Court File No: T-982-20

FEDERAL COURT

PROPOSED CLASS PROCEEDING

BETWEEN:

TODD SWEET ~~ANNE CAMPEAU, ALLY STANLEY AND SYDNEY STANLEY~~

Plaintiff~~s~~

and

HER MAJESTY THE QUEEN

Defendant

Brought pursuant to the *Federal Courts Rules*, SOR/98-106

THIRD FURTHER AMENDED STATEMENT OF CLAIM

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiffs. 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 defense in Form 171B prescribed by the Federal Courts Rules, serve it on the plaintiffs' solicitor or, where the plaintiffs do not have a solicitor, serve it on the plaintiffs, 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 defense is forty days. If you are served outside Canada and the United States of America, the period for serving and filing your statement of defense is sixty days.

Copies of the Federal Courts 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.

(Date)

Issued by:_____
(Registry Officer)
Address of local office

Pacific Centre
PO Box 10065
701 West Georgia Street
Vancouver, BC V7Y 1B67

TO: Her Majesty the Queen
Department of Justice
900 – 840 Howe Street
Vancouver, BC
V6Z 2S9

Relief Sought

1. The plaintiff~~s~~, Todd Sweet, ~~Anne Campeau, Ally Stanley and Sydney Stanley,~~ claim~~s~~ on ~~their her~~ his own behalf and on behalf of the proposed Class (as defined below):

a. an order certifying this action as a class proceeding and appointing Todd Sweet ~~Anne Campeau, Ally Stanley and Sydney Stanley~~ as representative plaintiff~~s~~ for the Class;

b. an ~~interim~~ order that the defendant fund appropriate credit monitoring services for the plaintiff~~s~~ and all Class Members;

c. general damages for the defendant's several liability plus damages equal to the costs of administering the plan of distribution;

d. damages for the ~~D~~defendant's several liability for time lost while communicating with the Canada Revenue Agency, Service Canada and other government agencies and while in engaging in precautionary communications with third parties to inform them about the unauthorized disclosure of the plaintiff's~~'~~ and other Class Members' personal and financial information;

e. special damages for the defendant's several liability in an amount to be determined, including but not limited to ~~CERB and CESB~~ Canada Emergency Response Benefits, Canada Emergency Student Benefits, and other benefits owed, costs incurred in preventing identity theft, including costs incurred for the purpose of credit monitoring, and other out-of-pocket expenses~~, and time lost in precautionary communications with third parties to inform them of the potential misappropriation of the plaintiffs' and other Class Members' credit information~~;

f. punitive damages;

g. pre- and post-judgement interest;

h. costs; and

i. such further and other relief as this Honourable Court deems just.

Nature of the Action

2. This action concerns the unauthorized disclosure to a third party of the personal and financial information of thousands of Canadians from their online accounts with ~~the Government of Canada Branded Credential Service ("GCKey"), and~~ the Canada Revenue Agency ("CRA"), ~~and~~ My Service Canada, ~~.~~ and other Government of Canada online accounts where those accounts are accessed using the Government of Canada Branded Credential Service ("GCKey").

3. The information was disclosed to a third party during several ~~cyber security incidents~~ unauthorized data breaches targeting the GCKey credential management service and targeting ~~and~~ CRA accounts~~,~~ and My Service Canada accounts - and the personal and financial information included in those accounts. The defendant was aware of cyber security concerns with these accounts and with GCKey and with its databases and online systems generally, and was aware of vulnerabilities in its security software, ~~both~~ all of which put at risk the personal and financial information of the plaintiff~~s~~ and other Class Members. ~~contained in Class Members' GCKey and CRA accounts.~~ Despite these concerns and vulnerabilities, the defendant failed to take timely and reasonable steps and precautions to prevent harm to the plaintiff~~s~~ and other Class Members.

4. The defendant's own cyber security guidance acknowledges that the burden of password protection falls on the system, not the user. The defendant should have followed its own cyber security guidance regarding passwords. The defendant also should have offered a non-vulnerable security question mechanism for users of online ~~GCKey,~~ CRA accounts~~,~~ and My Service Canada accounts and the GCKey credential management system and should have responded in a reasonable and timely manner to significant increases in failed login attempts to these accounts and to the GCKey credential management system. And the defendant should have followed industry norms regarding two-factor authentication for these accounts.

5. As a result of the ~~these cyber security incidents~~ unauthorized data breaches, the personal and financial information of the plaintiff~~s~~ and other Class Members - including their social insurance numbers ("SIN"), annual tax returns, notices of assessment, banking records and

account information, financial records and salary information, T4s, T5s, family information, disability benefit information, immigration status, ~~and~~ home addresses, and other inherently revealing and private information - was disclosed to a third party without their consent.

6. The plaintiff~~s~~ and other Class Members have had their privacy deeply invaded, and are distressed and fearful of the uses that may be made of their confidential personal and financial information by the third party. The plaintiff~~s~~ and other Class Members have already spent ~~considerable time~~ numerous hours notifying the CRA, Service Canada, credit bureaus, banks, and other appropriate companies and agencies about the issue and will require credit monitoring services for the rest of their lives. Many Class Members have also suffered other damages including, *inter alia*: identity theft; monies being withdrawn from their bank accounts without their consent; loans being applied for (and taken out) in their names without their consent; Canada Emergency Response Benefits ("CERB"), Canada Emergency Student Benefits ("CESB"), Employment Insurance payments, Canada Child Benefits, Canada Pension Plan payments, and other benefits being redirected to bank accounts or addresses that do not belong to Class Members and losses that flow directly from Class Members not having access to these monies.

The Parties

7. The plaintiff, Todd Sweet, is a retired police officer. He is a resident of Clinton, British Columbia, with an address for service c/o Rice Harbut Elliott LLP, 820 – 980 Howe Street, Vancouver, British Columbia, V6Z 0C81.

~~8. The plaintiff, Anne Campeau, is a police dispatcher with the city of Windsor. She is a resident of South Woodslee, Ontario, with an address for service c/o Murphy Battista LLP, 2020 – 650 West Georgia Street, Vancouver, British Columbia, V6B 4N7.~~

~~9. The plaintiff, Ally Stanley, is a full-time student attending Queens University and currently residing in Vancouver, British Columbia, with an address for service c/o Murphy Battista LLP, 2020 – 650 West Georgia Street, Vancouver, British Columbia, V6B 4N7.~~

~~10. The plaintiff, Sydney Stanley, is a full-time student attending Queens University and currently residing in Vancouver, British Columbia, with an address for service c/o Murphy~~

~~Battista LLP, 2020 – 650 West Georgia Street, Vancouver, British Columbia, V6B 4N7.~~

11. The defendant, Her Majesty the Queen (the "Crown"), is named as a representative of the Federal Government of Canada and is liable for the conduct, negligence and malfeasance of the ~~Canadian Revenue Agency ("CRA")~~ CRA, Service Canada, Employment and Social Development Canada, and other individuals and agencies who were at all material times Crown employees, agents and servants, pursuant to the *Crown Liability and Proceedings Act*, RSC 1985, c. C-50.

12. The Class is defined as:

> All persons whose personal or financial information in their Government of Canada Online Account was disclosed to a third party on or after March 1, 2020, excluding Excluded Persons.
>
> "Government of Canada Online Account" means:
>
> a. a Canada Revenue Agency account;
> b. a My Service Canada account; or
> c. another Government of Canada online account, where that account is accessed using the Government of Canada Branded Credential Service (GCKey).
>
> "Excluded Persons" means all persons who contacted Murphy Battista LLP about the CRA privacy breach class action, with Federal Court file number T-982-20, prior to June 24, 2021.
>
> (collectively "Class" or "Class Members").

~~All persons whose personal or financial information in their Government of Canada Branded Credential Service (GCKey) account or their Canada Revenue Agency account or their My Service Canada account was disclosed to a third party on or after March 15, 2020 March 1, 2020 ("Class" or~~ "Class Members" ~~to be further defined on the plaintiffs' application for certification~~).

Background

13. On or around March 15, 2020, the defendant began providing eligible employed and self-employed Canadians directly affected by COVID-19 with ~~the Canadian Emergency Response Benefit ("CERB")~~ CERB, a benefit that provided financial support to eligible applicants in the amount of $2,000 ~~a month~~ for a four week period.

14. On or around May 10, 2020, the defendant began providing eligible Canadian post-secondary students, and recent post-secondary and high school graduates who were unable to find work due to COVID-19, with ~~the Canadian Emergency Student Benefit ("CESB")~~ CESB, a benefit that provided financial support to eligible applicants in the amount of $1,250-$2,000 ~~a month~~ for a four week period.

15. With both the CERB and CESB programs, if a person required benefits beyond the initial four week period, they were required to re-apply for the CERB or CESB program.

16. The ~~cyber security incidents~~ timing of the first unauthorized data breach correlated to the Crown's introduction of the CERB program in or around early March 2020 and the unauthorized data breaches continued throughout the period that the CERB and CESB programs were being offered by the defendant and even after these programs ended. ~~were related to the online application for the CERB and CESB financial support payments.~~

17. The plaintiff~~s~~ and Class Members used unique usernames and passwords for their CRA, Service Canada, and GCKey accounts; they did not use usernames or passwords for these accounts that they used to log in to other online accounts in their names.

18. The online application system for the CERB and CESB programs was implemented hastily and recklessly by the defendant and without taking the necessary precautions to ensure that the plaintiff's~~'~~ and Class Members' inherently private personal and financial information ~~of the Class~~ included in their CRA accounts, My Service accounts, and other Government of Canada online account, where those accounts are accessed using the GCKey credential management system, ~~accounts~~ was not compromised.

19. The defendant knew, or ought to have known, that ~~their online application system for CERB and CESB was~~ its databases and online systems and the plaintiff's~~'~~ and Class Members' CRA accounts, Service Canada accounts, and other online Government of Canada accounts

accessed using the GCKey credential management system ~~accounts~~ were vulnerable to ~~cyber security incidents~~ unauthorized data breaches, and the defendant failed to take timely, reasonable and adequate measures to protect the plaintiff's~~,~~ and Class Members' personal and financial information ~~of the Class~~ both before and after launching the online CERB and CESB programs. The defendant should have followed its own cyber security guidance regarding passwords, should have offered a non-vulnerable security question mechanism for users of ~~GCKey,~~ CRA~~,~~ and My Service Canada accounts and the GCKey credential management system, and should have followed industry norms regarding two-factor authentication for these accounts.

20. All of the defendant's duties *vis-à-vis* the plaintiff~~s~~ and other Class Members were non-delegable.

21. As a consequence of the defendant's conduct, the ~~The~~ personal and financial information of the plaintiff~~s~~ and other Class Members was disclosed to a third party following a series of ~~three or more~~ ~~cyber security incidents~~ unauthorized data breaches between ~~March 15, 2020~~ approximately March 1, 2020 and at least the fall or winter of 2020 and may be ongoing into 2021 and beyond ~~and August 17, 2020 (when the defendant suspended its online services), and may also have been disclosed to a third party during further cyber security incidents on later dates~~.

22. The CRA was aware that there was an increase in fraudulent activity at the beginning of each monthly CERB and CESB pay period and generally during the time period at issue but did nothing to notify or warn the plaintiff~~s~~ or other Class Members of same in a timely manner or at all, and did nothing to reasonably prevent ~~the activity~~ further unauthorized data breaches from ~~continuing to occur~~ occurring. Some Class Members have still not been notified by the defendant, or any employees, agents, or servants of the defendant, that their accounts were affected by the unauthorized data breaches and that their confidential information was compromised.

23. The CRA disclosed to CBC News, days prior to publicly announcing the unauthorized data breaches, that the ~~agency~~ CRA was aware that there was an uptick in fraudulent activity at the beginning of each monthly CERB pay period ~~to CTV News days prior to publically announcing the cyber security incidents~~.

24. As a result of the ~~cyber security incidents~~ unauthorized data breaches, the ~~GCKey~~ online Government of Canada accounts of thousands of Class Members – accessed using the GCKey credential management system – were compromised. Used by approximately 30 federal departments, GCKey allows Class Members to access services such as Employment and Social Development Canada's My Service Canada Account or their Immigration, Refugees and Citizenship Canada account. These accounts contain detailed personal and financial information,~~.~~ ~~Class Members' My Service Canada GCKey A accounts include~~ including personal and financial details related to Employment Insurance, immigration status, Canada Pension Plan, Canada Pension Plan Disability, and Old Age Security. The defendant is aware that the ~~GCKey~~ Government of Canada accounts ~~the passwords and usernames~~ of at least ~~9,041~~ 9,300 GCKey service users were accessed and the personal and financial information included in them disclosed to an external third party. The plaintiff~~s~~ and other Class Members did not provide their consent to ~~such~~ the disclosure of their personal and financial information.

25. The My Service Canada accounts of thousands of Class Members were compromised by the unauthorized data breaches, during which the personal and financial information of ~~the plaintiffs and other~~ Class Members was disclosed to an external third party. The ~~plaintiffs and other~~ Class Members did not provide their consent to such disclosure. My Service Canada accounts contain sensitive personal and financial information of Class Members, including information on Employment Insurance, Canada Pension Plan payments, Canada Pension Plan Disability payments, and Old Age Security payments. My Service Canada accounts also contain an e-link, which enables a user to link directly from their My Service Canada account to their CRA account without the need to sign in to their CRA account directly.

26. The CRA accounts of thousands of Class Members were also compromised by the ~~cyber security incidents~~ unauthorized data breaches, ~~disclosing~~ during which the personal and financial information of the plaintiff~~s~~ and other Class Members was disclosed to an external third party. The plaintiff~~s~~ and other Class Members did not provide their consent to such disclosure. CRA accounts contain sensitive personal and financial information of Class Members, including financial records, notices of assessments, banking information, and information on income, disabilities, children, relationship status, and investments. The defendant is aware ~~that the personal and financial information contained in at least 5,500 CRA accounts was disclosed to an~~

~~external third party~~ of at least 48,500 CRA accounts having been compromised during the data breaches.

~~27. Contracts existed between the defendant and Class Members. When the plaintiffs and other Class Members registered for and logged in to their CRA, My Service Canada, and GCKey accounts, they agreed – for good and valuable consideration – to allow the defendant to collect and retain their personal and financial information. The defendant correspondingly agreed – for good and valuable consideration – that it would, *inter alia*:~~

- ~~a. use web analytics tools to mark the electronic device used to visit the defendant's websites to ensure the safety and security of the information contained in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members;~~
- ~~b. ensure the personal privacy of website visitors and the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts;~~
- ~~c. have in place appropriate security safeguards and software to protect the personal and financial information of the plaintiffs and other Class Members;~~
- ~~d. regularly review and update its cyber security measures and requirements to ensure they were reasonable and complied with industry standards;~~
- ~~e. be accountable for protecting and safeguarding the personal and financial information of the plaintiffs and other Class Members that it collects and uses;~~
- ~~f. safely store and protect and keep confidential the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts in accordance with the *Privacy Act*, RSC 1985, c P-21 and otherwise;~~
- ~~g. not disclose the personal and financial information included in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members to a third party without their consent; and~~
- ~~h. not subject the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts to unauthorized disclosure to a third party.~~

~~28. The defendant breached these contractual terms by, among other things, disclosing the personal and financial information included in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members to a third party without their consent and by failing to safely retain, store, protect, and keep private the personal and financial information of the plaintiffs and other Class Members.~~

29. The defendant has admitted that its security software was susceptible and vulnerable to ~~cyber security incidents~~ the unauthorized data breaches and that it knew about ~~the CRA's security vulnerability~~ vulnerabilities to the plaintiff's~~.~~ and other Class Members' online accounts prior to the data breaches taking place.

30. Annette Butikofer, the chief information officer at the CRA, said during a news conference on August 17, 2020 that it was a "vulnerability in security software, which allowed [the third party] to bypass security questions and gain access" to Class Members' accounts.

31. Also on August 17, 2020, Marc Brouillard, the acting Chief Technology Officer for the Crown said that the third party was "also able to exploit a vulnerability in the configuration of security software solutions, which allowed them to bypass the CRA security questions and gain access to a user's CRA account".

32. Some Class Members alerted the CRA to the ~~cyber security incidents~~ unauthorized data breaches and security vulnerabilities as early as March of 2020, yet the CRA failed to take timely and reasonable steps to prevent further harm to the plaintiff~~s~~ and other Class Members.

33. As early as April 2020, some Class Members were notified by their service providers - such as accounting firms or investment firms - about the ~~cyber security incidents~~ unauthorized data breaches and their potential ramifications. Some of these service providers alerted the CRA ~~to~~ about the ~~cyber security incidents~~ unauthorized data breaches and security vulnerabilities, yet the CRA failed to take timely and reasonable steps to prevent further harm to the plaintiff~~s~~ and other Class Members.

34. The defendant failed to have in place a mechanism for reasonably and effectively managing and addressing reports of unauthorized data breaches of the CRA~~, GCKey,~~

Employment and Social Development Canada, and My Service Canada, and other Government of Canada departments and agencies. Reports of unauthorized data breaches were routinely and recklessly ignored by the defendant.

35. The CRA failed to notify the Privacy Commissioner of Canada, in a timely manner, that the personal and financial information of the plaintiff~~s~~ and other Class Members had been compromised and was at risk of being further compromised.

36. The CRA failed to notify the plaintiff~~s~~, other Class Members, and the Canadian public, in a timely manner or at all, that the personal and financial information of the plaintiff~~s~~ and other Class Members had been compromised and was at risk of being further compromised. No such disclosure was made public until on or around August 15, 2020. Even then, the defendant failed to lock the GCKey, ~~and~~ CRA, and My Service Canada online account systems to prevent further harm to the plaintiff~~s~~ and other Class Members.

37. After announcing the ~~cyber security incidents~~ unauthorized data breaches on or around August 15, 2020, an additional ~~cyber security incident~~ unauthorized data breach or breaches took place, further compromising the personal and financial information of the plaintiff and other Class Members. It was then that the defendant finally locked the GCKey credential management system and the~~,~~ ~~and~~ CRA, and My Service Canada ~~GCKey~~ online account systems.

38. To date, the defendant has been unable to determine who is in possession of the personal and financial information of the plaintiff~~s~~ and other Class Members.

39. To date, the defendant has been unable to provide the plaintiff~~s~~ and other Class Members with any details regarding their identity theft and how ~~the~~ their inherently revealing and private personal and financial information ~~of the Class~~ has been accessed, disseminated, copied, published, shared, or used, by whom, and for what purpose.

40. The defendant's unauthorized disclosure to a third party of the confidential personal and financial information of the plaintiff~~s~~ and other Class Members (which was communicated to Canada in confidence for the purpose of being included in Class Members' CRA accounts, My Service Canada accounts, and other Government of Canada online accounts that were accessed using the GCKey credential management system ~~accounts~~), was intentional and reckless and

without lawful justification. The information was misused by Canada, to the detriment of the plaintiffs and other Class Members. And its unauthorized disclosure by the defendant to a third party invaded the private affairs and concerns of the plaintiffs and other Class Members. The information disclosed was inherently revealing and private, and its disclosure was offensive and caused distress, humiliation, and anguish to the plaintiffs and other Class Members.

~~41. The plaintiffs and other Class Members had the right to personal security and the right to non-disclosure of their confidential information, and the defendant intentionally and unlawfully interfered with these rights and freedoms.~~

42. As a result of the unauthorized data breaches, the plaintiffs and other Class Members have spent numerous hours notifying the CRA, Service Canada, credit bureaus, and other appropriate companies and agencies about the issue and will indefinitely require credit monitoring services.

43. As a result of the unauthorized data breaches, the plaintiffs and other Class Members have had their privacy deeply invaded, and are mentally distressed about and fearful of the uses that may be made of their personal and financial information by a third party.

44. As a result of the unauthorized data breaches, the disclosed personal and financial information of Class Members has already been used by a third party or parties to, *inter alia*:

a. steal the identity of Class Members;
b. fraudulently apply for CERB, CESB, and other government benefits in the name of Class Members;
c. fraudulently redirect CERB, CESB, Employment Insurance payments, Canada Pension Plan payments and other government benefits away from Class Members;
d. fraudulently gain access to Class Members' bank accounts to withdraw money;
e. fraudulently gain access to Class Members' credit cards to make purchases;
f. fraudulently apply for loans in the names of Class Members; and
g. damage the credit reputation of Class Members.

45. The defendant has advised some Class Members that they would pay for credit monitoring, but this "credit monitoring" solely involves flagging the credit accounts of Class

Members, a service that is already offered free of charge by credit monitors in Canada.

46. The plaintiff~~s~~ and Class Members seek, *inter alia*, general damages for the defendant's several liability, special damages, and punitive damages.

47. ~~To date - as a result of the cyber security incidents - some Class Members have been unable to access the CERB and CESB financial support to which they are entitled, and they have experienced financial strain as a result~~.

The Plaintiff~~s and the Class~~

48. The plaintiff, Todd Sweet, was assigned a SIN at a young age and has filed income tax returns for decades. He never applied for or received CERB.

49. On each of June 29 and June 30, 2020, the plaintiff received an email from the CRA which stated that his email address had been removed from his CRA account. After receiving each email, the plaintiff logged into his CRA online account to re-register his email address.

50. On July 2, 2020, the plaintiff discovered that four CERB applications had been made in his name and that his direct deposit banking information had been changed. His account also showed that his level two representative access had been changed. The plaintiff had not made or authorized any of these changes to his CRA account. The plaintiff immediately put a stop on his direct deposit information and shut down the level two representative access. He then contacted the RCMP, called the CRA Fraud Center and left a message, and changed the passwords for his other online accounts.

51. Later on July 2, 2020, the plaintiff called the CRA and advised the agent that he had not applied for CERB. He requested that the CRA lock down his account. He also contacted Transunion and Equifax about the breach, so that his credit accounts could be flagged.

52. On September 24, 2020, the plaintiff received a letter from the Government of Canada informing him that his personal information had been compromised in the CRA data breach.

53. On October 26, 2020, the plaintiff received a letter from the CRA asking him to verify that he did not receive the CERB payments that had been made in his name. The plaintiff phoned the CRA to advise them – again – that he had not applied for CERB and had not received the CERB payments that had been made in his name, and that there had been fraudulent activity associated with his CRA account.

54. In or around November 2, 2020, the plaintiff received a letter from the CRA stating that they had received his request to adjust his 2019 income tax return. He had not made this request. The plaintiff sent a letter to the T1 adjustment section of the CRA, dated November 11, 2020, explaining that he had not made a request to change his 2019 taxes and that his CRA account had been subject to a breach.

55. On November 6, 2020 – at the request of the CRA – the plaintiff provided the CRA with the RCMP file number for his related claim, proof of his address, proof of his identification, and his direct deposit information.

56. In January of 2021, the plaintiff was finally able to reactive and access his CRA online account.

57. In October 2021, the plaintiff received a letter from the CRA indicating that he was being taxed for the $8000 in CERB payments that he had never applied for and had never received.

58. The plaintiff first contacted Murphy Battista LLP about this proposed class proceeding on November 4, 2021.

59. As a result of the breach to his CRA account and learning that the personal and financial information in his account had been compromised and disclosed to a bad actor without his consent, the plaintiff spent at least 20 hours gathering information, filling out forms, and contacting different agencies to deal with the account breach and to protect his identity and to prevent further harm.

60. The plaintiff is very concerned that his personal and financial information disclosed in the CRA breach will be used inappropriately in the future by bad actors, to his detriment. He has experienced significant anxiety and stress as a consequence of the breach of his CRA account.

61. The plaintiff, Anne Campeau, logged into her CRA account on August 10, 2020 and discovered that her email address and direct deposit information had been altered on August 6, 2020. In her account, she saw that someone had applied for two CERB payments using her SIN. Ms. Campeau was not eligible for CERB and had never applied for it. On August 11, 2020, she reported the matter to the Canadian Online Anti-Fraud Centre and to the CRA. As a result, the CRA froze her online account.

62. As a consequence of the cyber security incidents unauthorized data breaches, Ms. Campeau has suffered from anxiety and stress mental distress. She is concerned how her personal and financial information will be used by the third party. She is also deeply concerned about the potential ramifications to her credit, and will require credit monitoring services for the rest of her life.

63. The plaintiff, Sydney Stanley – a university student – tried to log into her online CRA account in May of 2020 in an attempt to apply for the CESB benefit; however, the system said that she was unable to apply for the benefit CESB. Ms. S. Stanley was confident that she qualified and called the CRA. She spent several hours on the phone and was transferred to different departments and different agents in an attempt to figure out what was happening with her account. Eventually, she was told that it would take approximately eight weeks for the CRA to determine what was happening with her account.

64. In June of 2020, Ms. S. Stanley learned that her account had been subject to a cyber security incident an unauthorized data breach, and that her personal and financial information had been compromised.

65. As a consequence of the cyber security incident unauthorized data breach, Ms. S. Stanley has spent countless numerous hours trying to protect her personal and financial information. She requires credit monitoring services for the rest of her life. She is anxious and mentally distressed about the likelihood of identity theft or other improper uses that may be made of her personal and financial information.

66. The plaintiff, Ally Stanley – a university student – tried to log into her online CRA account on Saturday, May 30, 2020 in an attempt to apply for the CESB benefit. When she

~~realized that something was wrong with her online account, she immediately called the CRA. She spent hours on the phone and was transferred between seven different agents before eventually being disconnected. On June 2, 2020, she again called the CRA and spent approximately five hours on the phone, again being transferred between departments and to nine different agents who tried to determine what was wrong with her account. None of the sixteen different CRA agents that she spoke to could assist her or sufficiently identify the problem with her CRA account.~~

~~67. On June 3, 2020, Ms. A. Stanley was provided with the direct number of a CRA agent from an investment firm. She called that agent and learned that her account had been subject to a cyber security incident~~ an unauthorized data breach ~~and that her personal and financial information had been compromised. It was also disclosed to her during that phone call that her SIN number had likely been retrieved by the third party. She was advised that her CRA account would be locked, likely on a permanent basis.~~

~~68. As a consequence of the cyber security incident~~ unauthorized data breach~~, Ms. A. Stanley has spent numerous hours trying to protect her personal and financial information. She will require credit monitoring services for life. She is anxious and stressed~~ mentally distressed ~~about the idea that an unknown person has access to her most private information, including her SIN, with no idea who has the information and what they are doing with it~~ and is fearful of what this unknown person will do with this information.~~

The Law

Systemic Negligence

69. The defendant owed a common law duty to the plaintiff~~s~~ and other Class Members to use reasonable care in the collection, storage, and retention, ~~and disclosure~~ of their personal and financial information and a duty to ensure that this personal and financial information was safe, kept private, and protected and that it would not be subject to unauthorized disclosure to a third party. The defendant's duties were not delegable.

70. Pursuant to section 8(1) of the *Privacy Act*, RSC 1985, c P-21, personal information under the control of the defendant cannot, without the consent of the individual to whom the

information relates, be disclosed by the defendant. The defendant's breach of the *Privacy Act* is evidence that its conduct fell below the applicable standard of care.

71. Particulars of the ~~The~~ defendant's systemic~~ally~~ breaches ~~ed its~~ of duty, as set out in the whole of this claim, include: ~~in the following way:~~

a. failing to create or adhere to policies for the collection, storage, retention, and disclosure of ~~the~~ personal and financial information prior to instituting the CERB and CESB programs;

b. failing to adhere to its own policies to ensure protection of the plaintiff~~s~~ and other Class Members in the collection, retention and disclosure of ~~the~~ their personal and financial information;

c. failing to take reasonable steps to ensure that the personal and financial information of the plaintiff~~s~~ and other Class Members was kept safe, private, and protected was not retrieved, disseminated, or disclosed without the consent of the plaintiff~~s~~ and other Class Members;

d. disclosing to a third party the personal and financial information of the plaintiff~~s~~ and other Class Members without their consent;

e. failing to follow its own cyber security guidance regarding passwords;

f. failing to have offered a non-vulnerable security question mechanism for users of the GCKey credential management system and for users of ~~with~~ CRA~~,~~ and My Service Canada online accounts;

g. failing to have followed industry norms regarding two-factor authentication for these accounts;

h. failing to take reasonable steps, including freezing the online systems, when there was a significant increase in the number of failed attempts for CRA accounts, My Service Canada accounts, and/or the GCKey credential management system;

i. failing to take reasonable steps, including freezing the online systems, when they knew or ought to have known that ~~cyber security incidents~~ unauthorized data breaches were compromising the personal and financial information of the plaintiff~~s~~ and other Class Members ~~were taking place~~;

j. failing to act on reported concerns ~~regarding compromised security~~ communicated by the plaintiff~~s~~ and other Class Members about the unauthorized data breaches in a timely manner or at all;

k. failing to act on reported concerns communicated by financial institutions, accounting firms, or other institutions about the unauthorized data breaches in a timely manner or at all;

l. failing to take timely and reasonable steps that were required to ensure the integrity and security of its databases and online systems and to prevent unauthorized access to the personal and financial information of the plaintiff~~s~~ and other Class Members;

m. failing to take timely and reasonable steps to ensure the application process for CERB and CESB programs did not compromise the security, safety, or privacy of the plaintiff's~~'~~ and other Class Members' personal and financial information;

n. failing to disclose the ~~loss of the information~~ unauthorized disclosure of the plaintiff's~~'~~ and other Class Members' personal and financial information to its own security personnel and to the plaintiff~~s~~ and other Class Members in a timely manner or at all;

o. failing to rectify the ~~vulnerability~~ vulnerabilities in the configuration of its security software in a timely manner or at all ~~that allowed the information of the plaintiffs and other Class Members to be compromised~~ when it knew or ought to have known about the ~~vulnerability~~ vulnerabilities;

p. failing to provide adequate or any instructions to the plaintiff~~s~~ and other Class Members on how to mitigate their damages, including failing to provide adequate

paid credit monitoring services to the plaintiffs and other Class Members;

q. failing to disclose the pattern of cyber security incidents unauthorized data breaches and the loss of the information unauthorized disclosure of the personal and financial information of the plaintiffs and other Class Members occurring at the start of each CERB and CESB program monthly payment cycle or otherwise to the plaintiffs and other Class Members in a timely manner or at all; and

r. other particulars as counsel may advise.

72. Measures and steps finally taken by the defendant in the fall and winter of 2020 to protect its databases, systems, and the online CRA accounts, online My Service Canada accounts, and other Government of Canada online accounts – accessed using the GCKey credential management system – accounts of the plaintiffs and other Class Members are all measures and steps that should have been taken by the defendant prior to the unauthorized data breaches and, had they been taken, the unauthorized breaches in question would have been prevented.

73. The defendant's breaches of duty caused the plaintiffs and other Class Members harm and ongoing damages, including distress, anxiety, mental anguish, lost time, lost opportunities, and out of pocket expenses.

Breach of Privacy

74. The defendant had a statutory duty under subsection 8(1) of the *Privacy Act*, RSC, 1985, c P-21, not to disclose Class Members' personal and financial information without consent, and the defendant breached that duty to the plaintiffs and other Class Members, as set out above and in the whole of this claim.

75. The defendant failed to meet its statutory duties under the *Privacy Act* and *PIPEDA* in the collection, retention, and disclosure of the personal and financial information of the plaintiffs and other Class Members.

Breach of Confidence **and Intrusion upon Seclusion**

76. The personal and financial information of the plaintiffs and other Class Members, - which

was included in their CRA accounts, ~~GCKey and~~ their My Service accounts, and other Government of Canada online accounts accessed using the GCKey credential management system – was confidential and was communicated to the defendant in confidence. That information was misused by the defendant, to the detriment of the plaintiff~~s~~ and other Class Members, and constituted the tort of breach of confidence.

77. ~~The defendant's breach of privacy and the particulars of negligence set out above and in the whole of this claim, constitutes a breach of confidence, as the plaintiffs and other Class Members communicated their personal and financial information to the defendant, and the defendant misused that information to the detriment of the plaintiffs and other Class Members~~.

78. ~~The defendant's breach of privacy and the particulars of negligence set out above and in the whole of this claim constitute a breach of privacy and a reckless intrusion upon the seclusion of the plaintiffs and other Class Members in their private affairs, in a manner that would be highly offensive to a reasonable person.~~

Intrusion upon Seclusion

79. The defendant's unauthorized disclosure to a third party of the plaintiff's~~'~~ and other Class Members' personal and financial information was intentional and reckless and, without lawful justification, invaded the private affairs and concerns of the plaintiff~~s~~ and other Class Members. The information disclosed was inherently revealing and private, and a reasonable person would regard this invasion as highly offensive causing distress, humiliation, or anguish. The defendant's conduct constituted the tort of intrusion upon seclusion.

80. Class Members and their agents reported unauthorized data breaches of their ~~GCKey,~~ CRA accounts, ~~and~~ My Service Canada accounts, and other Government of Canada online accounts accessed using the GCKey credential management system, and their personal and financial information included in those accounts, to the defendant in the spring of 2020, and the defendant intentionally and recklessly and without lawful justification disregarded this information and failed to take reasonable and timely steps to protect the plaintiff~~s~~ and other Class Members from further unauthorized data breaches.

Crown Liability and Proceedings Act

The acts, omissions, torts, and faults of the defendant, as set out in detail in the whole of this claim, were also committed by servants of the Crown. Where the tort was committed by a servant of the Crown or where, in Quebec, damage was caused by the fault of a servant of the Crown, the Crown is liable for the damages for which, if it were a person, it would be liable, pursuant to section 3 of the *Crown Liability and Proceedings Act*, RSC 1985, c C-50.

Breach of Contract

81. The plaintiffs and other Class Members entered into contracts with the defendant when they registered for their CRA, My Service Canada, and GCKey accounts. Good and valuable consideration was given for these contracts and the parties were *ad idem* on the terms of the contracts. The contracts between the defendant and Class Members were all identical or substantially similar. And the performance of the contracts was ongoing.

82. The contracts provided peace of mind to the plaintiffs and other Class Members since, pursuant to the terms of the contracts, the defendant contracted and warranted that the personal and financial information included in Class Members' CRA, My Service Canada, and GCKey accounts would be kept private, safe, and secure and, in accordance with the defendant's statutory obligations under the *Privacy Act*, would not be disclosed to a third party without the consent of the plaintiffs and other Class Members.

83. Some of the terms of the contracts were contained in the defendant's Personal Information Collection Statement and its predecessor and subsequent versions.

84. Pursuant to the terms of the contracts, the defendant was required to:

a. use web analytics tools to mark the electronic device used to visit the defendant's websites to ensure the safety and security of the information contained in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members;
b. ensure the personal privacy of website visitors and the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts;
c. have in place appropriate security safeguards and software to protect the personal and financial information of the plaintiffs and other Class Members;

d. regularly review and update its cyber security measures and requirements to ensure they were reasonable and complied with industry standards;

e. be accountable for protecting and safeguarding the personal and financial information of the plaintiffs and other Class Members that it collects and uses;

f. safely store and protect and keep confidential the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts in accordance with the *Privacy Act*, RSC 1985, c P-21 and otherwise;

g. not disclose the personal and financial information included in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members to a third party without their consent; and

h. not subject the personal and financial information of the plaintiffs and other Class Members included in their CRA, My Service Canada, and GCKey accounts to unauthorized disclosure to a third party.

85. As set out in the whole of this claim, the defendant breached these contractual terms by disclosing the personal and financial information included in the CRA, My Service Canada, and GCKey accounts of the plaintiffs and other Class Members to a third party without their consent and by failing to safely store, retain, protect, and keep private the personal and financial information of the plaintiffs and other Class Members. The defendant further breached the contracts by failing to review and update its cyber security measures to comply with industry standards and by failing to have in place appropriate security safeguards and software to protect the personal and financial information of the plaintiffs and other Class Members.

86. The defendant's breaches were persistent and ongoing.

Québec Class Members

87. Where the acts and omissions of the defendant took place in Québec, they constituted fault giving rise to extra-contractual liability pursuant to the *Civil Code of Québec*, CQLR, c CCQ-1991, the *Crown Liability and Proceedings Act*, RSC 1985, c C-50 and the *Interpretation Act*, RSC 1985, c I-21 and any predecessor legislation. The conduct of the defendant also constituted unlawful and intentional interference with the rights of Québec Class Members

~~within the meaning of the *Charter of Human Rights and Freedoms*, CQLR c C-12 and any predecessor legislation.~~

~~88. Pursuant to section 1 of the *Charter of Human Rights and Freedoms*, every human being has the right to personal security and, pursuant to section 9, every person has the right to non-disclosure of confidential information.~~

~~89. The conduct of the defendant, as set out in the whole of this claim, constituted an unlawful interference with the rights and freedoms of Québec Class Members guaranteed by sections 1 and 9 of the *Charter of Human Rights and Freedoms*, CQLR c C-12 and entitle Quebec class members to obtain compensation for the moral or material prejudice resulting therefrom.~~

~~90. The conduct of the defendant, as set out in the whole of this claim, was also intentional interference with these rights and freedoms of Québec Class Members and condemn the defendant guilty of punitive damages.~~

~~91. The defendant is liable to pay damages, including punitive damages, to Québec Class Members pursuant to the *Civil Code of Québec*, CQLR, c CCQ-1991 and any predecessor legislation.~~

Damages

92. As a result of the defendant's negligence, breach of privacy, breach of confidence, ~~breach of contract,~~ and reckless intrusion upon seclusion, the plaintiff~~s~~ and other Class Members have suffered damages including:

a. costs incurred in preventing identity theft;

b. identity theft;

c. increased risk of future identity theft;

d. damage to credit reputation;

e. mental distress, ~~including~~ stress, ~~and~~ anxiety, humiliation, and anguish;

f. monies withdrawn from their bank accounts without their consent;

g. loans applied for in their names without their consent;

h. credit card fraud;

i. inability to access the benefit funds and payments they were entitled to and ~~the associated financial strain~~ financial and other losses flowing directly from their inability to access these benefits and payments;

j. the loss of employment insurance, Canada Pension Plan payments, Canada Child Benefits, and other benefits or payments they were entitled to that were redirected to bank accounts or addresses that do not belong to them, and other losses flowing directly from their inability to access these benefits and payments;

k. out-of-pocket expenses;

~~l. inconvenience, frustration and anxiety associated with taking precautionary steps to reduce the likelihood of identity theft or other improper use of their personal and financial information; and~~

m. time lost waiting on hold for and speaking with the CRA, Service Canada, Employment and Social Development Canada, and other Crown agencies, departments, servants, and individuals to address the unauthorized data breaches and to mitigate their damages; and

n. time lost in precautionary communications with third parties such as credit card companies, credit agencies, creditors, utility providers, and other parties, to inform them of the potential that their personal and financial information may have been compromised.

93. The plaintiff~~s~~ and Class Members seek, *inter alia*, general damages for the defendant's several liability and special damages.

94. As set out in detail in this claim, the actions of the defendant were reprehensible and

showed a callous disregard for the rights of the plaintiff~~s~~ and other Class Members. The conduct of the defendant was deliberate and represented a marked departure from ordinary standards of decent behavior, and as such merits punishment and warrants a claim for punitive damages.

Relevant Legislation

95. The plaintiff~~s~~ pleads and relies on ~~rely on~~ the following statutes:

~~a. *Charter of Human Rights and Freedoms*, CQLR c C-12;~~

~~b. *Civil Code of Québec*, CQLR, c CCQ-1991;~~

c. *Crown Liability and Proceedings Act*, RSC 1985, c C-50;

d. *Interpretation Act*, RSC 1985, c I-21;

e. *Privacy Act*, RSC 1985, c P-21; and

f. their predecessor and successor statutes.

General

96. The plaintiff~~s~~ propose~~s~~ that this action be tried at Vancouver, British Columbia.

Date: ~~August 24~~~~December 16, 2020~~
~~October 19, 2021~~
~~November 2, 2021~~
November 26, 2021

Lawyers for the Plaintiff~~s~~

Rice Harbut Elliott LLP
John M. Rice, Q.C.
Anthony Leoni
#820 – 980 Howe Street
Vancouver, B.C. V6Z 0C8
Telephone: (604) 682-3771
Fax: (604) 682-0587

Murphy Battista LLP
Angela Bespflug
Janelle O'Connor
#2020 – 650 West Georgia Street
Vancouver, B.C. V6B 4N7
Telephone: (604) 683-9621
Fax: (604) 683-5084