Court File No.: [ ]

FEDERAL COURT

PROPOSED CLASS ACTION

BETWEEN:

LAURANCE CLARKE

PLAINTIFF

AND:

HIS MAJESTY THE KING, BGRS LIMITED, SIRVA, SIRVA CANADA, SIRVA BGRS WORLDWIDE INC.

DEFENDANTS

STATEMENT OF CLAIM

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 a solicitor acting for you are required to prepare a statement of defence in Form 171B prescribed by the *Federal Court Rules,* serve it on the Plaintiff' solicitor or, where the Plaintiff do not have a solicitor, serve it on the Plaintiff, and file it, with proof of service, at a local office of this Court, WITHIN 30 DAYS after this statement of claim is served on you, if you are served within Canada.

If you are served 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 for serving and filing your statement of defence is sixty days.
Copies of the Federal Court Rules information concerning the local offices of the Court and other necessary information may be obtained on request to the Administrator of this Court at Ottawa (telephone 613-992-4238) or at any local office.

IF YOU FAIL TO DEFEND THIS PROCEEDING, judgment may be given against you in your absence and without further notice to you.

Toronto, February 14, 2024

Issued by:

(Registry Officer)

Address of Local Office:
180 Queen Street West
Suite 200
Toronto, ON M5V 3L6

TO: THE ATTORNEY GENERAL OF CANADA
Attention: Shalene Curtis-Micallef, Deputy Attorney General of Canada

AND TO: BGRS LIMITED
39 Wynford Drive
North York, ON M3C 3K5

AND TO: SIRVA
One Parkview Plaza
Oakbrook Terrace, IL 60181
United States of America

AND TO: SIRVA CANADA
80 Aberdeen Street
Suite 100
Ottawa, ON K1S 5R5

AND TO: SIRVA BGRS WORLDWIDE INC.
One Parkview Plaza
Oakbrook Terrace, IL 60181
United States of America

CLAIM OF THE PLAINTIFF

RELIEF CLAIMED

1. The Plaintiff claims on his own behalf and on behalf of the proposed class members, as follows:

   (a) an order pursuant to Rules 334.16(1) and 334.17 of the *Federal Court Rules* (the "Rules") certifying this action as a class proceeding and providing any ancillary directions;

   (b) an order pursuant to Rules 334.12(3), 334.16(1)(e) and 334.17(b) appointing the plaintiff as the representative plaintiff for the Class;

   (c) damages for negligence, breach of contract, breach of confidence, breach of privacy, intrusion upon seclusion, breach of the statutory torts under the Privacy Acts as described below and breaches of the *Civil Code of Quebec*, the *Act respecting the protection of personal information in the private sector*, and the *Quebec Charter of Human Rights*, including damages for:

      (i) breach of the right to informational privacy, moral damages, violations of privacy

      (ii) costs incurred in preventing identity theft;

      (ii) identity theft and financial harms ;

      (iii) damage to credit reputation;

      (iv) prolonged mental distress;

      (v) out-of-pocket expenses;

      (vi) inconvenience, frustration and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft or other improper use of credit information; and

      (vii) time lost in precautionary communications with third parties such as credit card companies, credit agencies, creditors, utilities, cable and internet providers, and other parties to inform them class members' credit information has been misappropriated and/or posted for sale on the Dark Web;

   (d) punitive damages;

(e) pre- and post-judgment interest pursuant to sections 36 and 37 of the *Federal Courts Act*;

(f) an order directing BGRS and SIRVA to delete and destroy the personal information of any class members whose relocation services have been completed; and

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

THE PARTIES

2. The Plaintiff, Laurance Clarke, is a resident of Nova Scotia and a serving member of the Canadian Armed Forces. Mr. Clarke relocated from Cape Breton, Nova Scotia to Halifax, Nova Scotia in August 2013. He was directed by the Crown to use BGRS' relocation services to move himself and his family. He provided BGRS with his name as well as those of his spouse and children. He provided them with his direct deposit banking information in order to settle bills. He also provided them with copies of his photo ID, service number and other military identification.

3. The Defendant, His Majesty the King, is named as a representative of the Federal Government of Canada (the "**Crown**").

4. The Defendant BGRS Limited (formerly "Brookfield Global Relocation Services") is a company that provides relocation services to governments and other entities. BGRS administers more than 14,000 relocations per year, maintaining over 8,000 third-party suppliers for activities related to member relocations. It is headquartered in Ottawa, Canada.

5. The Defendant SIRVA Canada is the Canadian subsidiary of SIRVA, a company which provides relocation services to governments and other entities. SIRVA was formed after the merger of North American Van Lines and Allied Vanlines. BGRS and SIRVA Canada have offices in Toronto and Ottawa and merged with each other in late 2022. SIRVA BGRS Worldwide, Inc., SIRVA and BGRS are referred to as the "**vendors**").

CLASS DEFINITION

6. The class is defined as current and former Government of Canada employees, members of the Canadian Armed Forces and Royal Canadian Mounted Police whose personal information was collected and retained by BGRS and/or SIRVA between 1999 and 2023 whose information was compromised in the breach (hereinafter "**class members**").

7. In the alternative, if the defendants identify everyone whose data was compromised and circulate a notice letter to the class, then the class will be everyone who received the notice letter.

8. Personal information, as used herein, means information about an identifiable individual, and in this case, includes but is not limited to, an individual's name, contact information, passport details, financial information such as bank account details, direct deposit information, credit card statements and other financial details reflecting confirmation of expenses incurred in relocation.

FACTS

9. Since approximately 1995, the Crown has contracted with BGRS to provide relocation support/services to class members. Starting around 2009, the Crown also contracted with SIRVA to provide similar services.

10. In the course of their careers, members of the Canadian Armed Forces, RCMP officers and other individuals who work for or with the federal government of Canada may be required to move in order to take a new position or as part of their duties.

11. When an individual is required to relocate, the government of Canada will generally provide them with a "relocation instruction". The relocation instruction will direct the individual to make use of BGRS or SIRVA and define the parameters for their move.

12. Individuals are instructed to create an online account using a portal on the BGRS Member Secure Website (MSW), or the equivalent SIRVA website. When creating an account, individuals are required to enter their personal information, such as name, address (new relocation address), passport information (if relocating internationally) and sensitive financial details.

13. The creation of an account also involves agreeing to the terms of use for relocation services, creating a contract between class members and the vendors. These contracts, which are not publicly available, included terms regarding how long class members' information could be held, what security measures would be taken and made explicit

references to the privacy policies which are publicly available for both SIRVA and BGRS. These contracts will be plead in further detail when they are made available to the plaintiff.

14. The individual will then be connected through their BGRS and/or SIRVA account to approved services to help with their move. The personal information gathered at the registration step is used in the process of the move.

15. Throughout the move, class members are required to submit valid receipts (scanned) through the portal to finalize their reimbursement claims. In doing so, they will submit sensitive financial information such as direct deposit information or credit card numbers and statements.

16. Once the individual has relocated and all reimbursements have been issued, there is a final statement of account which signals that the move (from the point of view of the Vendor and the government) is over. At that point, there is no need for the vendors to hold class members' personal information any longer.

17. Unfortunately, the vendors continued to hold the information, on a perpetual basis.

BGRS and SIRVA

18. BGRS and SIRVA merged in late 2022. Throughout the claim they will be referred to separately, as much of the relevant Class Member information was provided to them while they were still separate entities.

The Breach

19. On or about September 29, 2023, the vendors both experienced a cyberattack in which they were locked out of their systems through ransomware while criminals obtained complete

access to their computer systems, including the personal information for every class member who used either vendors' relocation services between at least 1999 and 2023. At the same time, the vendors were locked out of their computer systems through 'ransomware' software.

20. On or about October 19, 2023, BGRS informed the Crown of the cyberattack.

21. The Crown first issued an alert about a September online attack on BGRS servers on October 20, 2023. Its updated announcement on November 17, 2023, revealed that hackers had accessed data from BGRS as well as SIRVA.

22. On or about November 23, 2023, the Crown circulated notice by email to some impacted individuals of the attack but to date, the vast majority of the class have yet to receive notice.

23. The hacker group LockBit (the "**Hacker**") claimed to have conducted the hack and has circulated some or all of the personal information on the dark web. The group accessed archives containing 1.5 terabytes of stolen documents and made it available for sale on the dark web.

24. In a message posted on its website dated on or about December 15, 2023, the Crown recommended that anyone who was affected do the following:

    a) update login credentials that may be similar to those used with BGRS or SIRVA Canada;

b) enable multi-factor authentication on accounts that are used for online transactions; and

c) monitor financial and personal online accounts for any unusual activity.

25. Anyone who saw "unauthorized access to personal or financial accounts" was advised to contact their financial institutions immediately, contact local policy and contact the Canadian Anti-Fraud Centre.

26. The government has publicly stated that it intends to offer one year of free credit monitoring to affected class members through Equifax. However, as of February 2024, this has not yet been offered to all affected class members. Instead the Crown has publicly warned that individuals who purchase their own credit monitoring in the interim will not be reimbursed.

Contracts

27. As set out above, class members agreed to terms of use or account agreements when they signed up for relocation services accounts with the vendors. These agreements incorporated the vendors' privacy policies, and, as a result, also incorporated PIPEDA. The agreements also contained terms setting out how class members' information would be used, how it would be stored and secured, and how long it could be kept for.

28. These terms included express or implied statements that the information would be stored securely and encrypted.

Privacy Policies

29. Both BGRS and SIRVA have privacy policies which govern their collection of personal information from class members. These policies are made publicly available to users of their websites, including class members.

30. BGRS represents to its customers that “The BGRS Privacy Policy is based on, and complies with, Canada's personal information Protection and Electronic Documents Act ("PIPEDA"), which includes the Ten Privacy Principles outlined in the Canadian Standards Association Model Code for the Protection of Personal Privacy.”

31. Under Principle 5, BGRS states “Personal information will only be used or disclosed for the purpose for which it was collected unless the customer has otherwise consented, or when it is required or permitted by law. Personal information may only be retained for the amount of time needed to fulfil the purpose for which it was collected.”

32. Under “How we safeguard your personal information” BGRS writes that “BGRS have extensive controls in place to maintain the security of their information and information systems. Client files are stored according to their sensitivity. Appropriate controls (such as restricted access) are placed over our computer systems and data processing procedures. Physical access to areas where personal information is gathered, processed or stored, is limited to authorized employees. Where requested by your employer, your file will be returned to your employer after your file has closed.”

33. Under “Web site security” they write “BGRS is committed to your privacy and will ensure that any information you access or provide through this site remains secure.”

34. In their Privacy Statement, SIRVA Canada LP writes that "SIRVA Canada uses the privacy standards recommended by the Canadian Standards Association and adopted as part of the personal information Protection and Electronic Documents Act."

35. Under "Limiting Use, Disclosure & Retention" they write "Personal information shall be retained only as long as necessary for the fulfillment of those purposes or as required by Federal Law."

36. Under "Safeguarding Information", they write "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

37. SIRVA maintains a second privacy policy document in which they write "Sirva, Inc. ("Sirva") maintains this Privacy Policy for all persons to whom we provide services. Sirva is committed to complying with all applicable privacy laws."

38. Under "Information Use, Sharing & Storage", SIRVA writes that "Your personal information will be processed and retained as needed to provide you with your services. This may include a period of time after the services are complete in order to comply with our regulatory, audit, contractual and other legal obligations."

39. Under a section called, "For Customers in Canada" SIRVA writes "Canada's personal information Protection & Electronic Documents Act ("PIPEDA") covers our customers in Canada and their personal information."

40. Under "Data Integrity & Security" SIRVA writes "Sirva retains personal information for as long as we have determined it is needed for the purposes for which it was received or as

required by contractual, record keeping, or other legal requirements." They also write "We maintain physical, electronic and procedural safeguards to protect your personal information. We regularly assess security standards and procedures to protect against unauthorised access to personal information."

Real and Substantial Risk of Harm

41. Class members face a real and substantial risk of harm because their stolen personal information has been disseminated on the dark web by criminal hackers and is available for purchase by other hackers and bad actors. The class is exposed to a real and substantial risk of cybercrimes, such as the creation of fictitious bank accounts, or the use of their personal information to maliciously obtain loans, secure credit cards or to engage in other forms of identity theft and/or fraud.

42. The breach has not been contained and repaired, and the only reasonable course of action open to class members is to take steps to protect themselves through credit monitoring. The fact that the Crown has offered free credit monitoring, however inadequate, is further evidence of the reality of the risk.

CAUSES OF ACTION

Vicarious Liability for the vendors

43. The Crown selected each of the vendors to perform relocation work. The Crown closely dictated the work that the vendors were to perform and the parameters within which they performed it. Had the Crown performed the relocation services itself; it would have had an obligation under PIPEDA to protect the personal information of class members and delete

or destroy it when it was no longer necessary to perform the services for which it was collected. In these circumstances, the Crown's duty to protect personal information was a non-delegable duty and the crown is vicariously liable for the misconduct of the vendors.

44. Further and in the alternative, the Crown entered into an agency agreement with the vendors, in which they were its agents for the purpose of relocating class members. The agency relationship was implicit in the contract(s) between the Crown and the vendors as the vendors were required to take steps to move class members from one location to another in the way that the Crown would if it had not contracted out the work. When the contracts are made available to the plaintiffs, additional details regarding the agency relationship will be plead.

45. By directing class members to the vendors, the Crown implicitly or explicitly communicated to class members that the vendors were authorized to provide them relocation services, and to collect the personal information on behalf of the Crown and that they were doing so as agents on behalf of the Crown. The Crown directed class members to use the vendors and set up a detailed and highly technical system through which they would work with the vendors. Several Crown websites refer directly to the vendors' sites as if the vendors were merely arms of the Crown.

46. In the further alternative, the Crown entered into contracts with the vendors that governed what information they collected as well as the protection of class members' information. These contracts, which will be plead with more particularity once they are available to the

plaintiff, specified that the vendors would comply with PIPEDA. The Crown was negligent in selecting the vendors and in enforcing its contracts as plead more particularly below.

47. The result of the Crown's negligence in selecting the vendors and enforcing its contracts, as well as holding the vendors out to the class as cloaked with the authority to collect class members' personal information is that the Crown is vicariously liable for the misconduct of the vendors, which is particularized below.

Negligence – The Crown

48. The Crown owed a duty of care to the class members to ensure that when it directed class members to transfer their personal information to the vendors, it would not be lost, disseminated or disclosed to unauthorized persons and would be deleted and destroyed by the vendors after it was no longer needed for their move.

49. Specifically, the Crown owed a duty of care to class members to ensure that its designated vendors and/or agents took reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack, to ensure that any entity which it entrusted with the class members personal information did the same, and took appropriate steps to limit the exposure of the class members' personal information even in case of a successful cyberattack.

50. The Crown also owed a duty to class members to ensure that it enforced its contracts with the vendors and audited whether they were complying with the contracts.

51. There was a sufficient degree of proximity between the class members and the Crown at an operational level to establish a duty of care because:

a) it was reasonable for the plaintiff and other class members to expect that the Crown had selected vendors who class members were required to use for relocation services had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their personal information in case of a cyberattack, especially where the Crown created a situation where class members were required to provide their personal information to its vendors in order to secure continued employment and be reimbursed for relocation expenses;

b) It was reasonably foreseeable to the Crown that, if a cyberattack resulted in the theft of the class members' personal information, the class members would sustain damages, such that the Crown should have been mindful of the class members' privacy and on guard against a cyberattack.

c) It was reasonably foreseeable to the Crown that, if vendors failed to take appropriate security measures and to implement programs and policies designed to protect personal information, or to ensure that parties that they contracted with did the same, there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

d) In particular, it was reasonably foreseeable to the Crown that if personal information was not removed and/or deleted by its vendors when it was no longer needed, it would be available to any party which was able to successfully hack their systems;

e) The class members were entirely vulnerable to the Crown, in terms of relying on the Crown to select vendors who would take appropriate security measures to protect their personal information and comply with principle 4 of PIPEDA in terms of security and retention;

f) there is a sufficient degree of proximity between the class members and the Crown because the class members are, or were, members of the RCMP and armed forces.

g) The Crown was required by sections/principles 4.1, 4.5 and 4.7 of Schedule 1, of The personal information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"), to implement safeguards appropriate to the sensitivity of the information stored on their network and ensure their vendors did so, these safeguards included appropriate protections for the information and a requirement not to retain the information longer than needed;

h) It was reasonable for class members to expect the Crown would have its vendors delete and destroy personal information when the relocation ended and the need to have class members personal information was no longer required under principle 4.5.

52. The Crown failed in its duty to implement an appropriate standard of care in selecting, establishing guidelines for vendors and enforcing on the vendors those guidelines including adequate security safeguards and data retention in collecting, managing, storing, securing and/or deleting the class members' personal information, particulars being described below:

a) it failed to establish guidelines requiring its vendors to handle the collection, retention, security and disclosure of the class members' personal information in accordance with obligations under PIPEDA;

b) it failed to require its vendors to handle the collection, retention, security and disclosure of the class members' personal information in accordance with its promises and representations to class members;

c) it allowed the personal information to be used,retained and disclosed by its vendors for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule 1 to the PIPEDA;

d) it failed to require its vendors to keep the class members' personal information secure and confidential;

e) it failed to require its vendors to protect the class members' personal information from compromise, disclosure, loss or theft;

f) it failed to have a vendor risk management policy in place;

g) it failed to properly scrutinize the vendors' risk assessment policies and penetration testing strategies;

h) it failed to confirm that the vendors had sufficient basic security controls;

i) it failed to take steps to prevent the class members' personal information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet;

j) it failed to enter into data security and management contracts with its vendors or in the alternative failed to monitor and enforce such contracts; and

k) it failed to direct vendors to delete and destroy the personal information of class members when there was no longer a proper purpose for retaining the personal information.

Negligence – BGRS and Sirva

53. The class members retained the vendors BGRS and/or Sirva to perform relocation services. The vendors owed a duty of care in their collection, use and retention of the personal information, to keep the personal information confidential and secure, and to ensure that it would not be lost, disseminated or disclosed to unauthorized persons and to delete and destroy the personal information when it was no longer needed for their move.

54. Specifically, the vendors owed a duty of care to ensure they took reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and to ensure they took appropriate steps to limit the exposure of the class members' personal information even in case of a successful cyberattack.

55. There was a sufficient degree of proximity between the class members and the vendors to establish a duty of care because:

a) it was reasonable for the plaintiff and other class members to expect that the vendors had implemented appropriate security safeguards against a cyberattack and to limit the exposure of their personal information in case of a cyberattack by implementing appropriate safeguards and by destroying information after it was no longer needed;

b) it was reasonably foreseeable to the vendors that, if a cyberattack resulted in the theft of the class members' personal information, the class members would sustain damages, such that it should have been mindful of the class members' privacy and on guard against a cyberattack.

c) it was reasonably foreseeable to the vendors that if they failed to take appropriate security measures and to implement programs and policies designed to protect personal information there was a risk that the class members' privacy would be breached, because of the sensitivity of the types of data collected and stored, and the climate of increasing cyberattacks targeted toward institutions which collect sensitive and private information;

d) In particular, it was reasonably foreseeable to the vendors that if personal information they collected was not destoyed and/or deleted when it was no longer needed, it would be available to any criminal who was able to successfully hack its systems;

e) The class members were entirely vulnerable , in terms of relying on the vendors to take appropriate security measures to protect their personal information and to limit its retention in accordance with PIPEDA ;

f) There was a contractual relationship between the class members and the vendors;

g) The vendors were required by clauses 4.1, 4.5 and 4.7 of Schedule 1 of PIPEDA, to implement safeguards appropriate to the sensitivity of the information stored on their network and ensure their agents did so;

h) It was reasonable for class members to expect the vendors to comply with PIPEDA which, pursuant to section 5, is mandatory and in so doing would delete and destroy all personal information it collected when the need to retain the information no longer existed.

56. The vendors failed in their duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, securing and/or deleting the class members' personal information, particulars being described below:

a) they failed to handle the collection, retention, security and disclosure of the class members' personal information in accordance with their obligations under PIPEDA;

b) they failed to handle the collection, retention, security and disclosure of the class members' personal information in accordance with their promises and representations to class members;

c) they allowed the personal information to be used and disclosed for purposes other than those for which it was collected, contrary to clause 4.5 of Schedule 1 of PIPEDA;

d) they failed to keep class members' personal information secure and confidential;

e) they failed to protect class members' personal information from compromise, disclosure, loss or theft;

f) they failed to have risk management policies in place ;

g) they failed to have proper risk assessment policies and penetration testing strategies;

h) they failed to have sufficient basic security controls;

i) they failed to take steps to prevent the class members' personal information from being lost, disseminated, or disclosed to the public and unauthorized persons, and from being posted on the internet;

j) they failed to delete and destroy the personal information of class members when there was no longer a proper purpose for retaining the personal information;

Negligence Acts

57. As a direct result of the defendants' negligence, the Hacker was able to invade/gain access to and exfiltrate class members personal information, resulting in the class members sustaining damages or loss, caused by the fault of two or more persons.

58. But for the vendors' negligent data security and data retention practices, the Hacker could not have stolen and disseminated class members personal information.

59. But for the Crown's negligent referral practices and inappropriate supervision and enforcement of its contracts, the Hacker could not have stolen and disseminated class members' personal information.

60. The tortious acts of the defendants in negligence combined with the intentional tortious acts of the Hacker to produce the same damage. Both were materially contributing causes giving rise to non-pecuniary and pecuniary damages for violations of informational privacy, intrusion and moral damages.

61. The class members sustained indivisible injuries including distress, humiliation, anguish, reduced trust, feelings of lost privacy, ongoing increased levels of stress as well as pecuniary damages, all as a result of the combined tortious conduct of the defendants and the Hacker rendering the defendants liable with the Hacker for intrusion damages and statutory tort privacy damages sustained by the class members. These injuries have caused harm to the health, welfare, social, business and financial positions of the class members.

62. The plaintiff pleads and relies on the Negligence Act [RSBC 1996] Chapter 333 section 4(2)(a); the Negligence Act, RSO 1990, c N.1, section 1; the Contributory Negligence Act, RSS 1978 c C-31, section 3(2); the Contributory Negligence Act, RSA 2000, c C-27, sections 1 and 2; the Contributory Negligence Act, RSNB 2011, c 131, sections 1 and 3; the Tortfeasors and Contributory Negligence Act, CCSM c T90, sections 2 and 5; the Contributory Negligence Act, RSNS 1989, c 95, section 3; the Contributory Negligence Act, RSPEI 1988, c C-21, section 1; the Contributory Negligence Act, RSY 2022 c 42, section 1; the Contributory Negligence Act, RSNWT 1988, c C-18, sections 2 and 3; and

the Contributory Negligence Act, RSNL 1990, c C-33, section 3 (collectively, the "Applicable Negligence Legislation").

Class Members are Third Party Beneficiaries of Contracts with Crown

63. The vendors were retained by the Crown to provide relocation services to class members on behalf of the Crown. In offering to provide relocation services, the vendors contracted with the Crown to the effect that any information they collected from class members would be secured in accordance with PIPEDA, with strict safeguards and rigorous privacy and security standards appropriate to the sensitivity of the personal information. The vendors also promised that they would only retain class members' personal information for so long as it was necessary to provide the relocation services. Class Members are third party beneficiaries of the contract(s) between the Crown and the vendors because the contract(s) between the Crown and the vendors explicitly and implicitly contemplated benefits (the safeguards and security standards) which were aimed at class members – the individuals who would be providing their personal information to the vendors. One object of the contract(s) was that class members' personal information would enjoy adequate protection when provided to the vendors.

64. The Crown breached is contracts with the vendors by failing to enforce the privacy and security standards it contracted for on behalf of class members.

Contracts Between Class Members and the Vendors

65. The vendors also formed contracts directly with class members when class members signed up for their services, as pleaded more particularly above. These contracts explicitly

included compliance with the provisions of PIPEDA as a term of the contract as noted in the vendors' privacy policies.

66. The vendors breached their contracts with the plaintiff and the class members in the following ways:

    a) Contrary to the contractual promise that the data would be stored "securely" and "with appropriate controls", they failed to implement rigorous security standards;

    b) Contrary to the contractual promise that they would regularly asses their own security standards, they failed to assess them regularly or at all;

    c) Contrary to the promise that information would be protected according to its sensitivity and there would be extensive controls in place for records, they failed to encrypt the data on their systems;

    d) Contrary to the explicit promise that they would abide by the principles and requirements of PIPEDA, they contravened section 5 of PIPEDA, as well as clauses 4.1, 4.5 and 4.7 of Schedule 1 of PIPEDA; and

    e) Contrary to the explicit promise that personal information would be retained only as long as it was necessary for the purposes for which it was collected, they failed to comply with their own retention policies by not deleting the personal information when it was no longer necessary.

67. As a result of the breach of contract, class members' personal information was hacked and class members suffered damages as detailed below.

Breach of Confidence against the vendors

68. Class members were required to provide personal information to the vendors which was then collected and stored electronically on their internal computer networks.

69. Class members' personal information was confidential, exhibited the necessary quality of confidence, was not public knowledge, and involved sensitive private details about the personal affairs of the class members.

70. Class members' personal information was imparted to the vendor defendants in circumstances in which an obligation of confidence and trust arose, including an explicit assurance these Defendants would keep the information confidential.

71. The vendors received confidential information for a specific purpose, being to assist in providing relocation services and to document expenses for reimbursement by the Crown. Once those services were completed, the vendors were required by law (clause 4.5 of Schedule 1 of PIPEDA) to delete and destroy the confidential information but failed to do so. Instead, the vendors intentionally retained all class members personal information in perpetuity, contrary to law.

72. The vendors' continued retention of the personal information after their services were completed was for a non-permitted use. The vendors did not have consent or meaningful consent as defined by PIPEDA and in any case were not permitted by law to retain the information because of their mandatory imperative obligation under section 5 of PIPEDA to delete and destroy the personal information when its services came to an end.

73. By failing to delete and destroy the personal information when the relocations were complete and by continuing to store and/or use the information in contravention of the PIPEDA, including sections 4.1, 4.5 and 4.7 of Schedule 1 to that legislation, these defendants used the personal information for a non- permitted use.

74. The vendors improper retention practices constituted a non -permitted use to the detriment of the class members because the misuse resulted in a Hacker gaining unauthorized access to the confidential personal information to the detriment of the class members. As a result, the class members sustained nonpecuniary and pecuniary damages. The vendors are therefore liable for the tort of breach of confidence.

75. The Crown is vicariously liable for the vendors' breaches of confidence.

Intrusion Upon Seclusion – The Hacker

76. The tort of intrusion upon seclusion is made out against the Hacker because:

    a) the Hacker intentionally invaded the class members' privacy;

    b) class members' personal information was invaded without lawful justification; and

    c) the personal information that was invaded is highly sensitive and a reasonable person would consider the invasion to be highly offensive causing anguish, humiliation or distress.

77. The personal information was highly sensitive because it was the information necessary for an individual to establish their identity in a new location – both with the Crown and with businesses. As a result, the same information could easily be used to assume the identity of individuals, apply for a credit card, open a bank account, receive government benefits such as CPP, employment insurance, to receive tax refunds, to work illegally or to obtain credit, and ruin credit ratings.

78. The degree of the intrusion was significant because the extracted data was posted on the dark web and made available for sale. The hack has put each Class Member at a real and substantial danger of financial harm for an indefinite period of time, including the foreseeable future. There is no way for class members to know when their risk of harm will be at an end. The type of personal information for sale will be of value to criminals indefinitely to commit crimes such as identity theft and class members risk becoming the subject of phishing attacks and scams. Because the data has been released for sale to criminals on the dark web and because of the sensitivity of the personal information, class members experienced distress, humiliation, anguish, reduced trust, feelings of lost privacy, and ongoing increased levels of stress.

79. The intrusion was highly offensive to a reasonable person because class members' personal information was stolen by criminals.

80. The context of the unauthorized access to the information is a setting where, based on the vendors' privacy policies and their status as contractors for the Crown, people had a reasonable expectation of high levels of privacy protection and confidentiality.

81. The conduct and circumstances of the invasion were the vendors' lax cyber security practices and improper and unlawful date retention practices. The objective of the cyber-attack was to steal class member information for profit.

82. The objectives and expectations of the class members whose privacy was invaded was guided by the defendants' assurances the personal information was safe and secure and the class could place their trust in the vendors and the Crown.

Intrusion Upon Seclusion- the Vendors

83. The vendors invaded the privacy of their own customers by deliberately leaving "the door open" for criminals to access its databases and steal class member personal information. For years before the hack took place the vendors knew at the highest levels of management that its data security practices and retention practices were not in compliance with PIPEDA and were either nonexistent or fell well below industry standards but made a conscious decision to do nothing about it.

84. In the alternative, the vendors were recklessly indifferent to the consequences of their wholly inadequate security standards and unlawful retention practices. They knew their security and retention practices did not comply with PIPEDA and were contrary to their own privacy policies. The vendors knew their practices were unlawful and placed the class members at a material risk of having their personal information stolen by criminals, yet intentionally decided to do nothing about it.

85. The Crown is vicariously liable for the vendors intrusion.

Statutory Actions for Breach of Privacy – the Hacker

86. The plaintiff pleads and relies on the following statutory claims on behalf of the class members who are domiciled in, or are residents of the Provinces of British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador (collectively, the Statutory Privacy Act Claims).

British Columbia class members

87. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of British Columbia, that the Hacker violated section 1 of the Privacy Act, RSBC 1996, c. 373, as amended.

88. The Hacker without a claim of right willfully violated the privacy of the British Columbia class members when they accessed class members' personal information without class members' consent.

Manitoba class members

89. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Manitoba that the Hacker violated sections 2 of the Privacy Act, CCSM c. P125, as amended.

90. The Hacker substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba class members when they accessed class members' personal information without class members' consent.

91. As a result of this breach the Manitoba class members are entitled to rely upon section 4 of the Privacy Act, CCSM c. P125, as amended.

Saskatchewan class members

92. The plaintiff plead on behalf of all class members who are domiciled or are residents of the Province of Saskatchewan, that the Hacker violated section 2 of the Privacy Act, RSS 1978, c. P-24, as amended 1996.

93. The Hacker without a claim of right willfully violated the privacy of the Saskatchewan class members when they accessed class members personal information without class members' consent.

Newfoundland and Labrador class members

94. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Newfoundland and Labrador, that the Hacker violated section 3 of the Privacy Act, RSNL 1990, c. P-22, as amended.

95. The Hacker without a claim of right willfully violated the privacy of the Newfoundland and Labrador class members when they accessed class members personal information without class members' consent.

Statutory Privacy Act Claims – the Vendors

British Columbia class members

96. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of British Columbia, that the vendors violated section 1 of the Privacy Act, RSBC 1996, c. 373, as amended.

97. The vendors without a claim of right willfully violated the privacy of the British Columbia class members and class members residing in other provinces when they retained class members' personal information in perpetuity without class members' consent, and contrary to their duties to class members.

98. In addition, the vendors invaded the privacy of their own customers by deliberately leaving "the door open" for criminals to access and steal class member personal information. The vendors knew at the highest levels of management that their data security and retention practices were not in compliance with PIPEDA and were either nonexistent or fell well below industry standards but made a conscious decision to violate PIPEDA and to do nothing about it.

99. In the alternative, the vendors were recklessly indifferent to the consequences of their wholly inadequate security and unlawful retention practices. They knew their security and retention practices did not comply with PIPEDA and were contrary to their own privacy policies. The vendors knew their security and retention practices were unlawful and placed the class members at a material risk of having their personal information stolen by criminals, yet intentionally decided to do nothing about it.

100. The Crown is vicariously liable for the vendors' breach of privacy.

Manitoba class members

101. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Manitoba that the Defendants violated sections 2 of the Privacy Act, CCSM c. P125, as amended.

102. The vendors substantially, unreasonably, and without a claim of right violated the privacy of the Manitoba class members for the reasons set out above at paragraphs 97 to 99.

103. As a result of this breach the Manitoba class members are entitled to rely upon section 4 of the Privacy Act, CCSM c. P125, as amended.

104. The Crown is vicariously liable for the vendors' breach of privacy.

Saskatchewan class members

105. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Saskatchewan, that Capital One violated section 2 of the Privacy Act, RSS 1978, c. P-24, as amended 1996

106. The vendors without a claim of right willfully violated the privacy of the Saskatchewan class members for the reasons set out above at paragraphs 97 to 99 .

107. The Crown is vicariously liable for the vendors' breach of privacy.

Newfoundland and Labrador class members

108. The plaintiff pleads on behalf of all class members who are domiciled or are residents of the Province of Newfoundland and Labrador, that Capital One violated section 3 of the Privacy Act, RSNL 1990, c. P-22, as amended.

109. The vendors without a claim of right willfully violated the privacy of the Newfoundland and Labrador class members for the reasons set out above at paragraphs 97 to 99.

110. The Crown is vicariously liable for the vendors' breach of privacy.

Breach of the Québec Civil Code

111. With regard to the class members resident in Québec, the defendants breached arts. 35, 36 and/or 37 of the CCQ by failing to maintain adequate protections to safeguard class members' personal information from unauthorized use or loss and by failing to protect the

personal information, contrary to Division I, s. 3.1 of the *Act respecting the protection of personal information in the private sector*, CQLR c. P-39.1 (the "*PSA*");they retained it longer than necessary, contrary to Division III, s. 10 of the *PSA*; and they failed to destroy it, in accordance with Division III, s. 23 of the *PSA*.

112. As a result of the breaches of the CCQ, the class members resident in Québec are entitled to moral and material damages pursuant to arts. 1457 and 1463-64 of the CCQ.

113. In addition, class members resident in Québec are entitled to punitive damages pursuant to Article 49 of the Charter of Human Rights and Freedoms.

Damages

114. As a result of the defendants' wrongdoing, the class members suffered damages including, but not limited to:

a) damages to credit reputation;

b) mental distress that is serious and prolonged;

c) fear, apprehension, anxiety, risk, anger, anguish and humiliation in relation to the unauthorized or unknown future use of their personal information;

d) costs incurred in preventing or rectifying identity theft or fraud;

e) out-of-pocket expenses;

f) wasted time, inconvenience, frustration and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft, fraud or improper use of credit information;

g) time lost from employment engaging in precautionary communications with third parties such as credit card companies, credit agencies, banked and other parties and to inform said third parties of the potential that the class members'

personal information may be misappropriated and to resolve any delays thereby caused;

h) nominal damages for breach of contract; and

i) Costs of purchasing credit monitoring and identity theft insurance.

115. Class members had their sensitive personal information stolen which constitutes an injury to their person and property damage.

116. In addition, class members have suffered or will likely suffer further damages from identity theft and/or fraud in the event that the personal information was, and remains, publicly available on the internet and may be downloaded and used for criminal purposes. It is likely or, alternatively, there is a real and substantial risk and danger that in the future the personal information will continue to be available for sale on the internet and be used for criminal purposes such as to create fictitious bank accounts, obtain loans, secure credit cards or to engage in other forms of identity theft and/or fraud, thereby causing the class members to suffer damages.

Intrusion/Statutory Privacy Torts /Breach of Confidence Damages

117. Class members claim damages for the violation of their informational privacy, suffering, distress, humiliation, anguish, reduced trust, feelings of lost privacy, ongoing increased levels of stress that they experienced from the intrusion, breaches of the statutory privacy acts and pecuniary damages.

118. Class members sustained a detriment as a result of the non-permitted use of their personal information and breach of their informational privacy caused by the vendor defendants' non-permitted acts, including emotional distress, anguish, humiliation and/or pecuniary damages.

Injunctive Relief

119. Class members whose vendor relocation services have been completed continue to have their personal information unlawfully retained by the vendors. Class members continue to be at risk of further cyber-attacks for so long as the vendors continue to unlawfully retain their personal information.

120. Therefore, the class seeks interim orders restraining the vendors from continuing to retain the personal information on its servers and a preservation order.

121. A preservation order is sought requiring the vendors (at their own expense) to supply all personal information of the proposed class members to a court approved data security management company who will prepare a preservation plan for court approval, pending the outcome of the litigation. Once the litigation is concluded the plaintiff seeks a final order permanently destroying the personal information.

GENERAL

122. The Plaintiff proposes that this action be tried at Toronto, Ontario.

Date: February 14, 2024

CHARNEY LAWYERS PC
151 Bloor Street West, Suite 602
Toronto, ON M5S 1S4

Theodore P. Charney/LSO #26853E
Caleb Edwards/LSO #65132P

Tel. No. (416) 964-3408
Fax No. (416) 929-8179