ONTARIO
SUPERIOR COURT OF JUSTICE

BETWEEN:

D. MARCHAND

Plaintiff

and

CENCORA INC. and INNOMAR STRATEGIES INC.

Defendants

Proceeding under the *Class Proceedings Act, 1992*, S.O. 1992, C. 6

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, within the time for serving and filing your statement of defence you may move to have this proceeding dismissed 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 Issued by ……

Local registrar

Address of Court office: Ontario Superior Court of Justice
161 Elgin Street, 2nd Floor
Ottawa, ON K2P 2K1

TO: **INNOMAR STRATEGIES INC.**
3470 Superior Court
Oakville, ON L6L 0C4

AND TO: **CENCORA INC.**
1 West First Avenue
Conshohocken, Pennsylvania
United States of America, 19428

RELIEF SOUGHT

1. The Plaintiff, on his own behalf and on behalf of the Class Members, seek the following relief:

a. An order certifying this action as a class proceeding pursuant to the *Class Proceeding Act, 1992*, S.O. 1992, c. 6, as amended ("*CPA*");

b. An order and appointing the Plaintiff as the Representative Plaintiff of the Class;

c. Declarations that:

i. the Defendants owed a duty of care to the Plaintiffs and Class Members in the handling, storage, and protection of their personal health information and other sensitive personal identifying information;

ii. the security breach resulting in the compromise and theft of Plaintiff and Class Members information was caused by the Defendants' breach of the standards of care they were required to meet;

iii. the Defendants violated the Plaintiff and Class Members' common law privacy rights;

iv. the Defendants breached the Plaintiff and Class Members' statutory personal information and privacy protection rights under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; the *Privacy Act*, R.S.S. 1978, c. P-24, s. 2; the *Privacy Act*,

C.C.S.M., s. 2, the *Privacy Act*, R.S.B.C. 1996, c. 373, s. 1; the *Act respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, s. 10; and the *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12, art. 5; and the *Civil Code of Quebec*, C.Q.L.R., c. C.C.Q.-1991, arts. 35-36;

v. the Defendants are jointly and severally liable between themselves for the legally-cognizable injuries suffered by Plaintiff and Class Members;

d. the Defendants violated the *Consumer Protection Act, 2002*, S.O. 2002, c. 30, Sch. A; the *Consumer Protection Act*, C.Q.L.R., c. P-40.1; the *Consumer Protection Act*, R.S.P.E.I. 1988, c. C-19; the *Business Practices and Consumer Protection Act*, S.B.C. 2004, c. 2; the *Consumer Protection and Business Practices Act*, S.S. 2013, c. C-30.2; the *Consumer Protection Act*, R.S.A., 2000, c. C-26.3; the *Consumer Protection and Business Practices Act*, SNL 2009, c. C-31.1; the *Sale of Good Act*, R.S.N.B. 2016, c. 110; and the *Consumer Product Warranty and Liability Act*, S.N.B. 1978, c. C-18.1 (the "Applicable Consumer Protection Legislation");

e. in reliance on s. 24 of the CPA, an aggregate assessment of monetary relief, including nominal damages, and directions for distribution of aggregate damages to Plaintiff and Class Members;

f. general and special damages;

g. punitive and aggravated damages;

h. in reliance on s. 25 of the CPA, a direction for individual inquiries, hearings, and determinations to decide any issues not decided at the trial of the common issues;

i. costs of this action on a substantial indemnity basis plus HST or in an amount that provides full indemnity plus the costs of distribution of an award under ss. 24 or 25 of the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 ("*CPA*");

j. costs of administration and notice, plus taxes, associated with the distribution and the fees payable to a person administering the distribution pursuant to s. 26(9) of the *CPA*;

k. pre-judgment compounded and post-judgment interest pursuant to ss. 128 and 129 of the *Courts of Justice Act*, R.S.O. 1990, c. 43; and

l. Such further and other relief as this Honourable Court deems just.

OVERVIEW

2. The present class action concerns the liability of Defendants Cencora Inc. and Innomar Strategies Inc. with respect to a hacking incident that led to the compromise of thousands of Class Members' personal health and other identifying information collected, stored, retained, and used by the Defendants in the context of administering and delivering patient support programs and/or other services and products to Class Members.

3. Formerly known as Amerisource Bergen, Cencora is one of the largest wholesale purchasers, distributors, and providers of medicines, medications, and medical services in the United States. Innomar Strategies Inc. is Cencora's Canadian subsidiary affiliate.

4. As represented in the letter the Defendants sent to the Plaintiff on 12 July 2024:

> Cencora and its Innomar affiliate partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support and services, business analytics and technology, and other services.

5. Innomar operates approximately 165 clinics and pharmacies throughout Canada. Innomar identifies itself as "Canada's leading service provider for Patient Support Programs" and represents that it "operate[s] the most comprehensive national network of full-service specialty support and reimbursement programs."

6. In the context of administering and delivering patient support programs and services, the private and personal health information of patients paying for these programs and services – including Plaintiff and Class Members – is collected, administered, retained, and otherwise used by Innomar Strategies and Cencora.

7. As Innomar is "Canada's leading service provider for Patient Support Programs," it is reasonably estimated that it holds the personal information of tens of thousands of Class Members across Canada, making it an attractive target for cybersecurity breaches and hacking.

8. On 27 February 2024, Cencora announced in a form required under U.S. law to be filed with the U.S. Securities and Exchange Commission that it had been the victim of a cybersecurity incident involving compromise of personal information. It was later revealed that Cencora and Innomar first learned of the data breach on 21 February 2024, but that the breach had occurred on a previous and still undisclosed date.

9. As communicated to Plaintiff in a letter sent by the Defendants on 12 July 2024, and to other Class Members in an identical letter dated 4 June 2024, some of the personal information of

Plaintiff and Class Members that was compromised in the data breach is identified to include personal health information such as each person's:

> "first name, last name, address, date of birth, height, weight, telephone number, email address, dates and location of service, health diagnosis/condition, medications/prescriptions, medical record number, patient numbers, health insurance/subscriber number, signature, lab results, and medical history."

10. Only on 4 June 2024 – that is, more than three months after they became aware of the data breach – did the Defendants begin to notify affected Class Members that their highly sensitive personal information had been compromised in a data breach.

11. The letter not only confirms that the Defendants learned of the data breach on 21 February 2024, but also that they "confirmed" that Class Members' "personal information was affected by the incident… [o]n April 10, 2024." The almost two-month delay between that confirmation and its communication to Class Members is inexplicable and prevented Class Members from taking steps to protect themselves from the consequences of the compromise of their highly sensitive personal information.

12. The same is true for other Class Members who received an identical notification letter on 1 July 2024 – that is, over four months after the Defendants' discovery of the data breach and three months after they confirmed that Class Members' personal information had been compromised.

13. On 31 July 2024, Cencora's updated filing with Securities and Exchange Commission disclosed that more data was exfiltrated than initially concluded, including additional personally identifiable information and protected health information.

14. The exfiltrated personal information of Plaintiff and Class Members is so sensitive that it exposes them to an increased and significant realistic risk of harm, including identity theft, fraud, and other financial and personal damage that will endure for many years to come.

15. Owing to the highly sensitive nature of the personal information collected, retained, stored, and used by the Defendants – and to the increased risk of future harm to which it concomitantly gives rise – the Defendants ought, but failed to install effective safeguards and protections to prevent the data breach.

16. The Defendants' failure was intentional, wilful, reckless or – at the very least – negligent, as the Defendant knew or ought to have known that their immense cache of sensitive personal information was an attractive target for cybercriminals and that their information technology systems were inadequate and ripe for exploitation.

17. The Defendants' failure to take effective measures to prevent the egregious data breach is compounded by their failure to contain its scope and impact, and by their inexplicable omission to inform Plaintiff and Class Members for several months after first discovering it and confirming that their sensitive personal information had been compromised.

18. Individually and collectively, these failures fell far short of the standard of care applicable to custodians of personal and private information and exacerbated the violation of Plaintiff and Class Members' common law and statutory privacy rights and protections.

19. The Defendants' failure to implement, maintain, administer, and uphold rigorous information security measures, and standards preventing data breaches also reveals that their representations concerning the security of personal information collected and retained from

Plaintiff and Class Members were deceptive and/or misleading and therefore in breach of the Consumer Protection Act and analogous provincial and territorial consumer protection legislation.

20. The Defendant's remedial measure of paying for credit monitoring services provided from TransUnion Canada is inadequate and insufficient for at least three reasons. First, it is only provided for a temporary period of two years, whereas the significant realistic risk of future harm arising from the sensitive nature of the data compromised in the data breach extends far beyond into the future.

21. Second, coverage is partial, as some major banks, like TD Bank, CIBC, Desjardins and HSBC as well as smaller lenders, certain credit unions, and some utility companies do not report to TransUnion.

22. Further, credit monitoring does nothing to prevent the misuse of other sensitive personal information compromised in the data breach that does not fall within the categories of subjects or incidents encompassed within credit reports.

23. The Plaintiff brings the following Class Action on behalf of himself and that of the Members of the Class of which he is a part, namely:

> All persons resident in Canada whose personal information was subject to unauthorized access, discovered by the Defendants on February 21, 2024.

24. The Class is estimated to be comprised of tens of thousands of persons resident in Canada – if not more – but the precise number is within the exclusive knowledge of the Defendants.

THE PARTIES

The Defendants

25. Defendant Innomar Strategies is a legal person constituted under Ontario's *Business Corporations Act*, R.S.O. 1990, c. B-16. Its registered head office is situated in Oakville, Ontario.

26. The Defendant Cencora Inc. is an American corporation formerly known as AmerisourceBergen Corp, and whose headquarters are situated in Conshohocken, Pennsylvania. Cencora is one of the largest wholesalers of medicines in the United States.

27. Cencora Inc. principally carries on business in Canada and Ontario by way of Innomar Strategies Inc. On information and belief, Innomar was acquired by Cencora in 2009, at which point the former became a fully owned subsidiary of the latter. Also on information and belief, Innomar enters into contracts with provincial health authorities as Cencora's agent.

28. Cencora and Innomar Strategies notably specialize in the delivery of services linked to medications used to treat rare medical conditions, cancers, and immunological conditions. As Cencora's affiliate subsidiary in Canada, Innomar Strategies manages the administration of the medications as well as patient support programs in Canada on behalf of drug manufacturers including AbbVie, Bristol-Myers Squibb Canada, Pfizer Canada SRI, Sandoz, Sanofi, and Takeda.

29. The website with the address https://www.innomar-strategies.com features the following logo on the top left side of every page:

30. The identical corporate logo appears on the letter to the Plaintiff and Class Members dated 12 July 2024 and on the identical letter sent to other Class Members on 4 June 2024.

31. Each of the Defendants is jointly liable and/or vicariously liable for the acts and/or omissions of the other based on the following reasons:

a. each was the other's agent;

b. each Defendant's business was operated so as to be inextricably intertwined with the other's business as one corporate enterprise;

c. each Defendant entered into a common advertising and promotion strategy with the other;

d. each Defendant carried their operations pursuant to a common business plan;

e. each Defendant intended that the business appear to be operated, and in fact was operated, as one common business organization.

The Plaintiff

32. The Plaintiff resides in Ottawa, Ontario.

33. In July 2024, the Plaintiff received a letter from the Defendants dated 12 July 2024 and entitled "Re: Notice of Data Security Incident."

34. The letter informed the Plaintiff of the data breach, the nature of the information involved, the measures taken by the Defendants, and what the Plaintiff "can do to address this situation."

35. The letter received by the Plaintiff states that the data security incident was discovered by the Defendants on 21 February 2024, and that the Defendants confirmed on 10 April 2024 that the Plaintiff's personal information had been compromised in the data breach:

> **What Happened?**
> On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

36. The letter is, however, conspicuously silent as to why the Plaintiff was not first notified on 21 February 2024 or as soon as possible thereafter, or why it took the Defendants almost three (3) months to notify the Plaintiff that his personal information had been compromised after confirming same.

37. The Plaintiff has suffered legally-cognizable and compensable injuries that are the direct and proximate cause of the data breach that the Defendants failed to prevent, exacerbated, and failed to promptly notify the Plaintiff and Class Members.

38. On September 17, 2024, the Plaintiff signed up for the free two years of credit monitoring and protection against identity theft from TransUnion that was offered by the Defendants.

39. On September 17, 2024, the Plaintiff purchased credit monitoring and protection against identity theft from Equifax Canada in the amount of $24.95 plus HST per month, as the coverage offered by the Defendants from TransUnion to Class Members is inadequate, temporary, incomplete, and therefore ineffective to guard against the increase realistic risk of future harm including identity theft, fraud, and other harms.

40. The Plaintiff has also suffered moral injury in the form of stress and anxiety rising above the ordinary troubles and inconveniences of life, as well as costs incurred to acquire protection against fraud and identity theft additional to the inadequate measures provided by the Defendants.

NATURE OF THE ACTION

Negligence

40. The Plaintiff and Class Members were owed a duty of care by the Defendants in their collecting, retention, storage, administration, use, and disclosure of Plaintiff and Class Members sensitive personal health and other information. The Defendants were also subject to statutory and industry requirements and standards concerning the preservation of said information's confidentiality.

41. The Defendants committed several breaches of the applicable duties of care owed to the Plaintiff and Class Members. First, the Defendants fell short of abiding by industry standards and their own privacy policies in negligently collecting, storing, retaining, and using the Plaintiff and Class Members' sensitive health and other personal information.

42. Second, the Defendants inexplicably failed to follow standard industry practice in not encrypting the personal health and other information of Plaintiff and Class Members and in failing to implement, maintain, and administer adequate effective measures to safeguard that information, despite knowing of the dire consequences of omitting to do so.

43. Appreciating that there is no tort of statutory breach, an integral part of the Defendants' overall negligent conduct is their violation of the following statutes: the *Personal Health Information Protection Act, 2004*, S.O. 2004, c 3, Sch A; *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c 5; *Health Information Protection Act*, S.S. 1999, c H-0.021; *Health Information Act*, R.S.A. 2000, c H-5; *Personal Information Protection Act*, S.A. 2003, c P-6.5; *Personal Health Information Access and Protection of Act*, S.B.C. 2008, c 38;

Personal Information Protection Act, S.B.C. 2003, c 63; *The Personal Health Information Act*, CCSM c P33.5; *Personal Health Information Act*, S.N.L. 2008, c P-7.01; *Health Information Privacy and Management Act*, SY 2013, c 16; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *Act respecting the sharing of certain health information*, CQLR c P-9.0001; *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1; *Personal Health Information Act*, SNS 2010, c 41; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Health Information Act*, RSPEI 1988, c H-1.41; *Health Information Act*, SNWT 2014, c 2.

44. Finally, the Defendants exacerbated their negligent conduct by additionally negligently failing to notify the Plaintiff and one group of Class Members for almost five months since first discovering the data breach and for three months after confirming that their data had been compromised in that breach,[1] other Class Members for almost four months since discovering the data breach and for almost three months after confirming that their data had been compromised in the data breach.[2]

45. Finally, the Defendants' violation of s. 10 of Québec's *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1 and of Québec Class Members privacy rights under arts. 35-36 of the *Civil Code of Québec*, C.Q.L.R. C.C.Q.-1991 gives rise to a compensable fault under art. 1457 thereof, which provides that "Every person has a duty to abide by the rules of conduct which lie upon him, according to the circumstances, usage or law, so as not to cause injury to another." (emphasis added).

[1] The Plaintiff and Class Members who received the notification letter dated 12 July 2024.
[2] The Plaintiff and Class Members who received the notification letter dated 4 June 2024.

46. The Defendants' negligent and faulty conduct is the proximate or direct and immediate cause of significant legally-cognizable compensable injuries, identified below.

Violations of the *Consumer Protection Act, 2002*

47. The Defendants violated the *Consumer Protection Act, 2002* ["*CPA, 2002*"] and other provincial and territorial consumer protection legislation by making false and/or misleading representations in the form of both positive representations and omissions as concerns the security, reliability, and effectiveness of their information technology infrastructure and measures to ensure the security and protection of sensitive personal health and other information collected from the Plaintiff and Class Members and subsequently retained and used as part of the dispensation of services, programs, medications, medicines, and/or other medical products.

48. At all times relevant to this action, the Plaintiff and Class Members were "consumers" within the meaning of that term as defined in s. 1 of the *CPA, 2002* and provisions of other provincial and territorial consumer protection legislation.

49. At all times relevant to this action, the Defendants were "supplier[s]" as defined in s. 1 of the *CPA, 2002* and provisions of other provincial and territorial consumer protection legislation.

50. The contractual agreements respectively entered into between the Plaintiff and Class Members and the Defendants and pursuant to which the Plaintiff and Class Members purchased the patient support program services and/or medical products, other medical services, medications, medicines, or medical equipment sold to them by the Defendants fall within the definition of "consumer agreement" and "consumer transaction" codified in s. 1 of the *CPA, 2002* and provisions of other provincial and territorial consumer protection legislation.

51. The aforesaid services, products, equipment, medicines, and medications respectively purchased from the Defendants by Plaintiff and Class Members constitute "goods" within the meaning of that term as defined in s. 1 of the *CPA, 2002* and provisions of other provincial and territorial consumer protection legislation.

52. The representations made by and contained in advertising, marketing, packaging and/or instructional materials prepared, authored, and made public by the Defendants, including those found on the Innomar App, fall within the definition of "representation" codified in the *CPA, 2002* and in provisions of other provincial and territorial consumer protection legislation.

53. The definition of "representation" contained in s. 1 of the *CPA, 2002* is as follows:

> "representation" means a representation, claim, statement, offer, request or proposal that is or purports to be
>
> (a) made respecting or with a view to the supplying of goods or services to consumers, or
>
> (b) made for the purpose of receiving payment for goods or services supplied or purporting to be supplied to consumers"

54. The "representations" encompassed within the *CPA, 2002* and of other provincial and territorial consumer protection legislation are not limited to active statements but also extend to omissions and the failure to disclose information that a reasonable consumer would consider material.

55. The representations at issue were made respecting or with a view to the supplying of patient support services and/or medical equipment, products, services, medicines, and medications paid for by the Plaintiff and Class Members. A reasonable consumer would expect that the representations concerning the security of their highly sensitive personal medical information would indeed be accurate, failing which they would not enter into the contract that required them

to provide said information as a condition precedent to the dispensing of said services, programs, products, medications, medicines, and/or equipment.

56. As noted, the misrepresentations at issue in the present proposed class action concern the Defendants' repeated, deliberate, intentional, continuous, flagrant, ongoing omissions and failure to disclose to prospective purchasers that their information technology and/or data storage and protection systems were insufficient, ineffective, and/or vulnerable to cybersecurity breaches of the kind discovered by the Defendants on February 21, 2024.

57. The abovementioned active and passive misrepresentations constitute "Unfair Practices" within the meaning of Part III of the *CPA, 2002* and analogous provisions of other provincial and territorial consumer protection legislation.

58. Section 14(1) of the *CPA, 2002* provides that "It is an unfair practice for a person to make a false, misleading or deceptive representation," which s. 14(2) in turn identifies as including, but not being limited to:

- "A representation using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if such use or failure deceive or tends to deceive." (14)
- "A representation that the goods or services have sponsorship, approval, performance characteristics, accessories, uses, ingredients, benefits or qualities they do not have." (1)
- "A representation that the goods or services are of a particular standard, quality, grade, style or model, if they are not." (2)

59. As "[i]t is an unfair practice for a person to make a false, misleading or deceptive representation" and as "No person shall engage in an unfair practice" under ss. 14(1) and 17(1) of

the *CPA, 2002*, the Plaintiff and Class Members located in Ontario at the time the consumer transactions were made are entitled to remedies under s. 18(1) and/or (2).

60. Class Members who were situated in provinces other than Ontario are also entitled to remedies equivalent or analogous to those contemplated under s. 18(1) and/or (2) pursuant to the other consumer protection legislation respectively applicable to them.

61. Consistent with s. 2(1) of the *CPA, 2002*, the Plaintiff and Class Members rely upon the said Act in respect of all transactions at issue in the present proposed class action in which the consumer was located in Ontario when the transaction took place, and on the consumer protection legislation respectively applicable in each of the provinces and territories in which the non-Ontario Class Members were located at the time their respective transactions took place.

Violations of Provincial Privacy Legislation

62. The Defendants breached the Plaintiff and Class Members' statutory personal information and privacy protection rights under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; the *Privacy Act*, R.S.S. 1978, c. P-24, s. 2; the *Privacy Act*, C.C.S.M., s. 2, the *Privacy Act*, R.S.B.C. 1996, c. 373, s. 1; the *Act respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, s. 10; and the *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12, art. 5.

63. The British Columbia, Newfoundland, Saskatchewan, and Manitoba legislation all provides for a statutory tort for the violation or breach of Plaintiff and Class Members' privacy. This tort is actionable without proof of loss or damage.

64. It is indisputable that the personal information compromised in the underlying data breach is health and other sensitive personal information that forms part of Plaintiff and Class Members' respective biographical cores, attracts a high reasonable expectation of privacy, and entails significant realistic risks of being used for identity theft, fraud, and other harms when exfiltrated and stolen as part of a cybersecurity breach deliberately intended to steal said information.

65. The Defendants intentionally, wilfully, recklessly, or wilful blindly violated the privacy of Plaintiff and Class Members by failing to provide for effective measures to prevent, protect, and thwart the unauthorized access and misappropriation of Plaintiff and Class Members' personal health and other private information encompassed within the privacy protections of the aforementioned legislative regimes.

REMEDIES

Compensatory Damages

66. The Plaintiff and each Class Member has suffered legally-cognizable and compensable injuries and loss as a direct and proximate result of the Defendants' unlawful and tortious conduct.

67. The fundamental purpose of the law of compensatory damages is that the Plaintiff is to be compensated to the extent of the harm or loss suffered as a result of the Defendant's conduct (*restitutio in integrum*).

68. The Plaintiff claims on his own behalf and of that of Class Members, (a) the recovery of the entirety of monies spent to purchase credit monitoring and identity theft protection from Equifax; (b) the costs to purchase credit monitoring and identity theft protection beyond the time period offered free by the Defendants (i.e. 2 years) from Equifax and/or TransUnion – the whole

to palliate the inadequate, partial, ineffective and temporary credit monitoring protection from TransUnion that was offered by the Defendants to Plaintiff and Class Members; (c) the costs to purchase data removal services to have personal information removed from the dark web; and (d) the costs to purchase protection against malicious links (phishing, etc.) sent by email and SMS.

69. The Plaintiff claims for non-pecuniary damages flowing from the stress and anxiety arising from the theft of his and Class Members' highly sensitive personal information that exceed the ordinary troubles and inconveniences of life.

70. The Plaintiff also claims for the time and effort expended by Class Members trying to avoid suffering injury or correcting injury already suffered, such as fraud and identity theft.

Punitive Damages

71. The Plaintiff seeks on his own behalf, and of that of Class Members, punitive or exemplary damages for the Defendants' conduct at issue in the present proposed class action.

72. First, the Plaintiff seeks punitive or exemplary damages for Defendants' flagrant and undeniable violations of the prohibitions of false, misleading or deceptive representations under Part III of the *CPA, 2002* and equivalent prohibitions and provisions under the consumer protection legislation in other provinces and territories.

73. In particular, ss. 18(11) of the *CPA, 2002* expressly provides that "A court may award exemplary or punitive damages in addition to any other remedy in an action commenced" under the said *Act*. Equivalent or analogous provisions of provincial and territorial consumer protection legislation also provide for punitive or exemplary damages.

74. In addition, or alternatively, the Plaintiff also seeks punitive or exemplary damages on their own behalf and that of Class Members in respect of the Defendants' conduct falling beyond the scope of the *CPA, 2002* and other provincial and territorial consumer protection legislation.

75. The said conduct displayed serious negligence, carelessness, and ignorance, and was oppressive, callous, high-handed, wilful, outrageous, deliberate, wanton, reckless, and in total disregard for the rights and interests of Plaintiff and Class Members.

76. In particular, the Defendants failed to notify Class Members of the data breach for over three[3] or four months[4] after initially discovering it on February 21, 2024, and close to two months[5] and over three months[6] after confirming on April 10, 2024 that their respective personal information had been compromised in the data breach. This conduct directly prevented Plaintiff and Class Members from taking measures to prevent identity theft, fraud, and other measures to protect themselves from the consequences of the data breach.

77. The Plaintiff asserts that an award of punitive damages is required to denounce and condemn the Defendants' shocking and outrageous conduct and to deter further breaches by the Defendant and/or others.

JURISDICTION

78. The Plaintiff contends that there is a real and substantial connection between the Province of Ontario and the out-of-province Class Members and Defendants by virtue of the Defendant Innomar Strategies Inc. being headquartered, carrying on business, and having committed torts in

[3] For Class Members receiving the notification letter dated June 4, 2024.
[4] For Class Members receiving the notification letter dated July 12, 2024.
[5] For Class Members receiving the notification letter dated June 4, 2024.
[6] For Class Members receiving the notification letter dated July 12, 2024.

Ontario, and by virtue of contracts connected with the dispute having been made in the Province within the meaning of the Supreme Court of Canada's judgment in *Club Resorts Ltd. v. Van Breda*, 2012 SCC 17.

VENUE

79. The Plaintiff proposes that the present class action be tried in Ottawa, Ontario.

DATE: September 19, 2024

CONSUMER LAW GROUP P.C.
251 Laurier Ave. West, Suite 900
Ottawa, ON K1P 5J6

Tel: (613) 627-4894
Fax: (613) 627-4893

Jeff Orenstein (LSO No. 59631G)
Lawrence David (LSO No. 69517L)

Lawyers for the Plaintiff