Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

ADELE ANNE WORLEY-BURNS

Plaintiff

-and-

NATURAL HEALTH SERVICES LTD.AND SUNNIVA INC.

Defendants

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 WILL 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.

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: March 20, 2019 Issued by: _____
Local Registrar

Address of court office:
Court House
393 University Avenue
Toronto, Ontario M5G 1E6

TO: SUNNIVA INC.
Suite 400, 355 – 4th Avenue S.W.
Calgary, Alberta
T2P 0J1
Canada

AND TO: NATURAL HEALTH SERVICES LTD.
7900 Anchor Drive
Windsor, Ontario
N8N 5E5
Canada

THE DEFINITIONS

1. The following definitions apply for the purposes of this statement of claim:

(a) **"Act"** means the *Class Proceedings Act, 1992*, S.O. 1992 c. 6, as amended;

(b) **"ACMPR"** means *Access to Cannabis for Medical Purposes Regulations*

(c) **"CCQ"** means the *Civil Code of Quebec*, SQ 1991;

(d) **"Cannabis Act"** means the *Cannabis Act* (S.C. 2018, c. 16), which came into force on October 17, 2018;

(e) **"Class Members"** means all persons defined in paragraph;

(f) **"Class Period"** means the date of the data breach up to the date this court hears the motion for certification of this action as a class proceeding;

(g) ***"Consumer Protection Act"*** means the *Consumer Protection Act, 2002*, S.O. 2002, Chapter 30, Schedule A;

(h) **"Customer"** means a person who dealt with NHS;

(i) **"EMR"** means Electronic Medical Record system owned and operated by NHS;

(j) **"LP"** means licensed producer;

(k) **"Medical information"** means pieces of photo ID, health care cards and supporting medical documentation, and in Ontario "may include lab results, diagnostic reports and treatment plans";

(l) **"NHS"** means the defendant Natural Health Services Ltd.;

(m) "**Personal Information**" means under PIPEDA, any factual or subjective information, recorded or not, about an identifiable individual, including the name of the person;

(n) **"PIPEDA"** means the *Personal Information Protection and Electronic Documents Act*, [2000, c. 5];

(o) **"Privacy Act"** means the *Privacy Act*, RSC 1985, c P-21;

(p) **"Sunniva"** means the defendant, Sunniva Inc.; and

(q) **"Worley-Burns"** means the proposed representative plaintiff, Adele Anne Worley-Burns.

RELIEF SOUGHT

2. The plaintiff Worley-Burns CLAIMS on her own behalf and on behalf of the Class:

(a) an order pursuant to the *Act* certifying this proceeding as a class proceeding and appointing her as representative of the Class;

(b) damages in the amount of $50,000,000.00;

(c) an interim fund and a fund for credit monitoring services including any appropriate remedies for the breach of data, including customers' records and confidential medical information and Personal Information;

(d) an order for damages for breach of contract in relation to any customers who dealt with NHS and were subjected to the data breach;

(e) damages for breach of statute pursuant to any legislation under the *Consumer Protection Act* and/or PIPEDA and/or privacy law;

(f) damages for reckless intrusion upon seclusion, publicity given to private life, and breach of confidence, including costs for preventing identity theft, risk of future identity theft, monitoring, loss of reputation and harmed credit scores;

(g) damages for negligence as described hereunder, and/or including the following declarations:

i. a declaration that the defendants NHS and/or Sunniva negligently maintained customers' records, including confidential medical information and failed to design and implement a secure intellectual property system;

ii. a declaration that the defendants negligently implemented security for users' Private Information, including theirconfidential medical information, names, addresses, phone numbers and other Personal Information;

iii. a declaration that the defendants failed to warn that the customers' Private Information and confidential medical information had been subjected to a data breach, accessed improperly, retrieved, copied or stolen;

iv. a declaration that the defendants negligently implemented systems such that the customers' privacy was violated, and breached s. 14(1) and s. 14(2) subsections 7,

12-15, and s. 15(1), and s. 15(2) subsections (a), (c), (e) and (g) of the *Consumer Protection Act*;

v. a declaration that the defendants failed to advise the customers, the plaintiff and the other Class Members of the breach and/or theft immediately, and acted deliberately, intentional, and with reckless disregard for the protection of the customers' confidential medical information;

vi. a declaration that the defendants failed to rectify the security flaws inherent in the system, even when warned and/or knew or ought to have known of the vulnerabilities;

vii. a declaration that the defendants are strictly liable to the plaintiff and Class Members; and

viii. a declaration that the defendants are liable to the plaintiff and the other Class Members for the damages caused by their negligence in relation to the customers' data and confidential medical information that is preserved ad infinitum and capable of being disseminated and distributed on the "dark web";

(h) an order for the aggregate assessment of monetary relief and distribution, and/or a reference to assess same;

(i) special damages, including time lost for precautionary steps in dealing with credit monitoring and agencies, general damages, and the costs of administering the plan of distribution of the recovery in this action in the sum of $10,000,000.00 or such other sum as this Honourable Court finds appropriate;

(j) an accounting of all profits realized by the defendants;

(k) an accounting of all profits received by the defendants directly or indirectly related to the profits earned, and an order requiring the defendants to disgorge these amounts;

(l) an order that the defendants hold all proceeds received from the profits realized, and any other profits or income received relating directly or indirectly to profits, in a constructive trust for the benefit of the Class Members;

(m) aggravated damages, exemplary damages and punitive damages in the amount of $15,000,000.00, or such other sum as the Honourable Court finds appropriate;

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

(o) prejudgement interest pursuant to the *Courts of Justice Act*, R.S.O. 1990, c. C.43, s. 128 and 129;

(p) costs of this action pursuant to the *Act*, and s. 131(1) of the *Courts of Justice Act* on a substantial indemnity basis plus applicable taxes;

(q) costs of this action on a solicitor/client scale; and

(r) such further and other relief as to this court seems just.

THE NATURE OF THE ACTION

3. This action concerns the breach of privacy laws and breach of contract, and negligence, in relation to the EMR system implemented and operated by NHS. The company operates by allowing customers to obtain cannabis with a chosen LP. It is then shipped directly to their door by courier or Canada Post. NHS also sells a cannabis starter kit on its website. NHS operates as a referral network and has seven facilities owned and operated in Alberta, Saskatchewan, Manitoba and Ontario.NHS claims to have “leading edge proprietary technology” that connects physicians and patients with producers who comply with the regulations set out by Health Canada.

4. The plaintiff and putative Class understood that NHS protected its customer data such that confidential information, including medical conditions, allergies, and prescriptions, among other information, was secure. NHS held out that it had systems in place and employees who were trained to handle sensitive data and confidential medical information of customers. However, it failed to implement security features to protect customers’ data and information and a breach of this data transpired.

5. NHS allowed a breach of its customers' Private Information when itfailed to rectify the security flaws inherent in its system, allowing a hitherto undisclosed number of customers' private data, including medical information and Provincial health plan identities, to be irretrievably compromised and exposed publicly. To date, customers do not know if their confidential medical information, name and address, and other Personal Information, was part of the data breach, and in fact nor were they warned of the breach in a timely fashion.

6. NHS holds itself as Natural Health Services (NHS) is a wholly-owned subsidiary of Sunniva Inc., a vertically integrated cannabis company in the world's two largest cannabis markets in Canada and California. NHS owns and operates a network of medical clinics in Canada specializing in medical cannabis under the *Cannabis Act* and Regulations.

CONTRACT

7. The plaintiff and Class Members entered into a contract with NHS and/or Sunniva.

8. NHS collected reams of data concerning medical conditions and documentation of its customers. LP's are required under the ACMPR, when registering or renewing new clients, to ensure that:

(a) original medical documents are submitted as well as the application for registration;

(b) the information in the medical document is correct and complete by, in part, verifying its accuracy with the office of the health care practitioner (as per paragraph 132(1)(c) of the ACMPR); and,

(c) the documentation of these verifications are part of the record keeping obligations (Division 5 of the ACMPR).

9. The plaintiff and Class provided fairly extensive medical information to the defendants.

10. The privacy terms in using the NHS website also confirmed that data and confidential medical information and Personal Information was being held and maintained securely and in compliance with PIPEDA and protected under the CPA. In particular, it was agreed that the defendants would maintain customers' records in compliance with legislation pertaining to the collection, retention, and disclosure of Personal Information.

11. The plaintiff and Class plead that the data breach amounted to a breach of contract, which was a fundamental breach.

WEBSITE TERMS AND CONDITIONS and THE PRIVACY POLICY OF NHS

12. NHS and Sunniva have an extensive privacy policy on each of the websites.

13. In section 9 of its Privacy Policy, NHS discloses that the website collects information that customers specifically and knowingly provide and uses technological measures to collect information about use of the website. It states that by using the website, customers consent to the collection, use, disclosure and retention of personal information by or on behalf of NHS as explained in the NHS Privacy Policy as revised from time to time, and as otherwise permitted by applicable law.

14. The Privacy Policy stipulates the following:

> Natural Health Services Ltd. and its subsidiaries (collectively, "NHS") is committed to maintaining the privacy and confidentiality of all personal information that we collect, use and disclose. NHS strives to protect the privacy rights of our patients by meeting or exceeding the standards established by law.

> This Privacy Policy outlines why we collect patients' health information, how we manage patients' information and how we safeguard their information.

15. The plaintiff and Class plead and rely upon the entirety of the document including the provisions related to the definition of "Health Information," which includes:

> ...information about an individual in oral or recorded form. It includes any information about an individual's health or health care history that could identify an individual when used alone or with other information. This may include diagnostic, treatment and care Information.

16. The plaintiff and Class plead and rely upon the provisions of the document including the provisions related to "Safeguards & Security," in particular the following:

> NHS recognizes the importance of safeguarding health information and will take all steps that are reasonable in the circumstances to ensure that health information in our custody is protected against theft, loss or unauthorized access, use, or disclosure. We will also ensure that the records containing this information are protected against unauthorized copying, modification or disposal.

17. The plaintiff and Class plead and rely upon the statements made in the website's Terms and Conditions and separately in the Privacy Policy, as stated in the aforementioned.

18. The plaintiff and Class plead that these statements are representations that were relied upon, that the reliance was reasonable, and that it resulted in losses caused by the data breach.

19. Further or in the alternative, these statements formed part of the contractual terms, which were breached, in that the data breach revealed that the data was not safeguarded or secure.

THE DATA BREACH

20. On January 31, 2019, NHS filed a police report in relation to a data breach that had taken place in its EMR system between December 4, 2018 and January 7, 2019, "where your personal health information was accessed without authorization."

21. It took several weeks before NHS filed the police report, and fully until March 18, 2019 before the media was alerted. At some point, unknown to the plaintiff and Class, NHS began sending a letter to the customers. For the time period during the delay, no explanation was provided.

22. The letter stipulates that "[t]he personal health information that was inappropriately accessed includes any or all of the following: name, address, phone number, age, gender, health care number, health information including diagnosis, medical information, encounter notes, referrals, allergies, forms and completed questionnaires."

23. NHS advised that as a precaution, customers should verify and monitor "your personal transaction statements from governments, financial institutions, businesses and any other institutions to detect any unusual activity." It advised that if any suspicious activities are detected, customers are advised to contact those organizations "immediately."

24. The plaintiff and Class was also advised that if they notice companies (that they have no prior relationship with) reaching out to try to sell products and services, they need to be vigilant. In addition, they were advised to ask questions about where their information was obtained, and to be wary of email scams and cautious opening link and attachments. The defendants recognize the risks their breach has created, including phishing scams and other nefarious conduct.

25. Lastly, the plaintiff and Class were assured that the defendants take their "role in

safeguarding your personal information and using it an appropriate manner very seriously." They were also assured that NHS has taken steps to address operational and technology updates triggered by the incident to improve the protection of patient personal health information.

26. The plaintiff and Class plead that none of these measures adequately addresses the damages that result from the losses caused by the data breach. Notably, there was no mention at all of offering any credit monitoring and credit protection, or compensation.

THE DESCRIPTION OF THE CLASS

27. The plaintiff brings this action on behalf of herself and the Class of persons in Canada who have been subjected to the data breach of the medical record system operated by NHS. Included also are the Class Members' estates, executors, and personal representatives.

THE PARTIES

28. The plaintiff, Worley-Burns, resides in the unincorporated community of Wallaceburg, in the single tier municipality of Chatham-Kent.

29. The defendant, NHS, is the wholly owned subsidiary of Sunniva, and owns and operates a network of medical clinics in Canada specializing in medical cannabis under the *Cannabis Act*and Regulations. Its headquarters are in Calgary, located at Suite 400, 355 – 4th Avenue S.W. Calgary, AB T2P 0J1.

30. The defendant, Sunniva, through its subsidiaries, including NHS, is a vertically integrated cannabis company operating in the world's two largest cannabis markets – California and Canada. At all relevant and material times, it operated out of the location of NHS in Calgary, also at Suite 400, 355 – 4th Avenue S.W. Calgary, AB T2P 0J1.

FACTS IN RELATION TO THE PROPOSED REPRESENTATIVE PLAINTIFF

31. The plaintiff Worley-Burns has a number of medical conditions, for which was prescribed opioid pain medication. In 2003, the plaintiff was in two car accidents, the first being the more serious, in a span of a few months. She had and continues to have severe pain and also suffers from fibromyalgia and arthritis. As a result of the accidents and other conditions, her doctor prescribed Oxycodone, an opioid.

32. Worley-Burns was on this medication for over seven years before she weaned herself off as she felt it was not helping but making her condition worse. Subsequently, she also underwent surgery which precluded taking Ibuprofen. She was on multiple medications, for severe pain, including attending InMedic Pain Management Centre for pain management for over a year, receiving Lidocaine injections and a monthly Lidocaine infusion to help with the pain. She was also taking Tramadol (an opioid) and Lyrica.

33. Since she was still having severe pain, her doctor suggested medical marijuana and sent a referral for her to see the NHS for assessment for a medical marijuana licence. The company contacted her and asked her to fill out their online questionnaire, which she completed, and she was booked for an appointment.

34. Worley-Burns had some concerns about medical marijuana as she travels to the United States weekly and was worried about what would happen if the border agents stopped her from entering the United States. Accordingly, she cancelled the appointment with NHS and did not proceed with NHS, and was so concerned about the issue of border crossing and the impact that the disclosure of a medical marijuana prescription would have on her ability to freely cross the border, that she opted not even to proceed with obtaining a prescription.

35. On Friday March 15, 2019, she received a letter from NHS informing her that her data had been compromised in the data breach. She is now even more concerned about who has her information and what this will mean for her. She is now worried that even this information being in the wrong hands could make travel difficult for her and "what they can do with my information also is scary." Because she is so worried about how it may impact her ability to cross the border into the United States, she recognizes how the security of her data was of the utmost concern to her.

RELATIONSHIP AMONG THE DEFENDANTS

36. At the time of the data breach, both NHS and Sunniva were using the data obtained from customers for profit, as described in the within action.

37. NHS began a mail out of letters to advise customers whose information was stolen and compromised. Nothing has been posted on its website in relation to the data breach, nor on Sunniva's website.

38. The plaintiff and Class plead that the companies acted as one unit. Sunniva is currently building a facility in California but is operating out of the address in Calgary. NHS and Sunniva are responsible for the acts and omissions of one another. There is no indication that there is a separate controlling mind for the two entities.

39. The plaintiff and Class Members plead that the use of the customers' data and/or confidential medical information and Personal Information was a collaborative effort among the defendants, for which the defendants are in law responsible.

DUTIES AND OBLIGATIONS OF THE DEFENDANT and JURISDICTION

40. The plaintiff and Class adopt with reference the legislation under the ACMPR and the *Cannabis Act* and PIPEDA, along with Provincial privacy legislation.

41. Additionally, pursuant to s. 8. (1) of the *Consumer Protection Act*, a consumer may commence a proceeding on behalf of members of a class under the *Class Proceedings Act, 1992* or may become a member of a class in such a proceeding in respect of a dispute arising out of a consumer agreement despite any term or acknowledgment in the consumer agreement or a related agreement that purports to prevent or has the effect of preventing the consumer from commencing or becoming a member of a class proceeding.

42. The defendant NHS on its website purports to limit the applicability of class proceedings.

43. The plaintiff and Class plead that the proper forum is Ontario, where the tort occurred in relation to the representative plaintiff, and where a facility exists.

PROVISIONS UNDER THE CONSUMER PROTECTION ACT

44. Pursuant to Part III, which governs unfair practices, in respect of false, misleading or deceptive representation, s. 14 provides that it an unfair practice for a person to make a false, misleading or deceptive representation which includes a representation that the goods or services are of a particular standard, quality, grade, style or model, if they are not.

45. The plaintiff and Class Members plead that the data and customer information was not maintained securely. Pursuant to s. 14(1) and s. 14(2) subsections 7, 12-15, and s. 15(1), and s. 15(2) subsections (a), (c), (e) and (g) of the *Consumer Protection Act*, the defendant NHS engaged in the following unfair practices:

> (a) making a false, misleading or deceptive representation in relation to a representation that the goods or services have been supplied in accordance with a

previous representation, if they have not, in that the services did not comply with the stipulated Privacy Policy;
(b) making a representation that misrepresents the authority of a salesperson, representative, employee or agent to negotiate the final terms of the agreement, in that the employee was not protecting the customers' data;
(c) making a representation that the transaction involves or does not involve rights, remedies or obligations if the representation is false, misleading or deceptive, in that the information was subject to a data breach and not safeguarded or secure;
(d) making a representation using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if such use or failure deceives or tends to deceive, in that the customers' were not informed their data was subject to risk of breach;
(e) making a representation that misrepresents the purpose or intent of any solicitation of or any communication with a consumer, in that the data was not safeguarded or secure; and
(f) without limiting the generality of what may be taken into account in determining whether a representation is unconscionable, there may be taken into account that the person making the representation or the person's employer or principal knows or ought to know, in particular:

i. that the consumer is not reasonably able to protect his or her interests because of disability, ignorance, illiteracy, inability to understand the language of an agreement or similar factors;
ii. that the consumer is unable to receive a substantial benefit from the subject-matter of the representation;
iii. that the consumer transaction is excessively one-sided in favour of someone other than the consumer; and
iv. that a statement of opinion is misleading and the consumer is likely to rely on it to his or her detriment.

46. The representations in regard to privacy in NHS's Privacy Policy are unconscionable, in that the defendant knew or ought to have known that in circumstances of failing to safeguard and secure the data, the agreement is one-sided, misleading, obliterates any benefit received, and the consumer cannot protect her or his interests. The system was not properly designed and implemented. Even had the consumers known, there was no provision to avoid supplying the data.

47. NHS had an obligation, based on its own Privacy Policy to ensure that customers' records, including data and confidential information, was withheld and/or maintained.

48. NHS had an obligation to hire, train and supervise employees and implement systems such that the breach could not transpire. This duty encompassed a system whereby any potential breach would be detected and avoided.

49. It is an unfair practice to make an unconscionable representation, pursuant to s. 15 of the *Consumer Protection Act* which includes:

(a) that the consumer is not reasonably able to protect his or her interests because of ignorance, illiteracy, inability to understand the language of an agreement or similar factors;
(b) that the consumer is unable to receive a substantial benefit from the subject-matter of the representation;
(c) that the consumer transaction is excessively one-sided in favour of someone other than the consumer;
(d) that the terms of the consumer transaction are so adverse to the consumer as to be inequitable;
(e) that a statement of opinion is misleading and the consumer is likely to rely on it to his or her detriment; or
(f) that the consumer is being subjected to undue pressure to enter into a consumer transaction. 2002, c. 30, Sched. A, s. 15 (2).

50. The plaintiff and Class Members plead that subject to s. 17 (1) of the *Consumer Protection* Act, no person shall engage in an unfair practice, and (2) A person who performs one act referred to in section 14, 15 or 16 shall be deemed to be engaging in an unfair practice. Subject to s. 116 (1) in respect of offences under the *Consumer Protection Act*, a person is guilty of an offence if the person, (a) fails to comply with any order, direction or other requirement under this Act and pleads that the defendant breached s. 17 (1).

BREACH OF DUTY OF THE DEFENDANT

51. NHS represented its services to be used and maintained in a manner that would obviously not make the data collected, subject to a breach.

52. NHS represented that customers' records, including medical information, and other data, was secure and provided a means for customers to order through a chosen LP.

53. NHS represented in its Privacy Policy that it took a number of steps to safeguard and secure data. The plaintiff and Class plead and rely upon the steps as stipulated.

54. NHS owed the plaintiff and Class a duty to abide by its stipulated policy but failed to do so. Among other stipulations, the following are related to data:

(a) password controls and search controls;

(b) firewalls and anti-virus software;

(c) logging, auditing and monitoring of all access to electronic records of personal health information;

(d) privacy notices; and

(e) encryption of all electronic communication and of all information transmitted electronically.

55. NHS made other representations in its Privacy Policy, upon which the plaintiff and Class plead in entirety, and which duties and obligations were breached by NHS in that it owed the plaintiff and Class a duty to abide by its stipulated policy but failed to do so.

NEGLIGENCE

56. The plaintiff and Class claim that the aforementioned was caused as a result of the joint

and/or several negligence of the defendants, NHS and Sunniva, and/or the employees or agents of the defendants, for whose negligence the defendants are in law responsible, the particulars of which are as follows against the defendant NHS:

(a) it failed to meet the statutory requirements in the collection, retention and disclosure of data and confidential information of its customers;
(b) it failed to have adequate policies, protocols and procedures in place to deal with computer security and retention of information;
(c) it failed to train, supervise, hire, monitor, its employees and, in particular, allowed a rogue entity, outsider, employee, or hacker, to breach the data and/or confidential information of its customers;
(d) it failed to implement policies, procedures and protocols, to stop hacking or theft of data or confidential information;
(e) it failed to detect same in a timely manner or at all;
(f) it failed to alert the customers and regulatory authorities and/or computer security experts when the breach was detected, at all or in a timely manner;
(g) it failed to have outside monitoring, a security expert, or an adequate IT department to deal with a rogue entity, hacking, a breach, or to set up an adequate, impervious, secure system in the first place;
(h) it failed to protect its data by restricting access on an as-need basis, but rather allowed an employee, hacker, rogue entity, or someone else to download large quantities of customers' records, including data and confidential information;
(i) it failed to adhere to its policies for the collection, retention and disclosure of Personal Information;
(j) it failed to destroy information on a timely basis that was no longer needed and/or to collect only information that was required under the regulations;
(k) it kept customers' records when it was not required to do so, or could not protect their data and Personal Information, adequately or at all;
(l) it failed to take reasonable steps to prevent unauthorized access to Personal Information, including maintaining the data and confidential medical information in a manner so that it was not subject to a breach, disseminated, lost, stolen, or otherwise placed into the stream of commerce in Ontario and Canada;
(m) it failed to entrust its customers' records, including data and confidential medical information, on the basis that once same is on the worldwide web it is used ad infinitum on the "dark web" to commit fraud and other crimes;
(n) it allowed data and confidential medical information to be used perniciously, including in phishing campaigns, targeted email, fraudulent activity and so forth;
(o) it failed to have a system in place to alert the authorities immediately, and did not alert customers properly or adequately or in a timely fashion;
(p) it failed to disclose the breach, theft or Personal Information, and confidential information, including medical information, immediately to the responsible regulatory agencies, to the authorities, and to the public at large;

(q) it implemented a system without warning to the plaintiff and Class Members that led to the breach and/or hacking or theft of their data and confidential medical information;
(r) it failed to adequately test or monitor its systems for a potential breach, thereby allowing the data and confidential medical information to be placed into the Canadian stream of commerce and elsewhere;
(s) it failed to detect and/or communicate the breach and/or theft or hacking to its security department or personnel, or regulatory agencies who could have warned customers immediately;
(t) it failed to post notice of the theft on its website, to date, or any mention of the hacking and breach or theft;
(u) it failed to alert all of its customers in the most direct way, instead relying upon letters;
(v) it failed to provide the total numbers of persons subject to the breach or theft or hacking;
(w) it deliberately withheld information about the risks until the risks became public and/or failed to appreciate and assess the risks and to warn of the risks, adequately or at all;
(x) it failed to maintain computer systems, an IT Department, or hire security specialists to detect the breach or theft or hacking when files were printed, emailed, copied, downloaded, or otherwise infringed; and
(y) it failed to act in accordance with PIPEDA, s. 8(1) of the *Privacy Act*, ss. 14 and 15 of the *Consumer Protection Act*, and its Privacy Policy.

BREACH OF CONFIDENCE, INTRUSION UPON SECLUSION, PUBLICITY GIVEN TO PRIVATE LIFE

57. The plaintiff and Class were required to submit details to the defendant NHS in order to obtain cannabis, and to be approved to do so by a licensed medical professional, operating under a licensed, regulated regime instituted by government, pursuant to the *Cannabis Act* and ACMPR.

58. NHS allowed and in fact required persons to submit confidential medical information and Personal Information.

59. Under PIPEDA, all of this information is considered “Personal Information,” along with information such as your name, address and phone number.

60. The plaintiff and Class plead that even if names, addresses and publicly accessible

information is found not to be private for the purposes of the tort of inclusion upon seclusion of the person, the balance of the information, including items specified under Provincial health plan requirements, health card identification, and other and details of medical information, including medical conditions, is in law private.

TORT OF BREACH OF CONFIDENCE

61. The defendants' conduct, in enabling that this data and confidential information to be subjected to a breach, or stolen, by hacking or otherwise, constitute a breach of confidence, in that the plaintiff and Class Members provided that information on the basis that it would be held confidentially, and safeguarded and secured, and the defendants misused that information to the detriment of the plaintiff and Class.

62. This breach includes the fact that it has allowed, enabled and facilitated other actors to use it in bad faith, sell it on the "dark web" (in and out of Canada), and use it for other purposes, including hacking, phishing, theft and fraud.

TORT OF INTRUSION UPON SECLUSION OF THE PERSON

63. The plaintiff and Class provided information, including but not limited to medical information, on the basis that it would be held and maintained confidentially. The plaintiff also provided other information which may or may not be considered private for the purposes of this tort, but includes names and addresses and phone numbers.

64. NHS's conduct constitutes an intentional and reckless intrusion on seclusion in a manner that would be highly offensive to a reasonable person, for which it is liable.

65. By allowing the theft or disclosure, it invaded, with no lawful justification, the private

affairs of the plaintiff and Class.

66. The invasion was highly offensive, causing distress, humiliation and anguish to the plaintiff and Class.

67. The plaintiff and Class remain at risk of activities as described in the aforementioned.

68. Further or in the alternative, personal health information is among the most basic private information that an individual possesses. Intrusion upon same results in unmitigated immediate and potential harm. Among other things, it may impact the ability of the plaintiff and Class to obtain insurance or to travel.

TORT OF PUBLICITY GIVEN TO PRIVATE LIFE

69. HNS gave publicity to the plaintiff's and Class Members' confidential medical information and Personal Information, for which it is liable.

70. Their confidential medical information and Personal Information is of no legitimate concern to the public. The disclosure of this information is highly offensive to a reasonable person.

71. Further or in the alternative, the information was provided with the expectation of privacy, secured by contract, and NHS breached the privacy of the plaintiff and Class in permitting their confidential information to be breached, stolen, hacked, and used for nefarious purposes.

72. HNS ensured that it would protect customers' records, including data and confidential and medical information, and made representations in its Privacy Policy in particular, and on its website, and has breached the privacy of its customers, and accordingly is responsible in law for this breach, along with the torts of breach of confidence, intrusion upon the seclusion, and

publicity given to private life.

73. The plaintiff and Class adopt, repeat and rely upon the allegations against the defendant NHS as against Sunniva, as described herein, in regard to breach of confidence, intrusion upon seclusion, and publicity given to private life.

VICARIOUS LIABILTY AND *RES IPSA LOQUITER* AND PIERCING THE CORPORATE VEIL

74. The plaintiff and Class Members plead and rely upon the doctrine of vicarious liability in relation to HNS's rogue entities, hackers, and employees or others who may have caused the data breach.

75. Further, wherever NHS is stipulated, its parent company, Sunniva, is in law responsible for the acts and omissions of its subsidiary, as its profits, controlling mind, board, ownership, location in Canada, and systems were inseparable. The plaintiff and Class plead that piercing the corporate veil is the appropriate remedy under these circumstances.

76. The plaintiffand Class Members plead and rely upon the doctrine of *res ipsa loquiter*.

THEFT AND CONVERSION

77. The plaintiff and Class plead theft and conversion pursuant to s. 322(1) of the *Criminal Code*, in particular that bad actors fraudulently and without colour of right took, or fraudulently and without colour of right converted, to their own use or to the use of another person, with intent, the data of the plaintiff and Class, for which the defendants are ultimately liable for collecting the data, without safeguarding or securing the data.

PRIVACY LAW IN QUEBEC

78. For residents of Quebec, the plaintiff and Class plead that the defendants' conduct is in breach of articles 1457 and 1463-1464 of the CCQ, and that in communicating Personal Information to third parties (i) without authorization under law and (ii) without consent, and for a (iii) purpose other than for which it was obtained, and HNS and/or Sunniva are liable to the Plaintiff and Class pursuant to articles 3, 35 and 37 of the CCQ.

79. To the extent that the activity of HNS is controlled in part by the government, whose regulations permit and make lawful the sale of cannabis, the plaintiff and Class plead and rely upon s. 8(1) of the *Privacy Act*, in so far as Personal Information was disclosed without the consent of the individual to whom the information pertains.

DAMAGES

80. *PIPEDA* establishes ten principles that organizations must follow when collecting, using and disclosing personal information in the course of commercial activity. The principles are as follows:

(a) Accountability;
(b) Identifying purpose;
(c) Consent;
(d) Limiting collection;
(e) Limiting use, disclosure and retention;
(f) Accuracy;
(g) Safeguards;
(h) Openness;
(i) Individual access; and
(j) Challenging compliance.

81. Worley-Burnsand the Class Members plead that NHS breached the principles of *PIPEDA,* along with privacy law and consumer protection law in Canada.

82. Worley-Burns maintains that in providing information to NHS, she entrusted NHS to maintain her data and Personal Information, including her medical information, in a manner that would not allow it to be used for any purposes other than for which it was required, and that it would not be subjected to a breach, improperly retrieved, stolen, leaked, or used for any other purposes.

83. At no time was she warned, or did she believe that there was a risk of public disclosure that would last ad infinitum on the internet.

84. Her Personal Information has been made public. She, along with the Class Members, is now subject to other attempts to use her data and confidential information, the usage of which is unknown to her and the Class Members.

85. Worley-Burns is afraid that she may be subjected to online scams in email and otherwise, and that her banking and financial information and business and government information may be at risk. She is aware as a result of the letter from NHS received on March 15, 2019 that she now needs to check whenever a company reaches out to her for payment or even to provide services.

86. Worse than that, Worley-Burns has personal medical information that has been disclosed. As a private citizen who was on various medications, and was advised to try medical marijuana when it became legal, she would not have been willing to compromise the privacy in her life had she known that NHS would subject her data and confidential medical information, including conditions, to a data breach.

87. Further, as a person who lives close to the border and made frequent trips to the United States, she especially did not want to compromise her ability to cross the border, which may now be compromised as the law differs from Canadian law in relation to medical marijuana. This fear was so pronounced that she ultimately opted not even to fill a medical marijuana prescription.

88. She, along with the Class, now have to face that there is no certainty that the data subjected to this breach will not be used for financial fraud, or that HNS's system was ever adequate to prevent improper disclosure of their medical information and other Personal Information.

89. She is upset that HNS took so long to reveal the fact of this breach, and that it is still not being handled properly or even disclosed on its website.

90. Worley-Burns and the Class are anxious, stressed, and upset that their information was stolen or leaked in this breach, and that their medical and other information has been misappropriated and that it may be used for nefarious purposes, of which they are largely unaware, such as insurance premium hikes or in any number of ways that increase health related costs.

91. The plaintiff and Class Members plead that HNS gathered data and confidential information from the plaintiff and Class as part and parcel of using the service to obtain cannabis legally. Doing so was done on the basis that the Personal Information was protected. Through various means, including their use of the website, and supporting documentation, NHS obtained information about their names, addresses, medical conditions, health card numbers, and so forth, amassing a treasure trove of data about its customers that is now going to be made available on the so-called "dark web" for purchase, misappropriation, fraud, and scams.

92. In various ways, through contract, by statute, and in its Privacy Policy, the customers had the reasonable expectation that their data was held and maintained properly.

93. HNS allowed the breach of information on the plaintiff and Class, ultimately to place that information in the stream of commerce not only in Canada but also anywhere with internet access. HNS failed to have a system in place to avoid the breach, and/or allowed the customers' records, including data and confidential medical and other information, to be used improperly and bought and sold. Even in its letter to its customers it said its customers' data security is taken "very seriously." Despite saying so, it has not posted a single word about the breach on its website, and appears to have sat on the breach since January 7, 2019 if not before, and certainly since January 31, 2019, when it was finally reported to the police. Some customers may have moved and not updated their contact information, and it becomes increasingly obvious when there is a delay that it is difficult to ascertain the persons who needed to be informed.

94. During the delay, it was obvious that customers would not take any precautions (to the extent that it is even possible) unless they were informed.

95. NHS makes statements that it values its customers' privacy but has failed in the first instance, despite assurances, to limit access, and then again in the aftermath to advise and to warn its customers in a timely fashion.

96. The plaintiff and Class have suffered damages in relation to losses arising from ongoing credit monitoring, prevention of identity theft, increased risks on a permanent basis of identity theft, damage to their credit ratings, in addition to mental distress, loss of time monitoring their credit risks, and anxiety that their identity may be misappropriated.

97. The plaintiff and Class have suffered damages especially in relation to their most personal details being made available to the public, including medical conditions, allergies, and personal health matters.

98. Health concerns are among the most private. The plaintiff and Class had no intention to make theirs public, and in a manner that is now out of their control. The dissemination of this information is the very antithesis of privacy for the plaintiff and Class. Once the data has been subjected to this breach, it is irretrievable. The plaintiff and Class will have to undertake steps in relation to credit monitoring, health privacy, health plans and cards, financial and business services, government services, and with credit card companies and applications, and even with phone and other bills, utility payments, and so forth.

99. The defendants' conduct as described in the aforementioned, in particular in maintaining Personal Information related to health, a matter of utmost importance, was high-handed, outrageous, reckless, willful, in contumelious disregard of the interests of the plaintiff and Class Members, indifferent to the consequences and motivated by economic considerations, and in complete disregard to the security of the plaintiff and Class Members, and as such renders the defendant liable to pay aggravated, exemplary and punitive damages in the amount of $15,000,000.00.

THE RELEVANT STATUTES

100. The plaintiff and Class plead and rely upon, and the amendments made thereto and the regulations thereunder:

(a) *Access to Cannabis for Medical Purposes Regulations*
(b) *Cannabis Act* (S.C. 2018, c. 16);
(c) *Cannabis Regulations* (SOR/2018-144);

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

(e) *Consumer Protection Act*, 2002, S.O. 2002, Chapter 30, Schedule A;

(f) *Civil Code of Quebec*, SQ 1991;

(g) *Electronic Commerce Act*, 2000, S.O. 2000, c. 17;

(h) *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31;

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

(j) *Personal Information Protection and Electronic Documents Act*, [2000, c. 5]; and

(k) *Privacy Act*, RSC 1985, c P-21.

101. The plaintiff and Class Members plead and rely upon the following provisions of Rule 17 of the *Rules of Civil Procedure* in support of such service: 17.02 (f) – the contract was made in Ontario;17.02 (g) – the tort was committed in Ontario; and 17.02(p) – the defendants carry on business in Ontario.

The plaintiff and Class Members propose that this action be tried in the City of Toronto, in the Province of Ontario.

March 20, 2019

DIAMOND & DIAMOND LAWYERS LLP
500-255 Consumers Road
Toronto, ON M2J 1R4

Darryl Singer
LSO no. 34473R
T:(416) 256-1600
F:(416) 256-0100
darryl@diamondlaw.ca

Sandra Zisckind
LSO no. 48207W
T:(416) 256-1600
F:(416) 256-0100
sandra@diamondlaw.ca

Jeremy Diamond
LSO no. 55201U
T:(416) 256-1600
F:(416)256-0100
jeremy@diamondlaw.ca

Steven Wilder
LSO no. 59224R
T: (519) 419-5552
F: (519) 419-5554
steven@diamondlaw.ca

HOTZ LAWYERS
1 Maison Parc Crt., Suite 520
Vaughan, ON L4J 9K1

Glyn Hotz (40878M)
Tel: (416) 907-6666
Fax: 1-866-687-3958

Lawyers for the Plaintiff and Class Members

Electronically issued / Délivré par voie électronique : 20-Mar-2019

Court File No./N° du dossier du greffe: CV-19-00616577-00CP

Court File No.

ADELE ANNE WORLEY-BURNS -and- NATURAL HEALTH SERVICES LTD. AND SUNNIVA INC

PLAINTIFF DEFENDANTS

ONTARIO SUPERIOR COURT OF JUSTICE

PROCEEDINGS
COMMENCED AT TORONTO

STATEMENT OF CLAIM

DIAMOND & DIAMOND LAWYERS LLP
500-255 Consumers Road
Toronto, ONM2J1R4
T: (416) 256-1600
F:(416-256-0100

Darryl Singer (34473R)
darryl@diamondlaw.ca

Sandra Zisckind (48207W)
sandra@diamondlaw.ca

Jeremy Diamond (55201U)
jeremy@diamondlaw.ca

Steven Wilder (59224R)
Steven@diamondlaw.ca

Glyn Hotz (40878M)
1 Maison Parc Crt., Suite 520
Thornhill, ONL4J9K1

Tel: 416-907-6666
Fax: 1-866-687-3958

Solicitor for the Plaintiff and Class