Court File No.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

C.M.

Plaintiff

- and -

HIS MAJESTY THE KING AS REPRESENTED BY THE MINISTRY OF PUBLIC AND BUSINESS SERVICE DELIVERY INFRASTRUCTURE TECHNOLOGY SERVICES, HIS MAJESTY THE KING AS REPRESENTED BY THE ONTARIO MINISTRY OF GOVERNMENT AND CONSUMER SERVICES, AYOUB SAYID AND RAHIM ABDU

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 24, 2023

Issued by .....
Local registrar

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

TO: **HIS MAJESTY THE KING AS REPRESENTED BY THE MINISTRY OF PUBLIC AND BUSINESS SERVICE DELIVERY INFRASTRUCTURE TECHNOLOGY SERVICES**
777 Bay Street, 5th Floor
Toronto, ON M5B 2H7

TO: **HIS MAJESTY THE KING AS REPRESENTED BY THE ONTARIO MINISTRY OF GOVERNMENT AND CONSUMER SERVICES**
777 Bay Street, 5th Floor
Toronto, ON M5B 2H7

AND TO: **AYOUB SAYID**
777 Bay Street, 5th Floor
Toronto, ON M5B 2H7

AND TO: **RAHIM ABDU**

CLAIM

1. The plaintiff, on her 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 C.M. (a pseudonym) as representative plaintiff for the Class;

(b) A declaration that the defendants, His Majesty the King as represented by the Ministry of Public and Business Service Delivery Infrastructure Technology Services and His Majesty the King as Represented by the Ontario Ministry of Government and Consumer Services (hereinafter collectively referred to as the "Ministries"), and Mr. Ayoub Sayid (an employee of the Ministries), 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 Ministries and Mr. Sayid 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 Ministries and Mr. Sayid 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 Ministries breached a contract with the plaintiff and the Class Members in which they were 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 defendants 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 defendants 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) A declaration that the Ministries and Mr. Sayid breached the Class Members' rights as set out in section 7 of the *Canadian Charter of Rights and Freedoms*;

(i) A declaration that the defendants intruded upon the seclusion of the plaintiff and Class Members, either directly or as a consequence of being vicariously liabile for the acts of an employee;

(j) A declaration that the Ministries are vicariously liable for the actions of Mr. Sayid;

(k) Damages, including Charter 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;

(l) Punitive, aggravated and exemplary damages in the amount of $25,000,000 or such other amount as may be fixed by the Court on an aggregate or individual basis;

(m) 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;

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

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

(p) 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

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

THE PARTIES

Defendants

2. The defendant, His Majesty the King as represented by the Ministry of Public and Business Service Delivery Infrastructure Technology Services is a branch of the Ontario Provincial Government. The Ministry created, maintained, and controls a COVID-19 provincial vaccination management system known as "COVaxON".

3. The defendant, His Majesty the King as Represented by the Ontario Ministry of Government and Consumer Services is the predecessor Ministry to the Ministry of Public and Business Service Delivery Infrastructure Technology Services.

4. The COVaxON system enables the Ministry of Health, vaccination locations, and staff, to collect and use COVID-19 vaccination data. COVaxON is subject to the Ministry of Health's cybersecurity protocols.

5. Ontarians' COVID-19 vaccination information from COVaxON is made available online through eHealth Ontario's "Digital Health Drug Repository" ("DHDR"). The DHDR is a provincial repository of publicly funded drugs and pharmacy services for all monitored drugs. The DHDR allows authorized Ontario Health Care Providers to view patients' COVID-19 vaccination information.

6. The defendant, Ayoub Sayid, is a resident of Ontario. Mr. Sayid was an employee of the Ministries at all material times. He worked for one of the Ministries' vaccination locations. He had access to the COVaxON system at all material times. He was bound by the *Personal Health Information Protection Act, 2004* and the Ministries' cybersecurity protocols at all material times. The Ministries had direct control and oversight of his employment at all material times.

7. The defendant, Rahim Abdu, is a resident of Ontario. Mr. Abdu conspired with Mr. Sayid to obtain and collect Ontarians' personal health information available on COVaxON without authorization or lawful justification for doing so.

C.M. as the Proposed Representative Plaintiff

8. The plaintiff, C.M., is an individual residing in Ontario. She accessed the Ministries' vaccination service in 2021. She provided the Ministries with her confidential personal health and identifying information to access the Ministries' vaccination service.

9. C.M. seeks to be appointed as the representative plaintiff on behalf of a class of individuals whose personal information and personal health information was accessed without authorization as a result of the "Breach", defined below.

The Class

10. C.M. brings this action on behalf of all persons who were notified on November 16, 2021, by the Ministries that their Personal Information and/or Personal Health Information contained in the Ministries' COVID-19 vaccine database was breached (the "Class" or "Class Members").

11. 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 leading up to November 16, 2021, confirmed by the Ministries as having occurred, with notification that Class Members' Personal Information and/or Personal Health Information was seized by the Ontario Provincial Police ("OPP") on Mr. Sayid's and/or Mr. Abdu's laptop.

12. The class is comprised of approximately 360,000 individuals.

FACTS IN SUPPORT OF ALL CAUSES OF ACTION

The Breach

13. In or around November 2021, individuals who scheduled appointments and/or accessed vaccine certificates through the Ministries' Covid-19 vaccine booking system began to receive text messages intended to solicit their personal information through the booking portal.

14. In or around December 2022, the Ontario Government notified about 360,000 people that their personal information, which was included in a COVID-19 vaccine database, was breached on November 16, 2021. Two individuals were charged for the Breach, Mr. Ayoub Sayid, and Mr. Rahim Abdu. Mr. Sayid was an employee of the Ministries' vaccine contact centre at the time of the Breach.

15. On November 22, 2021, the OPP executed two search warrants in connection with the Breach. The OPP seized several devices, computers and laptops. As a result of the investigation, Mr. Sayid and Mr. Abdu were taken into custody. They were both charged with Unauthorized Use of a Computer contrary to s. 342.1(1)(c) of the *Criminal Code*.

16. As a result of the Breach, the victims' names, phone numbers, date of birth, and health card information were collected and accessed for an unauthorized purpose.

17. On December 9, 2022, C.M. received an email from Michael Amato, the Chief Information Officer/Assistant Deputy Minister of the Provincial Vaccine Contact Centre, advising her of a privacy breach that involved her Personal Health Information registered in the COVID-19 immunization system used by the Provincial Vaccine Contact Centre and vaccine administrators across the province. Mr. Amato advised C.M. that the centre is

overseen by the Ministries and that the Ministries became aware of the breach on November 16, 2021. His email further advises that the OPP laid charges against two individuals, one of whom was a “contracted former employee of the contact centre”. C.M. was advised that the accused’s laptops seized by the OPP contained her name and phone number.

18. To provide its patients with vaccine services, the Ministries collect and retain Personal Information, including Personal Health Information, from patients and in some cases, their family members. To that end, the Ministries collected Personal Information and Personal Health Information about C.M. while she was under their care. The information was recorded in hard copy paper form and in electronic form, which was stored on the Ministries’ computer network.

19. C.M. understood that, at all material times, she entered into a contractual agreement with the Ministries for valuable consideration. C.M. expected that, as a consequence of her contractual agreement, the Ministries would collect, use and store her personal information, would keep it confidential and secure, and ensure it would not be lost, disseminated, accessed, or disclosed to unauthorized persons or for unauthorized purposes.

The Ministries collected Personal Information and Personal Health Information from the Class

20. The Ministries collected, used, and stored Personal Information and Personal Health Information from all Class Members. The Ministries collected, used, and stored their names, contact information, health card numbers, vaccination status, and other personal information.

21. The Class Members understood that, at all material times, they had entered into a contractual agreement with the Ministries for valuable consideration. The Class Members expected that, as a consequence of the contractual agreement, the Ministries would collect, use and store their personal information, would keep it confidential and secure, and ensure it

would not be lost, disseminated, accessed or disclosed to unauthorized persons or for unauthorized purposes.

22. At the time of the Breach, the Ministries provided services to hundreds 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, the Ministries are health information custodians as that term is defined in s 3 of the *PHIPA*.

23. The Ministries were, and are, obliged to secure and safeguard Personal Information in its custody or control, much of which was stored electronically through eHealth Ontario. They were, and are, obliged to take reasonable steps to ensure that Personal Health Information in their 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.

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

25. The Ministries were in an employer-employee relationship with Mr. Sayid at the time of the Breach. The Ministries are vicariously liable for damages suffered by the Class as a result of Mr. Sayid's actions.

26. At all times, the Ministries were obliged to have effective, current and robust cyber security protective measures in place to secure all of the patient Personal Information which they collect and store, including protection from attack by its own employees. The Ministries

failed to do so. Their cyber security protective measures, if any, were antiquated, inadequate, unreasonable, and readily penetrable by their own employees and third parties.

27. The Ministries failed to encrypt the Personal Information stored on their computer network, which was a breach of the relevant standard of care that they were obliged to meet to protect Class Members' privacy.

28. At all times, the Ministries were obliged to screen, train, and monitor their employees to ensure that the Ministries' vaccination program was not being used for an improper, unauthorized purpose.

Privacy Representations

29. At all material times, the Ministries represented to their patients that they complied with the *Personal Health Information Protection Act, 2004* ("PHIPA") and their own policies designed to safely collect, use, store, and dispose of personal health information. These polices include: the Electronic Health Record Request for Access to Personal Health Information Policy; Electronic Health Record Request for Correction to Personal Health Information Policy; Electronic Health Record Privacy Incidents & Privacy Breaches Policy; Electronic Health Record Consent Directive & Consent Override Policy; Electronic Health Record Inquiries and Complaints Policy; Electronic Health Record Privacy and Security Training Policy; Electronic Health Record Retention Policy; Electronic Health Record Logging and Auditing Policy; Electronic Health Record Assurance Policy; and the Electronic Health Record Health Care Provider Guide.

Aftermath of the Breach

30. To date, the Ministries have not disclosed what specific steps they have taken to remediate the Breach, and to update their cyber-security systems and/or employee management protocols to avoid any future privacy breaches.

31. The Ministries' response to the Breach has been entirely inadequate and unresponsive to the risks, embarrassment, humiliation, distress, anxiety, financial and reputational damage and expenses to which they have exposed the Class.

32. C.M. was shocked, embarrassed, and distressed to learn that the Breach occurred, and that her personal information was accessed without her authorization and in connection with her vaccination status.

33. Ministries that operate in healthcare and collect patient data including Personal Health Information take on commensurate heightened responsibility to safeguard and protect patient privacy.

34. 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.

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

36. The confidentiality of patient records and of individuals' personal information (including health information) is an important public interest. The importance of maintaining confidentiality of health records is enshrined in legislation, such as PHIPA, which permits

disclosure of personal health information (including OHIP numbers) only in limited circumstances. Confidential patient health information strikes at the biographical core of an individual.

37. Users who access personal information without authorization and 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 organizations 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 unauthorized usage, by employing state-of-the-art and current cyber security processes and software.

38. 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

39. "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.

40. "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

41. 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.

42. 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.

43. The Ministries 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 outside of the COVaxON system.

44. At a minimum, among other things, the Ministries 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 eHealth Ontario 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.

CAUSES OF ACTION

45. The defendants, the Ministries and Mr. Sayid, are liable to the Class Members for negligence (breach of a duty of care), breach of a fiduciary duty of care, breach of *PHIPA* and other Provincial and Territorial privacy legislation, breach of *PIPEDA*, and breach of the *Canadian Charter of Rights and Freedoms*.

46. The defendants, the Ministries, are liable to the Class Members for breach of contract.

47. The defendants, Mr. Sayid and Mr. Abdu, are liable to the Class Members for intrusion upon seclusion. The Ministries are vicariously liable for Mr. Sayid's intrusions upon the seclusion of each Class Member.

Negligence

48. The defendants, the Ministries and Mr. Sayid, 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 Ministries and Mr. Sayid 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.

49. The Ministries and Mr. Sayid breached the applicable duty of care owed to each Class Member, 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 eHealth Ontario's 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 screen, vet, and supervise the Ministries' employees properly, and/or failing to provide the Ministries' 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 the Ministries' employees properly, and/or failing to provide the Ministries' 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 ensure and/or determine, to the extent that the Ministries were responsible for ensuring that the Class Members' Personal Information remained

confidential, that the Ministries had network and cyber security management sufficient to ensure that the Class Members' Personal Information remained confidential; and

(j) Collecting and storing Class Members' Personal Information and Personal Health Information on Mr. Sayid's and/or Mr. Abdu's personal computer for improper and unauthorized purposes.

50. The Ministries and Mr. Sayid knew or ought to have known that, because they were administering the COVID-19 vaccination program, the information from COVaxON was a target for theft and/or misuse by individuals seeking personal gain by exploiting Class Members. The Ministries also knew or ought to have known that their cyber security was grossly inadequate and vulnerable to unauthorized users, including employees accessing the information for unauthorized purposes, rendering the Ministries' patients' Personal Information and Personal Health Information vulnerable to theft or compromise. Nevertheless, the Ministries negligently, willfully and/or recklessly failed to have proper cyber security protections in place to protect the Personal Information of the Class Members.

51. As a result of the Ministries' and Mr. Sayid's negligence, the Class Members' Personal Information and Personal Health Information was collected, stored, and used for unauthorized purposes, resulting in the Class Members sustaining damages which is particularized below.

Breach of Contract

52. The plaintiff and Class Members entered into a contract with the Ministries for the provision of healthcare services. All of the terms in the eHealth Ontario policies are impliedly incorporated into the contract.

53. It was an express and/or implied term of the contract that the Ministries 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.

54. The Ministries breached their 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) They failed to take security measures to ensure that the collected Personal Information was protected from theft, unauthorized access, use, copying or disclosure;

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

(c) They failed to implement sufficient technical and administrative safeguards to protect the collected Personal Information; and

(d) They failed to notify the Class Members of the Breach at the first reasonable opportunity to do so.

Breach of Fiduciary Duty

55. The defendants, the Ministries and Mr. Sayid, 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 government-funding provided by Class Members for the purpose of administering the COVID-19 vaccination program.

56. In exchange for funds provided either by the plaintiff and Class Members, by way of taxes and fees, the Ministries and Mr. Sayid 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.

57. The Ministries and Mr. Sayid breached their 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 contract and their fiduciary duty;

(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 the Ministries' employees properly, and/or failing to provide the Ministries' 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 screen, vet and supervise the Ministries' employees properly, and/or failing to provide their employees with proper training with regard to network and cyber security management;

(e) Failing to ensure and/or determine, to the extent that the Ministries were responsible for ensuring that the Class Members' Personal Information remained

confidential, that the Ministries had network and cyber security management sufficient to ensure that the Class Members' Personal Information remained confidential; and

(f) Collecting and storing Class Members' Personal Information and Personal Health Information on Mr. Sayid's and/or Mr. Abdu's personal computer for improper and unauthorized purposes.

58. As a result of the defendants' negligence, the defendants breached their fiduciary duty to act in the best interest of the plaintiff and the Class Members and in accordance with the contract and their fiduciary duty owed to the Class Members.

Breaches of Provincial Health Legislation

59. In addition, or in the alternative to the above, as applicable, on behalf of the Class, the plaintiff pleads that the defendants violated the *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A.

Breach of section 7 of the *Canadian Charter of Rights and Freedoms*

60. The plaintiff and Class Members plead and rely upon the *Canadian Charter of Rights and Freedoms* ("*Charter*") and, specifically, section 7 of the *Charter*.

61. The plaintiff and the Class Members plead that the *Charter* applies to the *Ministries*, Mr. Sayid, and the Crown in Right of Ontario by operation of section 32(1)(b) of the *Charter*.

62. The defendants' failure to properly collect, store, transfer, maintain and secure the Class Members' personal information was the result of operational and systemic negligence, including a failure to implement adequate security policies at an operation level. This operational and systemic negligence exposed the Class Members to harm, which was a

reasonably foreseeable consequence of the defendants' operational and systemic negligence. This loss and the resulting exposure constitutes a breach of the security of the person pursuant to section 7 of the *Charter*.

Intrusion Upon Seclusion

63. The defendants, Mr. Sayid and Mr. Ayub are liable for instruction upon seclusion because their reckless conduct resulted in the deliberate intrusion upon the Class Members' privacy.

64. The tort of intrusion upon seclusion is made out because:

(a) The defendants, Mr. Sayid and Mr. Abdu, intentionally and/or recklessly accessed and collected the Personal Information and Personal Health Information belonging to the Class;

(b) The defendants, Mr. Sayid and Mr. Abdu, invaded the Personal Information and Personal Health Information belonging to the Class, without lawful justification or authorization, for their own malevolent purposes; and

(c) A reasonable person would regard the invasion and collection of their Personal Information and Personal Health Information on the defendants' computers as highly offensive causing distress, humiliation, or anguish.

65. The Ministries are vicariously liable for Mr. Sayid's intrusion upon seclusion of each Class Member as a result of the employer-employee relationship between the Ministries and Mr. Sayid at the time of the Breach.

DAMAGES

66. As a result of the defendants' actions, and in particular the defendants' 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.

67. The defendants are 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;

(f) Special damages caused by unlawful conduct by third parties, including identity theft or fraud, occasioned by or attributable the defendants' breaches as alleged herein; and

(g) Damages in accordance with section 24 of the *Charter* to compensate Class Members' for personal losses and suffering, to vindicate the rights of all Class Members, and/or to deter the defendants from allowing preventable, harmful privacy breaches.

68. The defendants' deliberate disregard for the confidentiality and security of the Class Members' Personal Information constitutes a flagrant betrayal of their trust. The defendants knew that medical service providers are at a particularly elevated risk of being targeted by unauthorized users of Personal Information and Personal Health Information, that they were particularly vulnerable to being targeted, and that the data in the Ministries' network would be a valuable treasure trove for unauthorized users. The defendants knew or ought to have known that their 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.

69. Moreover, subsequent to learning of the existence of an extensive privacy breach affecting its own systems and users of its services, the Ministries' 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

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

71. The plaintiff pleads that she has complied in all respects with the *Crown Liability and Proceedings Act*, 2019, S.O. 2019, C. 7 Sched. 17.

PLACE OF TRIAL

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

Date: February 24, 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

C.M.
Plaintiff

and

HIS MAJESTY THE KING et al.
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