S-198696

NO.
VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

[redacted]

PLAINTIFF

AND:

CAPITAL ONE FINANCIAL CORPORATION and
CAPITAL ONE BANK (CANADA BRANCH)

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c.50

NOTICE OF CIVIL CLAIM

This action has been started by the plaintiff(s) for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

TIME FOR RESPONSE TO CIVIL CLAIM

A response to civil claim must be filed and served on the plaintiff(s),

(a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,

(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,

(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

CLAIM OF THE PLAINTIFF(S)

Part 1: STATEMENT OF FACTS

A. Introduction

1. This proposed class proceeding involves the failure of the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), to adequately safeguard, protect, store and/or maintain the personal and/or financial information including, *inter alia*, the names, addresses, phone numbers, dates of birth, credit scores, credit limits, account balances, payment histories, social insurance numbers and bank account numbers (collectively referred to herein to as "PII"), of the Plaintiff and proposed class members with respect to customer credit card applications and accounts with the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), which were accessed, compromised and/or stolen as a result of an unauthorized data breach by third parties.

2. The Defendant , CAPITAL ONE FINANCIAL CORPORATION, is a financial services holding company that offers a broad array of financial products and/or services including, *inter alia,* credit cards, automobile loans and banking products to consumers, small businesses and

commercial clients through branches , the internet and other distribution channels. It is one of the largest banks and issuers of Visa and MasterCard credit cards in North America.

3. In Canada the Defendant, CAPITAL ONE FINANCIAL CORPORATION, extends credit through its wholly owned subsidiary, the Defendant, CAPITAL ONE BANK (CANADA BRANCH). The most popular of the Defendant, CAPITAL ONE FINANCIAL CORPORATION's, financial products are those credit and/or debit cards issued to cardholders for use as customers of Costco, Hudson's Bay Company and Saks.

4. On July 29, 2019 the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), announced that on "July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information [i.e., PII] relating to people who had applied for its credit card products and to Capital One credit card customers". The United States of America Federal Bureau of Investigations related that an individual accessed the PII by exploiting one of the Defendants, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, misconfigured firewalls, which allowed the individual to access the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, cloud repository and exfiltrate the PII of approximately 100 million American and 6 million Canadian consumers in or around March 2019 (the "Data Breach").

5. The hacker posted the PII of these approximately 100 million American and 6 million Canadian consumers to her GitHub internet account on April 21, 2019 which was free and available for any user on the internet to download and further exploit.

6. In addition to the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, failure to prevent the Data Breach, they also failed to detect the breach for approximately three months. The posted PII of approximately 100 million American and 6 million Canadian consumers on the hacker's GitHub account remained exposed until at least July 17, 2019, when an unidentified tipster informed the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), of the posting by emailing the bank's responsible disclosure address with a brief warning and a link to the GitHub internet address.

7. The Data Breach was the result of the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, inadequate approach to data security and protection of PII that they collected during the course of their business. The deficiencies in the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, data security were so significant that the misconfigured firewall permitted access to any consumer or small business that applied for one of their credit card products from 2005 through early 2019--approximately 14 years of data left unprotected and exposed for any malicious actor to access, download and exploit.

8. The Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), disregarded the rights of Plaintiff and proposed class members by:

(a) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure their computer data systems were protected;

(b) failing to disclose to their customers the material fact that they did not have adequate computer data systems and security practices to safeguard customer PII;

(c) failing to take available steps to detect and prevent the Data Breach; and

(d) failing to monitor and timely detect the Data Breach; and

(e) failing to provide the Plaintiff and proposed class members prompt and accurate notice of the Data Breach.

9. As a result of the Data Breach, the Plaintiff and proposed class members' PII have been exposed to unauthorized third parties or malicious actors for misuse. The injuries Plaintiff and proposed class members suffered as a direct result of the Data Breach include:

(a) theft of personal and financial information;

(b) costs associated with the detection and prevention of identity theft and unauthorized

use of financial accounts;

(c) damages arising from the inability to use debit and/or credit card accounts because such accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach including, but not limited to, foregoing cash back rewards;

(d) damages arising from the inability to withdraw or otherwise access funds because such accounts were suspended, restricted and/or otherwise rendered unusable as a result of the Data Breach including, but not limited to, missed bill and loan payments, late-payment charges, lowered credit scores and/or other adverse impacts on credit;

(e) costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts including, but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

(f) the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by the PII being exposed for theft and sale on the "Dark Web";

(g) damages to and diminution in value of the PII entrusted to the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), for the sole purpose of purchasing financial products and/or services from them; and

(h) the loss of privacy.

10. The injuries the Plaintiff and proposed class members suffered were directly and proximately caused by the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or

CAPITAL ONE BANK (CANADA BRANCH)'s, failure to implement or maintain adequate computer data security measures for the PII.

11. The Plaintiff and proposed class members retain a significant interest in ensuring that their PII, which remain in the Defendant, CAPITAL ONE FINANCIAL CORPORATION's, and/or CAPITAL ONE BANK (CANADA BRANCH)'s, possession, are protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose PII was stolen.

12. The Plaintiff and the proposed class members seek judgment requiring the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), to remedy the harm caused by their misconduct, which includes compensating the Plaintiff and proposed class members for the resulting fraud arising from the Data Breach and for all reasonably necessary measures the Plaintiff and proposed class members have had to take in order to identify, safeguard and protect their PII put at risk by the Defendant, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH)'s, negligent security.

B. The Parties

The Representative Plaintiff

13. [redacted]

14. In or about July 2012, the Plaintiff applied online for and received a credit card, Aspire Travel World Elite MasterCard, from the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA) BRANCH.

15. Since the announcement of the Data Breach, the Plaintiff continues to monitor his accounts in an effort to detect and prevent any misuses of his personal information.

16. The Plaintiff has, and continues to, spend his valuable time to protect the integrity of his finances and credit--time which he would not have had to expend but for the Data Breach.

17. The Plaintiff would not have applied for a credit card with and provided his PII to the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), during the period of the Data Breach had they disclosed that they lacked adequate computer systems and data security practices to safeguard consumers' PII from theft.

18. The Plaintiff suffered actual injury from having his PII accessed, compromised and/or stolen as a result of the Data Breach.

19. The Plaintiff suffered actual injury and damages in paying money to, and purchasing financial products and/or services through, the Defendants, CAPITAL ONE FINANCIAL CORPORATION's and/or CAPITAL ONE BANK (CANADA BRANCH), business during the Data Breach (e.g., paying interest on credit cards, paying minimum balance fees and other banking fees), expenditures which he would not have made with the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), had they disclosed that they lacked computer systems and data security practices adequate to safeguard consumers PII from theft.

20. The Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII--a form of intangible property that the Plaintiff entrusted to the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE BANK (CANADA BRANCH), for the purpose of applying for and using their financial products, which was accessed, compromised and/or stolen as a result of the Data Breach.

21. The Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has concerns for the loss of his privacy.

22. The Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from his PII being placed in the hands of unauthorized third parties or malicious actors.

23. The Plaintiff has a continuing interest in ensuring his PII, which remains in the possession of the Defendants, CAPITAL ONE FINANCIAL CORPORATION and/or CAPITAL ONE

BANK (CANADA BRANCH), is protected and safeguarded from future data breaches

The Defendants

24. The Defendant, CAPITAL ONE FINANCIAL CORPORATION, is a company duly incorporated pursuant to the laws of Delaware, one of the United States of America, and has a registered agent, Corporation Service Company, at 251 Little Falls Drive, Wilmington, Delaware, 19808, United States of America.

25. The Defendant, CAPITAL ONE BANK (CANADA BRANCH), is a national bank with its principal place of business at 161 Bay Street, Toronto, Ontario, M5J 2S1, Canada.

26. At all material times to the cause of action herein, the Defendant, CAPITAL ONE BANK (CANADA BRANCH), was, and is, a wholly owned subsidiary of the Defendant, CAPITAL ONE FINANCIAL CORPORATION.

27. At all material times to the cause of action herein, the Defendant, CAPITAL ONE FINANCIAL CORPORATION, issued Visa and/or MasterCard branded credit cards and other such similar financial products throughout Canada including the Province of British Columbia. Such credit was extended through the Defendant, CAPITAL ONE BANK (CANADA BRANCH).

28. At all material times to the cause of action herein, the business and interests of each of the Defendants, CAPITAL ONE FINANCIAL CORPORATION and CAPITAL ONE BANK (CANADA BRANCH), is interwoven with that of the other and each is an agent of the other for the shared common purpose of offering financial products and/or services to consumers in North America, including credit and/or debit cards.

29. The Defendants, CAPITAL ONE FINANCIAL CORPORATION and CAPITAL ONE BANK (CANADA BRANCH), are collectively hereinafter referred to as "CAPITAL ONE".

C. The Class and Class Period

30. This action is brought on behalf of members of a class consisting of the Plaintiff and all persons resident in Canada who applied for the Defendant, CAPITAL ONE's, credit card products from 2005 through 2019 and whose PII which was collected, recorded, stored and/or maintained by the Defendant, CAPITAL ONE, which was accessed, compromised and/or stolen from the Defendant, CAPITAL ONE, as a result of the Data Breach or such other class definition as the Court may ultimately decide on the motion for certification (the "Class Members").

D. Factual Allegations

The Banking System is a Constant Target for Malicious Actors

31. Data breaches have become widespread. The banking and financial sectors are a particularly high target among cyber criminals given the massive volumes of data and money that can be stolen.

32. The consequences to affected consumers are significant as sensitive personal and financial information is exposed. It is further exacerbated when, as here, compromised and/or stolen PII includes social insurance numbers ("SIN") which makes it possible for malicious actors to file fraudulent tax returns, file for unemployment benefits or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect and may not be uncovered until the SIN has been used in a fraudulent transaction. Moreover, it is no easy task to change or cancel a compromised and/or stolen SIN. Even then, a new SIN may not be effective as credit bureaus and banks are able to link the new SIN very quickly to the old SIN, so all of the old, bad information is quickly inherited into the new SIN.

33. The Defendant, CAPITAL ONE, knew the importance of safeguarding customer PII entrusted to it and of the foreseeable consequences if its computer data security systems were to be breached, including the significant costs that would be imposed on its customers as a result of a data breach.

The Defendant, CAPITAL ONE's, Customer Data Collection Practices

34. The Defendant, CAPITAL ONE, is one of the largest banking institutions in North America.

35. As part of applying for a credit card and/or other financial products or services, consumers provide banks their names, addresses, SINs and other valuable, sensitive and private PII.

36. At all relevant times to the cause of action herein, the Defendant, CAPITAL ONE, knew or ought to have known that the PII collected, maintained and stored from credit card customer applications is highly sensitive, susceptible to attack and could be used for wrongful purposes by third parties, such as identity theft and fraud.

37. Banking repositories and computer databases are popular targets for cyberattacks, especially given the extremely sensitive nature of the PII stored on those repositories and computer databases. The frequency and prevalence of attacks make it imperative that banks such as the Defendant, CAPITAL ONE, routinely monitor for exploits and cyberattacks and regularly update their computer software and security procedures.

38. Such exploits can go undetected for a long period of time, especially if industry best practices are not routinely used.

39. PII is a valuable commodity. A "cyber black market" exists in which criminals openly post stolen payment card numbers, SINs, and other personal, private information on multiple underground internet web sites. PII is valuable to identity thieves because they can use victims' personal data, including PII, to open new financial accounts and take out loans in another person's name, incur charges on existing accounts or clone ATM, debit and credit cards.

40. This is especially true for financial institutions, given that the PII disclosed in the Data Breach was precisely the PII the Defendant, CAPITAL ONE, requested to process and, in some cases, approve consumers for credit cards and other financial products and/or services.

41. Professionals tasked with trying to stop fraud and other misuse know that PII have real monetary value in part because criminals continue their efforts to obtain this data. In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred.

42. The PII of consumers remains of high value to identity criminals as evidenced by the prices criminals will pay through black market sources or what is often called the "Dark Web". Numerous internet sources cite Dark Web pricing for stolen identity credentials. For example, a complete set of bank account credentials can fetch $1,000.00 or more (depending on the associated credit score or balance available to criminals). A stolen credit and/or debit card number can sell for $5.00 to $110.00 on the Dark Web.

43. At all relevant times to the cause of action herein, the Defendant, CAPITAL ONE, knew or ought to have known of the importance of safeguarding PII and of the foreseeable consequences that would occur if its computer data security system was breached including, specifically, the significant costs that would be imposed on its customers as a result of a data breach.

44. The Defendant, CAPITAL ONE, was or should have been fully aware of the significant volume of daily online credit applications amounting to tens of thousands of daily interactions with consumers' PII and thus, the significant number of individuals who would be harmed by a breach of its computer data systems.

45. As alleged herein, despite all of this publicly available knowledge of the continued compromises of PII in the hands of third parties such as banking institutions, retailers and restaurant chains, the Defendant, CAPITAL ONE's, approach to safeguarding, protecting, storing and/or maintaining the privacy and security of the Plaintiff and Class Members' PII was reckless or at the very least, negligent.

The Data Breach

46. On July 29, 2019, the Defendant, CAPITAL ONE, admitted to one of the largest data

breaches in history in which more than 100 million American and 6 million Canadian consumers were affected. The Data Breach notice stated in relevant part:

> *Capital One Announces Data Security Incident*
>
> *MCLEAN, Va., July 29, 2019 /PRNewswire/ -- Capital One Financial Corporation*
>
> *(NYSE: COP) announced today that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.*
>
> * * *
>
> *Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.*
>
> * * *
>
> *The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:*
>
> - *Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information*

- *Fragments of transaction data from a total of23 days during 2016, 2017 and 2018.*

* * *

- *About 140,000 Social Security numbers of our credit card customers*

- *About 80,000 linked bank account numbers of our secured credit card customers*

* * *

We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.

Safeguarding our customers' information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.

* * *

For more information about this incident and what Capital One is doing to respond, visit www.capitalone.com/facts2019. In Canada, information can be found at www.capitalone.ca/facts2019 and www.capitalone.ca/facts2019/fr. The investigation is ongoing and analysis is subject to change. As we learn more, we will update these websites to provide additional information.

47. The Data Breach occurred as a result of the Defendant, CAPITAL ONE's, failure to adequately safeguard, protect and/or secure the PII of approximately 100 million American

and 6 million Canadian consumers in its cloud-based repository and computer database.

48. The Defendant, CAPITAL ONE, also reported that the Data Breach impacted consumers who applied for its credit card products from 2005 through "early 2019," with information that included "personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income".

49. In addition to the aforementioned "routine" collections, the Defendant, CAPITAL ONE, also admitted that consumers' credit scores, credit limits, balances, payment histories, contact information and "fragments of transaction data from a total of 23 days during 2016, 2017 and 2018" had been accessed during the Data Breach.

50. The Defendant, CAPITAL ONE, admitted that "about 140,000 Social Security numbers of [its] credit card customers" and "about 80,000 linked bank account numbers of our secured credit card customers" were also disclosed in the Data Breach.

51. At no point did the Defendant, CAPITAL ONE, offer any concrete assistance or offer to remunerate the Plaintiff and Class Members for its negligence. Despite acknowledging that the PII was stolen by a malicious actor and placed on the internet for anyone to access, download and use, the Defendant, CAPITAL ONE, attempted to downplay the gravity of breach claiming " it is unlikely that the information was used for fraud or disseminated by this individual".

52. The PII was accessed, compromised and/or stolen as a result of the Defendant, CAPITAL ONE's, acts and omissions and its failure to properly safeguard and protect the PII, despite being aware of cybersecurity standards, industry best practices and the vulnerability of financial service institutions to attack.

53. In addition to its failure to prevent the Data Breach, the Defendant, CAPITAL ONE, also failed to detect the breach for at least three months--despite it being publicly represented on the popular and often trafficked GitHub internet website. Intruders, therefore, had at least three months to access, collect, download and make use of this information for fraudulent

and/or other malicious purposes.

54. During this time, the Defendant, CAPITAL ONE, failed to recognize its computer data and cloud repository systems had been breached and that intruders were stealing the PII of 100 million plus credit card applicants. Indeed, the Data Breach was not even discovered as a result of the Defendant, CAPITAL ONE's, diligence or its internal cyber security systems, but rather by a third party who "sent a message to the company's responsible disclosure email address with a link to the GitHub page."

55. While timely action by the Defendant, CAPITAL ONE, in identifying the Data Breach would likely have significantly reduced the harmful consequences, instead, its inaction and negligence contributed to the scale of the Data Breach and the resulting damages to the Plaintiff and Class Members.

Defendant, CAPITAL ONE's, Privacy Policy

56. As a condition of credit, the Defendant, CAPITAL ONE, required applicants to provide them with certain personal information. In its ordinary course of business, the Defendant, CAPITAL ONE, stored and maintained this personal information including, but not limited to, names, addresses, dates of birth and SINs.

57. By obtaining, collecting, using and deriving a benefit from the Plaintiff's and Class Members' PII, the Defendant, CAPITAL ONE, assumed legal and equitable duties to those individuals. The Defendant, CAPITAL ONE, knew or ought to have known that it was responsible for protecting the Plaintiff's and Class Members' PII from disclosure. At all relevant times, the Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

58. The Plaintiff and Class Members, as credit card applicants, relied on the Defendant, CAPITAL ONE, to keep their PII confidential and securely stored, to use this information for business purposes only and to make only authorized disclosures of this information.

59. In addition to its obligations under the law, the Defendant, CAPITAL ONE, independently

and routinely promised to safeguard PII. Pursuant to its privacy policy the Defendant, CAPITAL ONE, represented in part the following:

> "*To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.*
>
> *Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you...*
>
> *At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices".*

The Data Breach Caused Harm and Will Result in Additional Fraud

60. The ramifications of the Defendant, CAPITAL ONE's, failure to keep customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

61. Consumer victims of data breaches are more likely to become victims of identity fraud. PII is a valuable commodity to identity thieves once the information has been accessed, compromised and/or stolen .

62. Identity thieves can use PII, such as that of the Plaintiff and Class Members which the Defendant, CAPITAL ONE, failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits

or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

63. As a result of the Defendant, CAPITAL ONE's, delay in detecting and notifying consumers of the Data Breach, the risk of fraud for the Plaintiff and Class Members has been driven even higher.

64. Moreover, reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

65. As a direct and proximate result of the Defendant, CAPITAL ONE's, wrongful actions and inaction, the Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and fraud. The Plaintiff and Class Members must take at least the following steps to attempt to prevent further misuse of their PII:

(a) review and monitor credit card statements for any unusual or unknown charges;

(b) contact their financial institution (which is not necessarily the Defendant, CAPITAL ONE) to determine if there is any suspicious activity on their accounts;

(c) change their account information;

(d) place a fraud alert on their credit bureau reports;

(e) place a security freeze on their credit bureau reports; and

(f) periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

66. Additionally, there is commonly lag time between when the harm occurs and when it is discovered and also between when the PII is stolen and when it is used. According to the United States Government Accountability Office, which conducted a study regarding data

breaches:

> *[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.*

67. There is a very strong probability that those impacted by the Defendant, CAPITAL ONE's failure to adequately safeguard, protect and secure the PII could be at risk of fraud and identity theft for extended periods of time.

68. As such, the Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Plaintiff and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

Plaintiff and Class Members Suffered Damages

69. The PII of the Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by the Defendant, CAPITAL ONE. The Defendant, CAPITAL ONE, did not obtain the Plaintiff's and Class Members' consent to disclose their PII to any other third party as required by applicable law and industry standards.

70. The Data Breach was a direct and proximate result of the Defendant, CAPITAL ONE's, failure to properly safeguard and protect the Plaintiff's and Class Members' PII from unauthorized access, use and disclosure, as required by government regulations and industry practices including the Defendant, CAPITAL ONE's, failure to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the Plaintiff's and Class Members' PII to protect against

reasonably foreseeable threats to the security or integrity of such information.

71. The Defendant, CAPITAL ONE, had the resources to prevent a data breach, but instead chose to put profit before consumers' privacy and protection of the consumers' PII.

72. Had the Defendant, CAPITAL ONE, remedied the deficiencies in its computer data systems, followed government regulations and adopted the appropriate industry security measures, the Defendant, CAPITAL ONE, would have prevented intrusion into its computer data systems and, ultimately, the theft of its consumers' confidential PII.

73. As a result of the Defendant, CAPITAL ONE's, wrongful actions, inaction, negligent security practices and the resulting Data Breach, the Plaintiff and Class Members have been placed at an imminent, immediate and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity and filing police reports. This time has been lost forever and cannot be recaptured.

74. The Defendant, CAPITAL ONE's, wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of the Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

(a) theft of their personal and financial information;

(b) unauthorized charges on their debit and credit card accounts;

(c) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of unauthorized third parties and misused *via* the sale of the Plaintiff's and Class Members'

information on the internet's black market;

(d) the untimely and inadequate notification of the Data Breach;

(e) the improper disclosure of their PII;

(f) loss of privacy;

(g) money paid to, and purchasing products from, the Defendant, CAPITAL ONE's, business during the Data Breach (e.g., paying interest on credit cards, paying minimum balance fees and other banking fees), expenditures which the Plaintiff and Class Members would not have made with the Defendant, CAPITAL ONE, had it disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII from theft;

(h) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

(i) ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established black market;

(j) loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

(k) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data

Breach.

75. While the Plaintiff's and Class Members' PII has been accessed, compromised and/or stolen, the Defendant, CAPITAL ONE, continues to hold the PII of consumers, including the Plaintiff's and Class Members' PII. Particularly because the Defendant, CAPITAL ONE, has demonstrated an inability to prevent a data breach, the Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

Part 2: RELIEF SOUGHT

1. The Plaintiff, on his own behalf, and on behalf of Class Members, claims against the Defendants as follows:

(a) an order certifying this action as a class proceeding pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c.50 and appointing the Plaintiff as the named representative of the class;

(b) a declaration that the Defendants were negligent in failing to adequately safeguard, protect, store and/or maintain the PII of the Plaintiff and Class Members;

(c) a declaration that the Defendants were in breach of their duty to adequately safeguard, protect, store and/or maintain the PII of the Plaintiff and Class Members;

(d) a declaration that the Defendants breached their contractual duties owed to the Plaintiff and Class Members by permitting or failing to prevent the compromise and/or theft of the PII of the Plaintiff and Class Members as a result of the Data Breach;

(e) a declaration that the Defendants breached the Plaintiff's and Class Members' common law and statutory right to privacy under the *Privacy Act*, R.S.B.C. 1996, c.373 by failing to adequately safeguard, protect, store and/or maintain their personal and/or financial information;

(f) a declaration that the Defendants breached their fiduciary duty of care to use reasonable means to keep the PII of the Plaintiff and Class Members strictly confidential and secure;

(g) a declaration that the Defendants negligently misrepresented to the Plaintiff and Class Members that their PII was secure and protected from unauthorized access by unauthorized third parties;

(h) a declaration that the Defendants engaged in fraudulent and/or deceptive acts by concealing, suppressing and/or omitting material facts as to the safety and security of the Plaintiff's and Class Members' PII on their computer data system;

(i) a declaration that the Defendants violated the *Business Practices and Consumer Protection Act*, S.B.C. 2004 by engaging in deceptive acts and/or business practices which misrepresented the safety and security of the Plaintiff's and Class Members' PII on their computer data system;

(j) a declaration that the Defendants violated the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 by failing to adequately safeguard, protect, store and/or maintain the PII of the Plaintiff and Class Members;

(k) a declaration that the Defendants are vicariously liable for the acts and omissions of their officers, directors, agents, employees and representatives;

(l) general damages;

(m) punitive, aggravated or exemplary damages;

(n) interim, interlocutory and permanent Orders as are necessary to protect the interests of the Plaintiff and Class Members as result of the Data Breach including, *inter alia*, that the Defendants provide appropriate credit monitoring services;

(o) costs on a solicitor/client basis;

(p) pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, R.S.B.C. 1996, c. 79; and

(q) such further and other relief as to this Honourable Court may seem just.

Part 3: LEGAL BASIS

A. Jurisdiction

1. There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act,* R.S.B.C. 2003, c.28 (the *"CJPTA"*) in respect of these Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10(e)(I), (g) and (h) of the *CJPTA* because this proceeding:

(e)(I) concerns contractual obligations, which to a substantial extent, were to be performed in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

B. Causes of Action

Negligence

2. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

3. The Defendant, CAPITAL ONE, solicited and took possession of Plaintiff's and the Class members' PII and it had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Further, the Defendant, CAPITAL ONE, had a duty to

destroy Plaintiff's and Class Members' PII within an appropriate amount of time after it was no longer required by it, in order to mitigate the risk of such non-essential PII being accessed, compromised and/or stolen in a data breach.

4. Upon accepting and storing the Plaintiff's and Class Members' PII in its computer data systems and on its networks, the Defendant, CAPITAL ONE, undertook and owed a duty of care to the Plaintiff and Class Members to exercise reasonable care to secure and safeguard the Plaintiff's and Class Members' PII and to use commercially-reasonable methods to do so. The Defendant, CAPITAL ONE, knew that the PII was private and confidential, and should be protected as private and confidential.

5. The Defendant, CAPITAL ONE, owed a duty of care not to subject the Plaintiff and Class Members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate computer data system security practices.

6. The Defendant, CAPITAL ONE, owed a duty of care to the Plaintiff and Class Members to quickly detect a data breach and to timely act on warnings about data breaches.

7. The Defendant, CAPITAL ONE's, duties arose from its relationship to the Plaintiff and Class Members and from industry custom.

8. The Defendant, CAPITAL ONE, through its actions and/or failures to act, unlawfully breached duties owed to the Plaintiff and Class Members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the PII entrusted to it.

9. The Defendant, CAPITAL ONE, through its actions and/or failures to act, allowed unmonitored and unrestricted access to unsecured PII.

10. The Defendant, CAPITAL ONE, through its actions and/or failures to act, failed to provide adequate supervision and oversight of the PII with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third

parties to gather the Plaintiff's and Class Members' PII, misuse that PII and intentionally disclose it to unauthorized third parties without consent.

11. The Defendant, CAPITAL ONE, knew or ought to have known the risks inherent in collecting and storing PII, the importance of adequate security and the well-publicized data breaches within the financial services industry.

12. The Defendant, CAPITAL ONE, knew or ought to have known that its computer data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

13. Due to the Defendant, CAPITAL ONE's, knowledge that a breach of its computer data systems would damage millions of its customers including the Plaintiff and Class Members, it had a duty to adequately protect its computer data systems and the PII contained thereon.

14. The Defendant, CAPITAL ONE, had a special relationship with the Plaintiff and Class Members. The Plaintiff's and Class Members' willingness to entrust the Defendant, CAPITAL ONE, with their PII was predicated on the understanding that it would take adequate security precautions to safeguard that information. Moreover, only the Defendant, CAPITAL ONE, had the ability to protect its computer data systems and the PII stored on those computer data systems from attack.

15. The Defendant, CAPITAL ONE's, own conduct also created a foreseeable risk of harm to the Plaintiff and Class Members and their PII. The Defendant, CAPITAL ONE's, misconduct included failing to:

(a) secure its computer data systems, despite knowing their vulnerabilities;

(b) comply with industry standard security practices;

(c) implement adequate system and event monitoring; and

(d) implement the systems, policies, and procedures necessary to prevent this type of data breach.

16. The Defendant, CAPITAL ONE, also had independent duties under government regulations that required it to reasonably safeguard the Plaintiff's and Class Members' PII, and promptly notify them about the Data Breach.

17. The Defendant, CAPITAL ONE, breached it's duties owed to the Plaintiff and Class Members, the particulars of which are:

(a) by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the Plaintiff's and Class Members' PII;

(b) by creating a foreseeable risk of harm through the misconduct as alleged herein;

(c) by failing to implement adequate security systems, protocols and practices sufficient to protect the Plaintiff's and Class Members' PII before and after learning of the Data Breach;

(d) by failing to comply with industry data security standards during the period of the Data Breach; and

(e) by failing to timely and accurately disclose that the Plaintiff's and Class Members' PII had been improperly accessed, compromised and/or stolen.

18. Through the Defendant, CAPITAL ONE's, acts and/or omissions as alleged herein including it's failure to provide adequate security and to protect the Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, the Defendant, CAPITAL ONE, unlawfully breached its duty to use reasonable care to adequately protect and secure the Plaintiff's and Class Members' PII while it was within its possession or control.

19. The Defendant, CAPITAL ONE, had an affirmative duty to timely disclose the unauthorized access and theft of the Plaintiff's and Class Members' PII so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

20. The Defendant, CAPITAL ONE, breached its duty to notify the Plaintiff and Class Members of the unauthorized access to their PII by waiting to notify them and then by failing to provide the Plaintiff and Class Members sufficient information regarding the Data Breach.

21. Through the Defendant, CAPITAL ONE's, acts and/or omissions as alleged herein including its failure to provide adequate security and to protect the Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen and misused, the Defendant, CAPITAL ONE, unlawfully breached its duty to use reasonable care to adequately protect and secure the Plaintiff's and Class Members' PII while it was within its possession or control.

22. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, the Defendant, CAPITAL ONE, prevented the Plaintiff and Class Members from taking meaningful proactive steps to secure their financial data and bank accounts.

23. The Defendant, CAPITAL ONE, improperly and inadequately safeguarded the Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the unauthorized access. The Defendant, CAPITAL ONE's, failure to take proper security measures to protect sensitive PII as described herein created conditions conducive to a foreseeable, intentional criminal act namely, the unauthorized access and theft of Plaintiff's and Class Members' PII.

24. The Defendant, CAPITAL ONE's, conduct was grossly negligent and departed from all reasonable standards of care including, but not limited to, failing to adequately protect the PII, failing to conduct regular security audits, failing to provide adequate and appropriate supervision of persons having access to the Plaintiff's and Class Members' PII, and failing to provide the Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been accessed, compromised and/or stolen.

25. Neither the Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their PII as described herein.

26. The Defendant, CAPITAL ONE's, failure to exercise reasonable care in safeguarding PII by

adopting appropriate security measures including proper encryption storage techniques, was the direct and proximate cause of the Plaintiff's and Class Members' PII being accessed, compromised and/or stolen through the Data Breach.

27. The Defendant, CAPITAL ONE, breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard the Plaintiff's and Class Members' PII.

28. As a result of the Defendant, CAPITAL ONE's, breach of duties, the Plaintiff and Class Members suffered damages including, but not limited to, damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia,* by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft as described herein.

Breach of Contract

29. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

30. The Defendant, CAPITAL ONE, solicited and invited the Plaintiff and Class Members to apply for credit card products by providing their PII. The Plaintiff and Class Members accepted the Defendant, CAPITAL ONE's, offers and provided their PII to the Defendant, CAPITAL ONE, to apply for its credit card products.

31. When the Plaintiff and Class Members applied for the Defendant, CAPITAL ONE's, credit card products, they provided their PII to the Defendant, CAPITAL ONE. In so doing, the Plaintiff and Class Members on the one hand, and the Defendant, CAPITAL ONE, on the

other, entered into mutually agreed-upon implied contracts pursuant to which the Plaintiff and Class Members agreed that their PII was valid, while the Defendant, CAPITAL ONE, agreed that it would use the Plaintiff's and Class Members' PII in its possession for only the agreed-upon purpose of processing the credit card product applications, and no other purpose.

32. Implicit in the agreement to use the PII in its possession for only the agreed-upon application and no other purpose was the obligation that the Defendant, CAPITAL ONE, would use reasonable measures to safeguard and protect the PII of the Plaintiff and Class Members in its possession.

33. By accepting the PII for credit card product applications, the Defendant, CAPITAL ONE, assented to and confirmed its agreement to reasonably safeguard and protect the Plaintiff's and Class Members' PII from unauthorized disclosure or uses and to timely and accurately notify the Plaintiff and Class Members if their data had been breached, accessed, compromised and/or stolen by unauthorized third parties.

34. The Plaintiff and Class Members would not have provided and entrusted their PII to the Defendant, CAPITAL ONE, to apply for the Defendant, CAPITAL ONE's, credit card products in the absence of the implied contract between them and the Defendant, CAPITAL ONE.

35. The Plaintiff and Class Members fully performed their obligations under the implied contracts with the Defendant, CAPITAL ONE.

36. The Defendant, CAPITAL ONE, breached the implied contracts it made with the Plaintiff and Class Members by failing to safeguard and protect the Plaintiff's and Class Members' PII and by failing to provide timely and accurate notice to them that their PII was accessed, compromised and/or stolen as a result of the Data Breach.

37. The Defendant, CAPITAL ONE, breached the implied contracts it made with the Plaintiff and Class Members by failing to ensure that the Plaintiff's and Class Members' PII in its possession was used only for the agreed-upon application verification and no other

purpose.

38. The Plaintiff and Class Members conferred a monetary benefit on the Defendant, CAPITAL ONE, which has accepted or retained that benefit. Specifically, the credit card products typically carry annual fees and other charges (e.g. interest) for use. In exchange, the Plaintiff and Class Members should have received the services that were the subject of the transaction and should have been entitled to have the Defendant, CAPITAL ONE, protect their PII with adequate computer data security measures.

39. The Defendant, CAPITAL ONE, failed to secure the Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit the Plaintiff and Class Members provided.

40. The Defendant, CAPITAL ONE, acquired the PII through inequitable means when it failed to disclose the inadequate computer data security practices as alleged herein.

41. Had the Plaintiff and Class members known that the Defendant, CAPITAL ONE, would employ inadequate computer data security measures to safeguard their PII, they would not have applied for the Defendant, CAPITAL ONE's, credit card products.

42. As a direct and proximate result of the Defendant, CAPITAL ONE's, breaches of the implied contracts between it on the one hand, and the Plaintiff and Class Members on the other, the Plaintiff and Class Members suffered actual losses and damages as described herein.

43. The Plaintiff and Class Members were harmed as the result of the Defendant, CAPITAL ONE's, breach of the implied contracts because their PII was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. The Plaintiff and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. The Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees and other expenses relating to identity theft losses or protective measures. The Plaintiff and Class Members are further damaged as their PII remains in the hands of those

who obtained it without their consent.

Breach of Privacy

44. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

45. The Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

46. The Defendant, CAPITAL ONE, owed a duty to its credit card product applicants, including the Plaintiff and Class Members, to keep their PII confidential.

47. The Defendant, CAPITAL ONE, failed to protect and released to unknown and unauthorized third parties computer databases containing the PII of the Plaintiff and Class Members.

48. The Defendant, CAPITAL ONE, allowed unauthorized and unknown third parties access to and examination of the PII of the Plaintiff and Class Members by way of the Defendant, CAPITAL ONE's, failure to protect the PII in its computer databases.

49. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of the Plaintiff and Class Members, especially where the information includes SINs and dates of birth, is highly offensive to a reasonable person.

50. The intrusion was into a place or thing which was private and is entitled to be private. The Plaintiff and Class Members disclosed their PII to the Defendant, CAPITAL ONE, as part of their use of Defendant, CAPITAL ONE's, financial products and/or services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. The Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

51. The Data Breach at the hands of Defendant, CAPITAL ONE, constitutes an intentional interference with the Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person causing them distress, humiliation and/or anguish.

52. The Defendant, CAPITAL ONE, acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its computer data security practices were inadequate and insufficient.

53. By permitting unauthorized third parties to access to the Plaintiff's and Class Members' PII, the Defendant, CAPITAL ONE, breached the Plaintiff's and Class Members' common law and statutory right to privacy under the *Privacy Act,* R.S.B.C. 1996, c.373, including but not limited to the tort of intrusion upon seclusion and the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (*"PIPEDA"*), which the Plaintiff and Class Members plead and rely upon.

54. As a proximate result of the above acts and/or omissions of the Defendant, CAPITAL ONE, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing the Plaintiff and Class Members to suffer damages.

55. Unless and until enjoined and restrained by order of this Court, the Defendant, CAPITAL ONE's, wrongful conduct will continue to cause great and irreparable injury to the Plaintiff and Class Members in that the PII maintained by Defendant, CAPITAL ONE, can be viewed, distributed and used by unauthorized persons. The Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for the Plaintiff and Class Members.

Breach of Fiduciary Duty

56. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

57. The Defendant, CAPITAL ONE, was in a fiduciary relationship with the Plaintiff and Class

Members by reason of their entrustment of the PII belonging to the Plaintiff and Class Members.

58. By virtue of this fiduciary relationship and the vulnerability of the Plaintiff and Class Members, the Defendant, CAPITAL ONE, had a duty of care to use reasonable means to keep the private information of the Plaintiff and Class Members strictly confidential and secure. The Defendant, CAPITAL ONE, unlawfully breached this duty.

Negligent Misrepresentation

59. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

60. By virtue of the trust reposed in the Defendant, CAPITAL ONE, by the Plaintiff and Class Members, there existed a special relationship between the parties giving rise to a duty of care owed by the Defendant, CAPITAL ONE, to the Plaintiff and Class Members.

61. The Defendant, CAPITAL ONE, represented to the Plaintiff and Class Members that any PII provided by the Plaintiff and Class Members to the Defendant, CAPITAL ONE, would be secure and protected from unauthorized access by third parties. The Defendant, CAPITAL ONE, ought reasonably to have foreseen that the Plaintiff and Class Members would reasonably rely on that representation.

62. The Defendant, CAPITAL ONE, made numerous representations in its privacy policy regarding the supposed secure nature of its computer data system. Such representations were false as the Defendant, CAPITAL ONE, utilized outdated encryption and failed to disclose that it did not use reasonable industry standard means to safeguard against hacking and theft of the Plaintiff's and Class Members' PII.

63. The Defendant, CAPITAL ONE's, representations that the PII received by it from the Plaintiff and Class Members would be adequately safeguarded and protected was untrue, inaccurate and/or misleading. The representations were made negligently.

64. The Plaintiff and Class Members reasonably relied on these misrepresentations to their detriment. Such misrepresentations were material to customers of the Defendant, CAPITAL ONE. The Plaintiff and Class Members would not have applied for a credit card and provided their PII had they known the truth that the Defendant, CAPITAL ONE's, computer data system was not as secure as represented or by any industry standard.

65. The Defendant, CAPITAL ONE, intended that the Plaintiff and Class Members rely on their security representations, as it knew that no would-be customer would submit their PII to unreasonable security risks. In reliance on these representations and/or omissions, the Plaintiff and Class Members contracted with the Defendant, CAPITAL ONE, and provided their PII.

66. By failing to disclose the Data Breach in a timely manner and to protect the PII of the Plaintiff and Class Members against loss, theft and/or unauthorized access, the Defendant, CAPITAL ONE, misled customers into believing that its computer data system was secure from intrusions.

67. As a direct and proximate result of the Defendant, CAPITAL ONE's, negligent misrepresentations the Plaintiff and Class Members have experienced damage to their PII provided to the Defendant, CAPITAL ONE, actual identity theft and/or being placed at an imminent, immediate and continuing increased risk of harm from identity theft and/or fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the data breach.

Fraud By Concealment

68. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

69. In the alternative, the Plaintiff pleads a cause of action for fraud by concealment.

70. The Defendant, CAPITAL ONE, engaged in fraudulent and/or deceptive acts with regard to its computer data system by concealing, suppressing and/or omitting the material fact of

the inadequacy of the privacy and security protections of the PII of the Plaintiff and Class Members. Further, the Defendant, CAPITAL ONE, made representations in its privacy policy regarding the supposed secure nature of its computer data system. Such representations were false and made with reckless disregard for the truth.

71. The Defendant, CAPITAL ONE, failed to disclose to the Plaintiff and Class Members that its computer data system failed to meet industry standards for the protection of the Plaintiff and Class Members PII.

72. At all material times to the cause of action herein, the Defendant, CAPITAL ONE, knew or ought to have known that its computer data system was inadequate to protect and safeguard the Plaintiff's and Class Members' PII and the risk of a data breach or theft was highly probable.

73. By failing to disclose the Data Breach in a timely manner and to protect the PII of the Plaintiff and Class Members against loss, theft and/or unauthorized access, the Defendant, CAPITAL ONE, misled customers into believing that its computer data system was secure from intrusions.

74. As a direct and proximate result of the Defendant, CAPITAL ONE's, fraudulent and/or deceptive acts, the Plaintiff and Class Members experienced loss or damage to their PII, actual identity theft and/or were placed at an imminent, immediate and continuing increased risk of harm from identity theft and/or fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach.

Violation of the *Business Practices and Consumer Protection Act,* S.B.C. 2004 ("*BPCPA*")

75. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

76. The *BPCPA* was enacted to protect consumers against unfair and/or deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in

the sale of goods or services to consumers. The Defendant, CAPITAL ONE's, acts, omissions, representations and/or practices, as described herein, as to its computer data system for the purposes of providing financial products and/or services falls within the *BPCPA*.

77. The Plaintiff and Class Members are "consumers" within the meaning of the *BPCPA.*

78. The Defendant, CAPITAL ONE's, acts, omissions, misrepresentations and/or practices were and are likely to deceive consumers. By misrepresenting the safety and security of its computer data system, the Defendant, CAPITAL ONE, violated the *BPCPA*. The Defendant, CAPITAL ONE, had exclusive knowledge of undisclosed material facts, namely, that its computer data system was defective and/or unsecured, and withheld that knowledge from the Plaintiff and Class Members.

79. The Defendant, CAPITAL ONE's, acts, omissions, misrepresentations and/or practices, as alleged herein, violated the *BPCPA*, the particulars, *inter alia*, of which are:

(a) representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities which they do not have; and

(b) representing that goods or services are of a particular standard, quality or grade when they are not.

80. The Defendant, CAPITAL ONE, stored the Plaintiff's and Class Members' PII in its computer data system. The Defendant, CAPITAL ONE, represented to the Plaintiff and Class Members that its computer data system was secure and the PII would remain private and protected.

81. The Defendant, CAPITAL ONE, knew or ought to have known that it did not employ reasonable measures to keep the Plaintiff's' and Class Members' PII secure and prevented the loss or misuse of that information.

82. The Defendant, CAPITAL ONE's, deceptive acts and/or business practices induced the

Plaintiff and Class Members to provide their PII for the purpose of acquiring financial products and/or services from the Defendant, CAPITAL ONE. But for these deceptive acts and/or business practices, the Plaintiff and Class Members would not have provided their PII to the Defendant, CAPITAL ONE.

83. The Defendant, CAPITAL ONE's, representations that it would safeguard and protect the Plaintiff's and Class Members' PII in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to acquire the Defendant, CAPITAL ONE's, financial products and/or services.

84. The Plaintiff and Class Members were harmed as the result of Defendant, CAPITAL ONE's, violations of the *BPCPA* because their PII was accessed, compromised and/or stolen, placing them at a greater risk of identity theft and their PII was disclosed to unauthorized third parties without their consent.

85. The Plaintiff and Class Members have suffered loss or damage as a result of the Defendant, CAPITAL ONE's, failure to adequately safeguard, protect, secure and/or maintain the Plaintiff's and Class Members' PII.

Violation of *PIPEDA*

86. The Plaintiff re-alleges all prior paragraphs of the Notice of Civil Claim as if set out here in full.

87. The Defendant, CAPITAL ONE, provided financial products and/or services to the public through electronic communications , namely, the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications received from and on behalf of customers.

88. *PIPEDA* contains provisions that provide customers of entities providing electronic communication services to the public with redress if a company mishandles their electronically stored information.

89. The Data Breach was the result of the Defendant, CAPITAL ONE's, failure to implement safeguards appropriate to the extreme sensitivity of customers PII in breach of the *PIPEDA*.

90. The Defendant, CAPITAL ONE, failed to designate the appropriate individuals who were responsible and accountable for its computer data system security management, including compliance with its internal policies and reasonable industry standards in its collection, storage, protection and destruction of customer PII, contrary to section 4.1 of Schedule 1 to the *PIPEDA*.

91. The Defendant, CAPITAL ONE, allowed the PII of the Plaintiff and Class Members to be used and disclosed for purposes other than those for which it was collected contrary to section 4.5 of Schedule 1 to the *PIPEDA*.

92. The Defendant, CAPITAL ONE, failed to implement appropriate organizational and technological safeguards to protect the PII of the Plaintiff and Class Members against loss, theft, unauthorized access, disclosure, copying, use and/or notification contrary to section 4.7 of Schedule 1 to the *PIPEDA.*

93. As a result of the Defendant, CAPITAL ONE's, conduct and violations of sections 4.1, 4.5 and 4.7 of Schedule 1 to the *PIPEDA,* the Plaintiff and Class Members have suffered injuries, including various forms of identity theft, lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. The Plaintiff and Class Members seek the maximum statutory damages available under *PIPEDA* in addition to the cost for credit monitoring services.

Damages

94. As a result of the Defendant, CAPITAL ONE's, wrong doing as above, third parties improperly obtained access to the Plaintiff's and Class Members' PII.

95. The Plaintiff and Class Members have suffered significant loss and damages including harm and injury to their financial and other interests, all of which were damages directly resulting from the loss and disclosure of their PII by the Defendant, CAPITAL ONE.

96. As a result of the Defendant, CAPITAL ONE's, acts, omissions and/or breaches, the Plaintiff and Class Members are exposed to theft of their identity, theft from their bank accounts, and theft from their credit card and debit card accounts. The compromise of the Plaintiff's and Class Members' PII and the resulting burden, fear, anxiety, emotional distress, loss of time spent seeking to undo harm and prevent further harm, and other economic and non-economic damages suffered by the Plaintiff and Class Members were the direct and proximate result of the Defendant, CAPITAL ONE's, violations of its duties.

97. As a result of the Defendant, CAPITAL ONE's, acts and/or omissions, the Plaintiff and Class Members have suffered harm for which they claim damages. They have suffered and will continue to suffer injuries including the stress and inconvenience of knowing that unauthorized persons have their PII. Further, the Class Members' losses and expenses have occurred, are ongoing and include, *inter alia*:

(a) loss from their bank accounts as a result of the theft of credit or debit card numbers;

(b) fraudulent charges against their credit card accounts;

(c) loss of their time spent consulting with legal counsel, banking officials, credit professionals or with other individuals relevant to the loss of the subject information, with resultant financial loss;

(d) funds directly or indirectly expended in furtherance of gathering information about the loss of the confidential information, such as that spent on long-distance telephone charges, or postage; and

(e) funds directly or indirectly expended in the course of attempting to secure PII, financial data and usage data as a result of the loss of security of same by the Defendant, CAPITAL ONE, such as fees incurred changing credit cards, changing personal identifies (such as SINs), monitoring bank accounts and credit card statements, monitoring their credit bureau information, purchasing fraud insurance, and other preventative measures.

Punitive Damages

98. The Plaintiff pleads that the Defendant, CAPITAL ONE's, conduct as particularized above was reckless, wanton, negligent, callous and in total disregard of the Plaintiff's security and rights as well as those of the Class Members. The conduct of the Defendant, CAPITAL ONE, was, and continues to be, indifferent to the consequences and was, and is, motivated singularly by economic and reputational considerations. The particulars of the Defendant, CAPITAL ONE's, reprehensible conduct is as follows:

(a) given previous data breaches experienced by financial institutions, the Defendant, CAPITAL ONE, was aware of the danger of another possible data breach but failed to take the necessary precautions to protect the Plaintiff's and Class Members' PII;

(b) the Defendant, CAPITAL ONE, deliberately failed to advise the Plaintiff and Class Members of the Data Breach as soon as it became aware of same;

(c) the Defendant, CAPITAL ONE, deliberately failed to advise the Plaintiff and Class Members that their PII had been accessed, compromised and/or stolen as soon as it became aware of same;

(d) the Defendant, CAPITAL ONE, deliberately placed its' own reputational and financial interests ahead of those of the Plaintiff and Class Members;

(e) the Defendant, CAPITAL ONE, failed to immediately notify the Plaintiff and Class Members as how best to search their credit card records and to place fraud alerts on their credit cards;

(f) the Defendant, CAPITAL ONE's, response to the Data Breach was secretive, haphazard, and tardy, motivated singularly by reputational and financial considerations;

(g) the Defendant, CAPITAL ONE, deliberately left the Plaintiff and Class Members exposed to greater damages while it engaged in spin doctoring and public relations

strategies;

(h) the Defendant, CAPITAL ONE, took a cavalier and arbitrary approach with respect to its obligations to the Plaintiff and Class Members;

(i) the Defendant, CAPITAL ONE, failed to warn the Plaintiff and Class Members in a timely fashion that its computer data system had been hacked and that the PII of the Plaintiff and Class Members may have been accessed, compromised and/or stolen;

(j) the Defendant, CAPITAL ONE, waited approximately three months to warn the Plaintiff and Class Members about the Data Breach;

(k) the Defendant, CAPITAL ONE, did not timely advise the Plaintiff and Class Members of remedial steps that could be taken to protect themselves such as cancelling credit cards and engaging the services of credit card fraud alert agencies;

(l) the conduct of the Defendant, CAPITAL ONE, s set forth above was wilful, wanton, and reckless; and

(m) the Defendant, CAPITAL ONE's, acts, missions, wrong doings, breaches of legal duties or obligations constitute a wanton disregard for fair business practices.

Aggravated Damages

99. The activities of the Defendant, CAPITAL ONE, were carried out with reckless and wanton disregard for the privacy and confidentiality interests of the Plaintiff and Class Members. The Defendant, CAPITAL ONE, knowingly failed to inform the Plaintiff and Class Members that their PII had been improperly taken by third parties and knew that such information could be used to engage in identity theft or fraud. By failing to inform the Plaintiff and Class Members of the Data Breach, the Defendant, CAPITAL ONE, left the Plaintiff and Class Members exposed while at the same time preventing the Plaintiff and Class Members from taking steps, such as use of credit monitoring services or obtaining identity theft insurance. The Defendant, CAPITAL ONE, put its own financial interests ahead of those of the Plaintiff

and Class Members in failing to adequately protect the private and confidential information of the Plaintiff and Class Members and then failing to timely advise the Plaintiff and Class Members of the Data Breach. The Plaintiff and Class Members are entitled to aggravated damages, either on an individual or aggregate basis, commensurate with the Defendant, CAPITAL ONE's, outrageous behaviour.

100. The acts, omissions, wrong doings, breaches of legal duties or obligations of the Defendant, CAPITAL ONE, have caused or materially contributed to the Plaintiff's and Class Members' suffering injury, economic and non-economic losses and damages warranting aggravated damages.

Statutes

The Plaintiff pleads and relies, *inter alia*, upon the following legislation:

(a) *Class Proceedings Act*, R.S.B.C. 1996, c.50;

(b) *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28;

(c) *Business Practices and Consumer Protection Act,* S.B.C. 2004;

(d) *Negligence Act,* R.S.B.C. 1996, c.333;

(e) *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5;

(f) *Privacy Act,* R.S.B.C. 1996, c.373

and similar statutes in other Canadian provinces, as amended and the regulations made thereunder.

Plaintiff's(s') address for service:

Garcha & Company
Barristers & Solicitors
#405 - 4603 Kingsway
Burnaby, BC V5H 4M4
Canada

Fax number address for service (if any):

604-435-4944

E-mail address for service (if any):

none

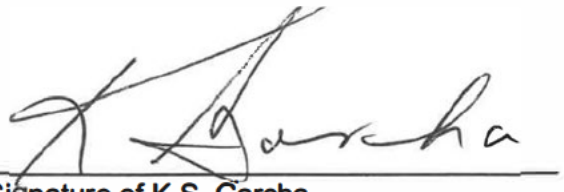
Place of trial:

Vancouver, BC
Canada

The address of the registry is:

800 Smithe Street
Vancouver, BC V6Z 2E1
Canada

Dated: August 6, 2019.



Signature of K.S. Garcha
lawyer for Plaintiff(s)

Rule 7-1(1) of the Supreme Court Civil Rules states:

(1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,

(a) prepare a list of documents in Form 22 that lists

(i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and

(ii) all other documents to which the party intends to refer at trial, and

(b) serve the list on all parties of record.

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28 (the *"CJPTA"*) in respect of these Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to sections 10 (e)(I), (g) and (h) of the *CJPTA* because this proceeding:

(e)(I) concerns contractual obligations, which to a substantial extent, were to be performed in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

APPENDIX

[The following information is provided for data collection purposes only and is of no legal effect.]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a proposed class proceeding brought on behalf of the Plaintiff and all persons resident in Canada whose personal and/or financial information was accessed, compromised and/or stolen from the Defendants computer system following a data breach by unauthorized third persons.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:
[ ] motor vehicle accident
[ ] medical malpractice
[ ] another cause

A dispute concerning:
[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] personal property
[ ] the provision of goods or services or other general commercial matters
[ ] investment losses
[ ] the lending of money
[ ] an employment relationship
[ ] a will or other issues concerning the probate of an estate
[x] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know
x] a matter not listed here

Part 4:

1. *Class Proceedings Act*, R.S.B.C. 1996, c.50;
2. *Court Jurisdiction and Proceedings Transfer Act* R.S.B.C. 2003 c.28
3. *Business Practices and Consumer Protection Act,* S.B.C. 2004 ;
4. *Negligence Act,* R.S.B.C. 1996, c.333
5. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5
6. *Court Order Interest Act*, R.S.B.C., c. 79
7. *Privacy Act,* R.S.B.C. 1996, c.373

[redacted]