it failed to take security measures to ensure that the Class Members' 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; and

(c) it failed to implement sufficient technical and administrative safeguards to protect the Class Members' Personal Information.

Breach of the *Consumer Protection Act*

76. The Patient Subclass Members entered into consumer transactions with the defendant, as defined in the *Consumer Protection Act*.

77. The defendant engaged in unfair practices by making the representations set out in the Privacy Pledge (the "Privacy Representations"), which were false, misleading or deceptive representations to the Patient Subclass Members regarding the security and confidentiality of their Personal Information, contrary to the *Consumer Protection Act*.

78. By making the Privacy Representations, the defendant represented to the Patient Subclass Members that it maintained strict cyber security measures to safeguard their Personal Information and to prevent unauthorized access or disclosure. As evidenced by the occurrence of the Breach, the defendant, in fact, failed to maintain appropriate or adequate cyber security measures.

79. The Patient Subclass Members are entitled to an award of damages in respect of the defendant' unfair practices pursuant to s. 18 of the *Consumer Protection Act*.

80. It is in the interests of justice that the Patient Subclass Members receive a waiver of the notice requirement in s. 18(15) of the *Consumer Protection Act*.

81. In addition, the Patient Subclass Members are entitled to exemplary or punitive damages pursuant to s. 18(11) of the *Consumer Protection Act*.

DAMAGES

82. 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.

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

(a) serious and prolonged mental distress;

(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 CarePartners' breaches as alleged herein.

84. In addition, the plaintiff and Class Members seek moral damages for intrusion upon seclusion.

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

86. Moreover, subsequent to learning of the existence of an extensive privacy breach affecting many of its patients and employees, CarePartners 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

87. The plaintiff pleads and relies upon the *CJA*, the *CPA*, the *PHIPA*, the *Consumer Protection Act*, and associated regulations.

PLACE OF TRIAL

88. The plaintiff proposes that this action be tried in the City of Toronto.

Date: September 11, 2020

WADDELL PHILLIPS
PROFESSIONAL CORPORATION

36 Toronto Street, Suite 1120
Toronto, ON M5C 2C5

Margaret L. Waddell (LSO No.: 29860U)
marg@waddellphillips.ca

Tina Q. Yang (LSO No.: 60010N)
tina@waddellphillips.ca

Tel: 647.261.4486
Fax: 416.477.1657

HOWIE, SACKS & HENRY LLP
20 Queen Street West, Suite 3500
Toronto, ON M5H 3R3

Paul Miller (LSO No.: 39202A)
PMiller@hshlawyers.com
Christine Sesek (LSO No.: 77807S)
CSesek@hshlawyers.com

Tel: 416.361.5990
Fax: 416.361.0083

SCHNEIDER LAW FIRM
1120 Finch Avenue West, Suite 700
Toronto, ON M3J 3H7

Cary Schneider (LSO No.: 44428L)
CSchneider@schneiderlawfirm.ca
Adam Warner (LSO No.: 65022I)
AWarner@schneiderlawfirm.ca

Tel: 416.849.6633
Fax: 416.514.0695

Lawyers for the Plaintiff

NITY NURSING SERVICES FOU

PLAINTIFF

DEFENDANTS

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

STATEMENT OF CLAIM

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

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

Tel: 647.261.4486
Fax: 416.477.1657

HOWIE, SACKS & HENRY LLP
20 Queen Street West, Suite 3500
Toronto, ON M5H 3R3

Paul Miller (LSO No.: 39202A)
PMiller@hshlawyers.com
Christine Sesek
(LSO No.: 77807S)
CSesek@hshlawyers.com

Tel: 416.361.5990
Fax: 416.361.0083

Lawyers for the Plaintiff

SCHNEIDER LAW FIRM
1120 Finch Avenue West, Suite 700
Toronto, ON M3J 3H7

Cary Schneider (LSO No.: 44428L)
CSchneider@schneiderlawfirm.ca
Adam Warner (LSO No.: 65022I)
AWarner@schneiderlawfirm.ca

Tel: 416.849.6633
Fax: 416.514.0695