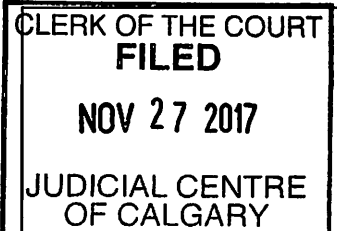


Clerk's stamp



FORM 10
[RULE 3.25]

COURT FILE NUMBER

1701-16003

COURT OF QUEEN'S BENCH OF ALBERTA
JUDICIAL CENTRE

CALGARY

PLAINTIFF

DIONE SETOGUCHI

DEFENDANTS

UBER B.V., RASIER OPERATIONS B.V., UBER
CANADA INC. and UBER TECHNOLOGIES INC.

DOCUMENT

STATEMENT OF CLAIM

ADDRESS FOR SERVICE AND CONTACT
INFORMATION OF PARTY FILING THIS
DOCUMENT

BRANCH MACMASTER LLP
Barristers
1410 – 777 Hornby Street
Vancouver, British Columbia V6Z 1S4

Luciana P. Brasil
Chelsea Hermanson
Avichay Sharon
Phone: 604-654-2999
Fax: 604-684-3429

JENSEN SHAWA SOLOMON DUGUID HAWKES LLP
Barristers
800, 304 - 8 Avenue SW
Calgary, Alberta T2P 1C2

Carsten Jensen, QC, FCI Arb
Kajal Ervin
Sean Carrie
Phone: 403 571 1520
Fax: 403 571 1528
File: 7777

NOTICE TO DEFENDANT(S)

You are being sued. You are a defendant.
Go to the end of this document to see what you
can do and when you must do it.

Statement of facts relied on:

The Parties

1. The Plaintiff, Dione Setoguchi, is an individual resident in the City of Calgary, in the province of Alberta. Ms. Setoguchi makes this claim on her own behalf and on behalf of Class Members, pursuant to the *Class Proceedings Act*, SA 2003, c C-16.5, as amended (the “CPA”).
2. The Defendant, Uber Canada Inc., is a corporation duly incorporated pursuant to the laws of Alberta as a Federal Corporation, with head offices in 100 King Street West, Suite 6200, Toronto, Ontario. It carries on business in Alberta as Uber Canada Inc. and operates out of offices located at 2500, 450- 1 ST Street SW, Calgary, Alberta.
3. The Defendant, Uber Technologies Inc., is a corporation duly incorporated pursuant to the laws of Canada, with head offices in 1812 Serenity Place, Victoria, BC. It carries on business in Alberta as Uber Technologies Inc.
4. The Defendant, Uber B.V., is a corporation duly incorporated pursuant to the laws of the Netherlands, with head offices in Amsterdam. It carries on business in Alberta as Uber B.V.
5. The Defendant, Rasier Operations B.V., is a corporation duly incorporated pursuant to the laws of the Netherlands, with head offices in the city of Amsterdam. It carries on business in Alberta as Rasier Operations B.V.
6. At all material times Uber B.V., Rasier Operations B.V., Uber Canada Inc. and Uber Technologies Inc. acted in concert and jointly in carrying out their business activities. The Defendants shall be collectively referred to as “Uber”.

Overview

7. This claim is brought by the Plaintiff, Dione Setoguchi, who, along with all of the Class Members, as defined below, had their personal information recorded and/or stored by Uber, and had that personal information accessed by unauthorized individuals in or around October 2016.
8. Uber is a worldwide transportation network company. Uber develops markets and operates the Uber Internet Application (“Uber App”), which allows Uber users (“Users”) to submit requests for transportation and/or deliveries using their smartphones. Once a User submits a request, the Uber App then alerts Uber drivers (“Drivers”) located in the vicinity of the user of his or her request. The Uber driver may then choose to provide that service to the user using the Uber App. The App connects the user and driver, and

also facilitates payment – part of which goes to the driver and part of which is retained by Uber for the services it provides.

9. Uber is the largest company of its kind, operating in 83 countries and over 674 cities around the world.
10. Uber services were first launched in Canada in or around 2008. Uber currently operates in 13 major cities in the Provinces of Alberta, Ontario, Quebec and British Columbia. In the Province of Alberta it operates in the cities of Calgary and Edmonton. Once an individual is signed up they can use the Uber App in any location worldwide where Uber operates.
11. Services that are provided by Uber include, but are not limited to, the following:
 - (a) Uber EATS: a food delivery services;
 - (b) Uber X: a ride service provided in standard, 4-door sedan vehicles;
 - (c) Uber XL: a ride service which is substantially similar to Uber X, but which includes larger vehicles and at a premium price to Uber X;
 - (d) Uber Select: a ride service which is substantially similar to Uber X and Uber XL, but which includes luxury cars and at a premium price to Uber XL;
 - (e) Uber Black: a ride service which is substantially similar to Uber X, Uber XL and Uber Select, but which provides transportation services in limousines offered by licensed limousine drivers;
 - (f) Uber SUV: a ride service which is substantially similar to Uber Black, but which is provided in larger, SUV-type limousines at a premium price to Uber Black;
 - (g) Uber Taxi: a ride service that is provided by licensed taxi drivers and vehicles at metered rates; and
 - (h) Uber Access: a ride service similar to Uber Taxi utilizing wheelchair-accessible taxis.
12. The transportation network services provided through Uber X, Uber XL, Uber Select, Uber Black, Uber SUV, Uber Taxi and Uber Access are based on the same or a similar platform or App. Uber EATS is a food delivery network service that is provided through a separate App. All of these services are referred to collectively herein as the “Uber App”.
13. In order to gain access to any of these services, an individual must download the Uber App and agree to the Uber terms and conditions. As part of the process of signing up for the services, and in order to download and use the App, whether as a user or as a driver, one must provide Uber with personal information including, but not limited to:

- (a) Name;
- (b) Email address;
- (c) Mobile phone number;
- (d) Credit card information; and
- (e) In the cases of persons who wish to become Uber Drivers: drivers' license information.

(the "Personal Information")

- 14. The Plaintiff and Class Members provided the Personal Information to the Defendants. The Defendants recorded and stored the Personal Information provided by the Plaintiff and the Class Members on its network(s), pursuant to the Uber terms and conditions, including any Uber privacy policies which were in effect at the relevant times.
- 15. Subsequently, Uber decided, at a time known only to the Defendants, to store the Personal Information on a third-party, cloud-based network service. Uber did not advise the Plaintiff and the Class Members that it intended to do so.
- 16. In or around October 2016, the precise date of which is known at this time only to the Defendants, two individuals (collectively, the "Cybercriminals") accessed, through the third-party, cloud-based network service, Personal Information provided by at least 57,000,000 (million) individuals worldwide (the "Uber Hack").
- 17. Uber learned about the Uber Hack soon after it had occurred. Uber deliberately concealed the Uber Hack from Class Members and other affected parties, as well as from regulators in the jurisdictions in which Uber operated. Instead of reporting the Uber Hack, and giving the Plaintiff and other Class Members the opportunity to take proactive measures in response to monitor and protect their Personal Information, the Defendants paid \$100,000.00 to the Cybercriminals.
- 18. The Uber Hack was never disclosed by Uber; rather, it was exposed by the media over a year later, in or around November 21, 2017. At no time did Uber notify the Office of the Privacy Commissioner, the Plaintiff, Class Members or other affected individuals. Had it not been for recent media exposure of the Uber Hack, Class Members would to this day remain unaware that their Personal Information had been compromised.
- 19. The Defendants knew, or ought to have known, that electronic records containing the Personal Information of the Plaintiff and Class Members, which were stored on the third-party, cloud-based server, were vulnerable to theft.

20. The information contained on the third-party, cloud-based service which was accessed by way of the Uber Hack is personal information of the Class Members as defined in the *Privacy Act*, RSA 1985, c P-21.

The Class Members

21. This claim is brought by the Plaintiff who seeks Court approval to advance this Action as a class action on behalf of the proposed Class Members, being all persons whose personal information was recorded and/or stored by Uber, including but not limited to Uber Users and Drivers, as of October 1, 2016, and whose personal information was access by unauthorized individuals in or around October 2016 ("**Class Members**" or "**Proposed Class Members**").

The Plaintiffs Experience

22. The Plaintiff, Ms. Setoguchi, registered to use the Uber App as a User in or around 2012. When registering, she was required to provide her name, address, telephone number, email address and credit card information. Further, since her initial registration Ms. Setoguchi has also been required by the Defendants to update her personal information if any changes had occurs in order to continue using the Uber App.
23. The Plaintiff expected and relied on the Defendants' guarantees that her personal information would be protected and safeguarded pursuant to the Uber terms and conditions, including Uber's privacy policy, and relevant statutes.
24. Ms. Setoguchi first found out about the Uber Hack on November 21, 2017 through media coverage. Prior to November 21, 2017 she was not aware of the Uber Hack or that the Personal Information she provided Uber was in any way compromised. Furthermore, the Plaintiff has not received any information from Uber concerning the Uber Hack and the state of her Personal Information.

Extra-Provincial Law

25. In pleading all causes of action, the Plaintiff relies on the common law of Alberta. The Plaintiff also relies on the laws of the other provinces in respect of Class Members who reside in other provinces, and who provided Personal Information to the Defendants.
26. For the purposes of the causes of action pleaded herein, the Plaintiff and the Class Members plead that those laws are the same as the laws of Alberta, and will be assumed by the Plaintiff and Class Members to be the same at Trial, except where otherwise stated herein.

Breach of Contract

27. Uber operates three Apps:

- (a) Uber Users or Uber Riders use the Rider App to request rides, track rides on their smartphones, facilitate payment for rides and rate Uber Drivers.
 - (b) Uber Drivers use the Uber Driver App to receive ride requests and to rate their riders at the completion of a trip.
 - (c) Uber EATS facilitates food delivery services. Uber Users can order food from participating businesses and make a delivery request. Through the Uber Driver App Uber Drivers are notified of the delivery request and can choose to provide that service to the Uber User.
28. In order to become an Uber User a rider must meet certain requirements:
- (a) the rider must be at least 18 years old and the must agree to the Uber terms and conditions;
 - (b) the terms set out the Rider's rights and obligations, including a limited license to use the Uber User App;
 - (c) the Rider must provide Uber with their name, phone number and email address as well as credit card payment information.
29. In order to gain access to the Uber Driver's App the driver must satisfy several safety and security conditions the Driver:
- (a) must be 21 years of age or older;
 - (b) possess a valid driver's license;
 - (c) provide proof of vehicle registration;
 - (d) provide proof of vehicle insurance;
 - (e) provide proof of eligibility to work in Canada;
 - (f) pass background criminal and driver's abstract checks conducted by a third party on behalf of Uber and pass a safety inspection of their vehicle.
30. If the requirements are met the Driver must then accept the Uber terms and conditions and thereupon he or she enters into a contract with Rasier Operations B.V.
31. The same or similar pre-conditions must be met to become an Uber Driver or User of Uber EATS. Likewise, Users and Drivers using Uber EATS are required to provide the same personal information.

32. By accepting the terms and conditions set out by Uber, Users and Drivers enter into a contractual relationship with Uber. While these are separate contracts, it is important to note that in both cases the agreements are standard contracts of adhesion, as the terms and conditions are universally and uniformly set out by Uber and are non-negotiable.
33. In the terms and conditions of the Uber User agreement Uber sets out the Users' obligations to provide and maintain accurate personal information. It reads as follows:

Account registration requires you to submit to Uber certain personal information, such as your name, address, mobile phone number and age, as well as at least one valid payment method (either credit card or accepted payment partner). You agree to maintain accurate complete, and up-to-date information in your Account. Your failure to maintain accurate and complete up-to-date Account information, including having an invalid or expired payment method on file, may result in your inability to access and use the Services or Uber's termination of these Terms with you.

34. The agreement also sets out the ways in which Uber is authorized to use personal information provided by Users and Drivers:

Our collection and use of personal information in connection with the Services is as provided in Uber's Privacy Policy located at <https://www.uber.com/legal>. Uber may provide to a claims processor or an insurer any necessary information (including your contact information) if there is a complaint, dispute or conflict, which may include an accident, involving you and a Third Party Provider (including a transportation network company driver) and such information or data is necessary to resolve the complaint, dispute or conflict.

35. At the time of the Uber Hack, Uber had two separate privacy policies in place, one for Users and one for Drivers. Uber has since amended its privacy policy and consolidated the two into one policy which came into effect on November 1, 2017. The User Privacy Policy which was in effect at the time of the Uber Hack in late 2016 sets out the ways in which Uber is authorized to use personal information provided to it by Users as well as Uber's obligations to ensure that Users' personal information is not compromised. It reads as follows:

Collection of Information

Information You Provide to Us

We collect information you provide directly to us, such as when you create or modify your account, request on-demand services, contact customer support, or otherwise communicate with us. This information may include: name, email, phone number, postal address, profile picture, payment method, items requested (for delivery services), delivery notes, and other information you choose to provide.

Information We Collect Through Your Use of Our Services

When you use our Services, we collect information about you in the following general categories:

- **Location Information:** When you use the Services for transportation or delivery, we collect precise location data about the trip from the Uber app used by the Driver. If you permit the Uber app to access location services through the permission system used by your mobile operating system ("platform"), we may also collect the precise location of your device when the app is running in the foreground or background. We may also derive your approximate location from your IP address.
- **Contacts Information:** If you permit the Uber app to access the address book on your device through the permission system used by your mobile platform, we may access and store names and contact information from your address book to facilitate social interactions through our Services and for other purposes described in this Statement or at the time of consent or collection.
- **Transaction Information:** We collect transaction details related to your use of our Services, including the type of service requested, date and time the service was provided, amount charged, distance traveled, and other related transaction details. Additionally, if someone uses your promo code, we may associate your name with that person.
- **Usage and Preference Information:** We collect information about how you and site visitors interact with our Services, preferences expressed, and settings chosen. In some cases we do this through the use of cookies, pixel tags, and similar technologies that create and maintain unique identifiers. To learn more about these technologies, please see our Cookie Statement.
- **Device Information:** We may collect information about your mobile device, including, for example, the hardware model, operating system and version, software and file names and versions, preferred language, unique device identifier, advertising identifiers, serial number, device motion information, and mobile network information.
- **Call and SMS Data:** Our Services facilitate communications between Users and Drivers. In connection with facilitating this service, we receive call data, including the date and time of the call or SMS message, the parties' phone numbers, and the content of the SMS message.
- **Log Information:** When you interact with the Services, we collect server logs, which may include information like device IP address, access dates and times, app features or pages viewed, app crashes and other system

activity, type of browser, and the third-party site or service you were using before interacting with our Services.

...

Information We Collect From Other Sources

We may also receive information from other sources and combine that with information we collect through our Services. For example:

- If you choose to link, create, or log in to your Uber account with a payment provider (e.g., Google Wallet) or social media service (e.g., Facebook), or if you engage with a separate app or website that uses our API (or whose API we use), we may receive information about you or your connections from that site or app.
- If your employer uses one of our enterprise solutions, such as Uber for Business, we may receive information about you from your employer.
- When you request on demand services, our Drivers may provide us with a User rating after providing services to you.
- If you also interact with our Services in another capacity, for instance as a Driver or user of other apps we provide, we may combine or associate that information with information we have collected from you in your capacity as a User or rider

Use of Information

We may use the information we collect about you to:

- Provide, maintain, and improve our Services, including, for example, to facilitate payments, send receipts, provide products and services you request (and send related information), develop new features, provide customer support to Users and Drivers, develop safety features, authenticate users, and send product updates and administrative messages;
- Perform internal operations, including, for example, to prevent fraud and abuse of our Services; to troubleshoot software bugs and operational problems; to conduct data analysis, testing, and research; and to monitor and analyze usage and activity trends;
- Send or facilitate communications (i) between you and a Driver, such as estimated times of arrival (ETAs), or (ii) between you and a contact of yours at your direction in connection with your use of certain features, such as referrals, invites, split fare requests, or ETA sharing;

- Send you communications we think will be of interest to you, including information about products, services, promotions, news, and events of Uber and other companies, where permissible and according to local applicable laws; and to process contest, sweepstake, or other promotion entries and fulfill any related awards;
- Personalize and improve the Services, including to provide or recommend features, content, social connections, referrals, and advertisements.
- We may transfer the information described in this Statement to, and process and store it in, the United States and other countries, some of which may have less protective data protection laws than the region in which you reside. Where this is the case, we will take appropriate measures to protect your personal information in accordance with this Statement.

Sharing of Information

We may share the information we collect about you as described in this Statement or as described at the time of collection or sharing, including as follows:

Through Our Services

We may share your information:

- With Drivers to enable them to provide the Services you request. For example, we share your name, photo (if you provide one), average User rating given by Drivers, and pickup and/or drop-off locations with Drivers;
- With other riders if you use a ride-sharing service like UberPOOL; and with other people, as directed by you, such as when you want to share your estimated time of arrival or split a fare with a friend;
- With third parties to provide you a service you requested through a partnership or promotional offering made by a third party or us;
- With the general public if you submit content in a public forum, such as blog comments, social media posts, or other features of our Services that are viewable by the general public;
- With third parties with whom you choose to let us share information, for example other apps or websites that integrate with our API or Services, or those with an API or Service with which we integrate; and

- With your employer (or similar entity) and any necessary third parties engaged by us or your employer (e.g., an expense management service provider), if you participate in any of our enterprise solutions such as Uber for Business.

Other Important Sharing

We may share your information:

- With Uber subsidiaries and affiliated entities that provide services or conduct data processing on our behalf, or for data centralization and / or logistics purposes;
- With vendors, consultants, marketing partners, and other service providers who need access to such information to carry out work on our behalf;
- In response to a request for information by a competent authority if we believe disclosure is in accordance with, or is otherwise required by, any applicable law, regulation, or legal process;
- With law enforcement officials, government authorities, or other third parties if we believe your actions are inconsistent with our User agreements, Terms of Service, or policies, or to protect the rights, property, or safety of Uber or others;
- In connection with, or during negotiations of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or into another company;
- If we otherwise notify you and you consent to the sharing; and in an aggregated and/or anonymized form which cannot reasonably be used to identify you.

36. The Uber Driver Privacy Policy which was in effect at the time of the Uber Hack provided that Uber may use the information provided by a Driver in one of the following circumstances:

Collection of Information

Uber may collect personal information from or about you when you create an account for, and use, the Uber Services, including location data, which information may be stored, processed, and/or accessed by Uber, as well as its service providers, for business purposes, including for marketing, lead generation, service development and improvement, analytics, industry and market research, and such other purposes consistent with Uber's and its Affiliates' legitimate business needs. By submitting information to Uber during the account creation process

and/or by using the Services, you consent to such collection and use of personal data.

Disclosure of Driver Information to Third Parties

Subject to all applicable laws, Uber may provide to a third party any information (including personal data and any Uber Data) about Drivers provided hereunder if: (a) there is a complaint, dispute or conflict, including an accident, relating to a Driver; (b) it is necessary to enforce the terms of the driver agreement; (c) it is required, in Uber's sole discretion, by applicable law, regulation, ordinance, license, or operating agreement; (d) it is necessary, in Uber's sole discretion, to protect the safety, rights, property, or security of Uber, the Uber Services, or any third party; to detect, prevent or otherwise address fraud, security or technical issues; and/or to prevent or stop activity which Uber, in its sole discretion, considers to be, or to pose a risk of being, illegal, unethical, or legally actionable.

37. The User and Driver Privacy Policies formed an integral part of the agreements between the Plaintiff and the proposed Class Members and Uber. Prior to the Uber Hack, the precise date of which is yet unknown to the Plaintiff, Uber breached the terms of the agreement and its obligations under the privacy policies by transferring bulk personal information data of Users and Drivers to a third part cloud-based service. Uber did not notify the Class Members of its intention to share their personal information with a third party, let alone store it on an inherently unsecure cloud-based service. Needless to say, at no time did Uber obtain the consent of the Plaintiff or other Class Members for disclosing and using their personal information in this manner.
38. The transfer and storage of the information on a third party cloud-based service was done *en masse* and was unrelated to the provision of Uber services to Users and/or Drivers. It was also not done in an anonymized manner and no steps were taken to protect the identities of Users and Drivers. Further, the transfer of the personal information and its ongoing storage on the third party cloud-based service was not done in the context of a specific complaint or legal dispute. It was entirely unnecessary and was done with total disregard to the privacy interests of Uber Users and Drivers. As such the Defendants' conduct constituted an unauthorized and unlawful disclosure of Class Members' personal information to a third party in violation of the terms of the agreement, including the Defendants' privacy policies.
39. A second and ongoing breach of contract was committed by Uber subsequent to its learning of the Uber Hack in or around October 2016. After learning of the hack and the theft of personal information of at least 57 million Users and Drivers worldwide, including the Proposed Class Members, Uber chose to conceal the matter from Uber Users and Drivers as well as regulators, thereby depriving affected individuals the ability to take appropriate actions to secure their personal information and limit their exposure

to economic and other injuries, including but not limited to identity and credit card theft.

40. Instead Uber chose to pay off the criminal hackers a sum of \$100,000 in order to avoid the embarrassment of having its own failure and data breach being made public. By doing so, Uber put its own corporate interests before the privacy interests of the Plaintiff and other Class Members. In its amended Privacy Policy which came into effect on November 1, 2017, approximately 3 weeks before the Uber Hack was uncovered by the media, Uber commits to the following:

At Uber we care about you & the trust you give us. When you use Uber, you trust us with your information. We are committed to keeping that trust... This policy applies to any users of the services of Uber or its affiliates anywhere in the world, and to anyone else who contacts Uber or otherwise submits information to Uber, unless noted below. **This includes those who use Uber or its affiliates' services to:**

- Request or receive transportation (riders)
- Provide transportation individually or through partner transportation companies (driver partners)
- Request deliveries of food or other items (delivery recipients)
- Any other user of Uber's services (including apps, websites and API), and anyone else who contacts Uber or otherwise submits information to Uber, unless subject to a separate privacy policy, notice or agreement such as the Uber Freight Privacy Policy.

(Emphasis in original)

41. The ongoing concealment of the unauthorized transfer and storage of Class Members' personal information on a third party cloud-based service, as well as the concealment of the eventual theft of that information from the third party service, constitutes a separate breach of contract under both the previous and current privacy policies.
42. To sum, upon submitting personal information to Uber, whether as a User, Driver or otherwise, a contract was established between the Plaintiff and Class Members and Uber. It was a term of that contract, express or implied, that when Class Members provided the Defendants with their personal information:
- (a) the Defendants would treat the personal information as confidential;
 - (b) the Defendants would handle the personal information of the Class Members in accordance with its established privacy policy;

- (c) the Defendants would treat the personal information of Class Members in accordance with all legislation and regulations governing the collection, storage, disclosure and use of personal information;
- (d) the Defendants would not disclose the personal information of Class Members without their consent, except as provided under the contract and privacy policy;
- (e) the Defendant would protect the personal information of Class Members from being compromised, including loss or theft;
- (f) The Defendants would take necessary steps to ensure Class Members are not put at risk as a result of providing Uber with current and accurate personal information; and
- (g) Such further and other terms as may be proved at the Trial of this Action.

43. The Defendants breached the contractual duties owed to the Class Members.

Negligence, Breach of Confidence and Invasion of Privacy

- 44. The Defendants failed to or refrained from using appropriate and up-to-date data security programs and/or technology and/or procedures to protect the personal information of the Plaintiff and Class Members.
- 45. The Defendants failed to or refrained from using appropriate and up-to-date back-up programs and/or technology and/or procedures to protect the personal information of the Plaintiff and Class Members.
- 46. The personal information provided by the Class Members to the Defendants was collected and maintained in digital form by the Defendants, using various storage devices and programs.
- 47. The Defendants failed to maintain the personal information of the Class Members in a secure fashion. Specifically, the Defendants negligently and unlawfully disclosed the personal information of the Class Members to a third party and authorized its storage on a cloud-based service. The Defendants knew or ought to have known that storing sensitive personal information in this manner would make it vulnerable to being accessed by unauthorized third parties and theft.
- 48. The Defendants failed to utilize adequate security measures and technologies to ensure that the personal information of the Class Members would remain safe and secure from loss, theft or unauthorized third parties.
- 49. The digital information security programs utilized by the Defendants, namely the use of a third party cloud-based service to maintain the personal information of the Class

Members, were inadequate and eventually led to that personal information falling into the hands of the Cybercriminals.

50. The Defendants were negligent because they failed to maintain a reasonable standard of care in safeguarding the personal information entrusted to it by the Class Members.
51. The Defendants owed each of the Class Members a duty of care to ensure that the personal information of each Class Member remained confidential and was not released, disclosed or otherwise made available to third parties, unless expressly authorized under the agreement with the Class Members or otherwise consented to by each Class Member.
52. The Defendants also owed a duty of care to each Class Member because the personal information of each individual Class Member was unique to that Class Member. Further, the personal information pertained to the identity and financial interests of each Class Member.
53. There was a sufficient relationship of proximity between the Plaintiff and Class Members and the Defendants to establish a duty of care because:
 - (a) There was a direct exchange of personal information by the Plaintiff and Class Members to the Defendants, which was required by the Defendants;
 - (b) It was reasonable for the Plaintiff and Class Members to expect that the Defendants would implement adequate safeguards to ensure that the personal information provided by the Plaintiff and Class Members would be safeguarded by the Defendants; and
 - (c) Such further and other factors as may be referred to and proved at Trial of this Action.
54. The Defendants were reckless in sharing and authorizing the storage of the Plaintiff and Class Members' personal information on a third party cloud-based service. Further, the Defendants were reckless in their failure to properly store, maintain and secure the personal information of Class Members, including the failure to maintain, update and implement appropriate digital security policies, procedures and technology, and appropriate digital back-up policies, procedures and technology.
55. The Defendants failure to properly collect, store and maintain the personal information of the Class Members was the result of operational negligence and recklessness, including a failure to maintain, update and implement proper digital security policies and safeguards. The Defendants' reckless and negligent conduct exposed the Class Members to harm. Specifically, the harm suffered by the Class Members, the theft of their personal information and the consequences that flow therefrom, was a reasonably foreseeable consequence of the Defendants' negligence.

56. In addition, the Defendants' response to the Uber Hack and the theft of Class Members' personal information constitutes reckless behavior which exposed Class Members to further harm. In an attempt to avoid the bad publicity that would follow from exposure of the Uber Hack, and the Defendants' failure to properly protect the personal information of Uber Users and Drivers, the Defendants chose to pay the criminals in order to conceal the theft. In doing so the Defendants aligned themselves with the criminals who stole the personal information of Class Members and showed willful and wanton disregard to the Class Members privacy interests and legal rights.

Breaches of Statutory Duties

Personal Information Protection and Electronic Documents Act and Personal Information Protection Act

57. The information provided to the Defendants, at their request, by Class Members and which was collected, maintained, used and/or disclosed by Uber constitutes personal information pursuant to the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*"PIPEDA"*] and the *Personal Information Protection Act*, SA 2003, c P-6.5 [*"PIPA"*]. The Defendants were subject to the duties prescribed therein for the collection, maintenance, use and/or disclosure of the Class Members' personal information.
58. Under both *PIPEDA* and *PIPA* the Defendants had a duty to protect the personal information it had obtained from Class Members.
59. The Defendants failed to protect the personal information of Class Members by failing to implement and enforce privacy policies, practices and protocols as well as security safeguards appropriate to the sensitivity of the information.
60. Specifically by disclosing personal information of Class Members and maintaining it on a third party cloud-based service, without obtaining the consent of Class Members, the Defendants breached their obligations pursuant to ss. 6.1 and 7 of *PIPEDA*.
61. The Defendants' failure to develop and implement appropriate policies, procedures and technology to protect the personal information of Class Members constitutes a breach of ss. 5 and 6 of *PIPA*.
62. Further, the Defendants contravened ss. 7-8 of the *PIPA* by failing to obtain the consent of Class Members prior to disclosing their personal information to the third party cloud-based service.
63. The Defendants' actions and/or failure to protect the personal information of Class Members constitute a breach of their obligations pursuant to ss. 17, 19-20 and 34 of *PIPA*. The Defendants' failures to meet their obligations under *PIPA* led to the unauthorized disclosure and theft of Class Members' personal information.

64. In addition, after learning about the Uber Hack the Defendants failed to notify the Information and Privacy Commissioner pursuant to s. 34.1(1) and (2) of *PIPA* and/or the Plaintiff, Class Members and other affected parties.

***Fair Trading Act* and Equivalent Consumer Protection Statutes**

65. The Plaintiff and Uber are located in Alberta for the purposes of the *Fair Trading Act*, RSA 2000, c F-2 (the "*FTA*").
66. The Defendants took advantage of the Class Members' inability to fully understand the terms and conditions imposed by the Defendants, including the ways in which the Defendants in fact collected, stored, disclosed and used their personal information. The Defendants concealed material facts from Class Members, thus making misleading and deceiving representations regarding the security of the personal information they had provided Uber. As such, the Defendants' acts and/or omissions as described above constitute an unfair practice and a breach of s. 6 of the *FTA*.
67. Further, the Defendants' ongoing failure to notify Class Members that their personal information has been compromised constitutes a continuing breach of the Defendants' duties and obligations as described above.

Damages – Particulars

68. The Plaintiff and the Class Members claim that the Defendants are liable and responsible for damages sustained through its breach of privacy of each Class Member.
69. As a consequence of the Defendants' acts or omissions, as described above and which will be further particularized prior to Trial, the Plaintiff and all Class Members have suffered significant loss and damages including harm and injury to their interests, all of which were the direct result of the unauthorized disclosure and theft of their personal information and its subsequent concealment by the Defendants.
70. As a result of the Defendants' acts or omissions, the Plaintiff and all Class Members are continuously exposed to ongoing risk of identity theft and economic loss.
71. As a result of the Defendants' acts or omissions, the Plaintiff and Class Members have suffered harm for which they claim damages. The Plaintiff and Class Members suffered and will continue to suffer injuries including the unauthorized release, disclosure and use of their personal information, including sensitive financial information. The Plaintiff and Class Members will incur expenses for credit reporting, credit monitoring services, credit counselling, identity theft monitoring services, identity theft protective services and additional services. The Class Members have also been forced to expend time and resources to investigate the theft of their personal information and take steps to address the risks arising therefrom.

72. The Plaintiff pleads that the Defendants' conduct as particularized above was willful, reckless, wanton, negligent, callous and in total disregard for the security and rights of the Plaintiff and Class Members, and was indifferent to the consequences of their acts and/or omissions and, as such, renders the Defendant liable to pay punitive and aggravated damages.
73. The Defendants' acts, omissions, wrong doings, breaches of legal and/or statutory duties or other obligations have materially contributed to the Plaintiff and Class Members injuries, economic loss or damages.
74. The Plaintiff and Class Members have suffered injury, economic loss, or damages arising from the aforesaid acts, omissions, wrong-doing, breaches of legal or statutory duties, or other obligations.

A Class Proceeding is Appropriate

75. All of the Class Members have in common that they provided the Defendants their personal information prior to October 2016 and have suffered a loss as a result of the Defendants' failure to protect their personal information. Therefore the act or omission that has given rise to their loss is identical. Further, the Defendants owed all Class Members the same duties and obligation to protect their personal information. The terms and conditions for all Class Members were uniformly imposed by the Defendants. Likewise, all Driver Class Members and User Class Members were required to provide the same personal information respectively.
76. There are questions of law and fact that are common to the Class Members which predominate over potential questions affecting only individual Class Members. Common questions include, but are not limited to the following:
 - (a) Did the Defendants breach their obligations to protect the Class Members' personal information under the contract with the Class Members?
 - (b) Did the Defendants owe a duty of care to the Class Members in relation to the collection, storage, disclosure and use of the personal information they collected from the Class Members? If so did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that breach?
 - (c) Did the Defendants have a duty to maintain the confidence of the Class Members as a consequence of the Defendants' collection, storage and use of their personal information? If so, did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that breach?

- (d) Did the Defendants owe the Class Members a duty to protect their personal information pursuant to *PIPEDA*? If so, did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that statutory breach?
 - (e) Did the Defendants owe the Class Members a duty to protect their personal information pursuant to *PIPA*? If so, did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that statutory breach?
 - (f) Did the Defendants have a duty to notify the Commissioner that the personal information of Class Members was compromised once they learned of the Uber Hack pursuant to *PIPA*? If so, did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that statutory breach?
 - (g) Did the Defendants owe the Class Members a duty to refrain from engaging in unfair practices, including but not limited to a duty to advise Class Members about all material facts relating to the collection, storage, disclosure and use of their personal information pursuant to the *FTA*? If so, did the Defendants breach that duty? If so, was it reasonably foreseeable that the Class Members would suffer harm as a result of that statutory breach?
 - (h) If it is established that the Defendants breached any of its duties referred to above, are the Class Members entitled to an award of damages? If so, what is the appropriate quantum of damages? If so, are the Class Members entitled to an aggregate assessment of damages for part or all of the damages they suffered? If so, which part of the damages? How will the damages be distributed among the Class Members?
 - (i) Are the Class Members entitled to punitive and/or aggravated damages? If so, in what amount?
 - (j) Should the Defendants be ordered to pay pre-judgment interest?
 - (k) Should the Defendants pay the cost of administering and distributing recovery? If so, in what amount?
77. A determination of the common issues will substantially advance the proceeding even though some individual issues may remain to be determined.
78. The Class is composed of an unknown number of Uber Users and Drivers and persons who provided Uber their personal information. The identity of each affected Class Member is known to the Defendants. The identities of the Class Members will be easily ascertained using the Defendants' records.

79. Class Members, are individuals, cannot match the resources of the Defendants. The individual claims of each Class Member would not be economical to pursue individually. The Class Members would be denied access to justice in the absence of a class proceeding.
80. It is unlikely that an individual Uber User or Driver could or would seek prospective relief to deter future misconduct by the Defendants. The Defendants are sufficiently large and well-resourced that an individual lawsuit would be unlikely to have any significant impact on their policies, procedures and practices. This class proceeding will impact the Defendants such that they will have to ensure that their policies, procedures and practices are sufficient to protect the personal information of Uber Users and Drivers.
81. This class proceeding is an appropriate method for the fair and efficient adjudication of the issues and of achieving fairness and justice without over-burdening the Court system with a multiplicity of individual claims. The prosecution of potentially hundreds of thousands of individual claims would be inefficient and would create the risk of conflicting decision on the same facts and issues.
82. All of the Class Members have in common that they suffered a loss as a result of the Defendants' failure to protect their personal information and their failure to notify them that their personal information had been compromised. Members of the Class are so numerous that joinder of individual claims in a single action is not practical. As such, a class proceeding is the most efficient, economical and fair method of proceeding under the circumstances.
83. Once the identity of all Class Members is known they can be notified of the commencement of this Class Action directly through the Defendants own network, through advertisements in newspapers and other media, through social media and other methods for providing notice as this Honourable Court may deem appropriate under the circumstances. The Plaintiff and Class Members shall request that the Defendants bear the cost of this notice program.
84. The Plaintiff is committed to prosecuting this Class Proceeding and has retained competent counsel experienced in Class Action litigation. The Plaintiff's claim is typical of the claim or other Class Members and on the common issues, and she has no interest which is in conflict with other Class Members.
85. The Plaintiff will fairly and adequately protect the interests of the other Class Members.
86. The Representative Plaintiff and Class Members propose the Trial of the common issues take place at the Calgary Court Centre in the City of Calgary, in the Province of Alberta.
87. The Representative Plaintiff and Class Members plead and rely on the *CPA*, the *Alberta Rules of Court*, *Alta Reg 124/2010*, *PIPEDA*, *PIPA* and the *FTA*.

Punitive Damages

88. The conduct of the Defendants merits punitive damages in that the conduct constituted high-handed, malicious and reprehensible conduct that departs to a marked degree from the standards expected of them.

Real and Substantial Connection to Alberta

89. The Plaintiff proposes to serve this claim on the Defendants, Uber B.V. and Rasier Operations B.V. outside of Alberta. Service outside of Alberta is necessary, and permitted pursuant to Rule 11.25(1), (2) and (3) of the Alberta *Rules of Court*, Alta Reg 124/2010 in that the Defendants, Uber B.V. and Rasier Operations B.V., are incorporated outside of Alberta, and there is no head office or address for service in Alberta or Canada.
90. Where this claim is served on Defendants outside of Alberta, it will be served on the basis that a real and substantial connection exists between Alberta and the facts on which the claim is based. That connection arises from the following:
- (a) A contract was made, performed and breached in Alberta;
 - (b) A tort was committed in Alberta:
 - (i) Uber services were provided to the Plaintiff in Alberta;
 - (ii) The Plaintiff is a resident of the Province of Alberta. The breach of the Defendants' duties and obligations led to the unlawful and unauthorized disclosure of the Plaintiff's personal information;
 - (c) The Defendants distribute, market, promote and sell the Uber services in Alberta, and derive revenue from such distribution;
 - (d) The Defendants, Uber B.V. and Rasier Operations B.V., although outside of Alberta, are necessary and proper parties to the action brought against Uber Canada Inc. and Uber Technologies Inc., who will be served in Alberta; and
 - (e) The claim relates to a breach of contract in Alberta.

Remedy sought:

91. The Representative Plaintiff and Class Members seek:

- (a) An Order pursuant to the *CPA* certifying this action as a class proceeding and appointing the Plaintiff as the representative of a class to be certified by the Court;
- (b) A finding that the Defendants breached the contract as between the Defendants and the Class Members;
- (c) A finding that the Defendants contravened their statutory duties under *PIPEDA*;
- (d) A finding that the Defendants contravened their statutory duties under *PIPA* and the equivalent provisions in other jurisdictions across Canada;
- (e) A finding that the Defendants engaged in unfair practices contrary to the *FTA* and the equivalent provisions in other jurisdictions across Canada;
- (f) A finding that the Defendants committed breaches of confidence and an invasion of privacy;
- (g) An award of damages in an amount to be proven at Trial comprised of one or more of the following:
 - (i) Damages for breach of contract;
 - (ii) Damages for breach of the Defendants' statutory duties under *PIPEDA*;
 - (iii) Damages for breach of the Defendants' statutory duties under *PIPA*;
 - (iv) Damages for breach of the Defendants' duty of care owed to Class Members;
 - (v) Damages for breach of confidence;
 - (vi) Damages for invasion of privacy;
 - (vii) General damages;
 - (viii) Aggravated damages;
 - (ix) Punitive damages;
 - (x) Special damages and out-of-pocket incurred by the Plaintiff and Class Members, including:
 - (A) Costs of credit counselling;
 - (B) Compensation for lost time and/or loss of income;

- (C) Costs associated with or incurred for credit monitoring services, identity theft monitoring services, identity theft protective services and additional services;

Or such other amount as may be proven at Trial or as the Court may deem just and appropriate in the circumstances;

- (h) An order, pursuant to s. 30 of the *CPA* directing an aggregate monetary award;
- (i) An order, pursuant to s. 32 of the *CPA* allowing for the use of standard claim forms or other documentary evidence or such other procedure as warranted under the circumstances;
- (j) An order that the damages be paid by the Defendants into a common fund and distributed to the Class Members in an appropriate manner as directed by the Court;
- (k) An order or declaration that the Defendants take specific steps to:
 - (i) Implement and enforce appropriate privacy policies;
 - (ii) Implement and enforce protocols or procedures regarding the manner of storage and use of personal information of Uber Users and Drivers;
 - (iii) Ensure internal compliance with privacy policies, procedures and protocols and the need for appropriate technologies for the purposes of protecting personal information of Uber Users and Drivers;
 - (iv) Ensure internal compliance with privacy policies, procedures and protocols by employees, agents, servants and third parties engaged by the Defendants for the purposes of collecting, storing, maintaining and/or using personal information of Uber Users and/or Drivers;
 - (v) Educate, train and supervise employees, agents, servants and third parties engaged by the Defendants for the purposes of collecting, storing, maintaining and/or using personal information of Uber Users and/or Drivers on the privacy policies, procedures and protocols;
 - (vi) Implement spot audits;
 - (vii) Ensure timely reporting of privacy breaches to affected individuals and the Office of the Privacy Commissioner; and
 - (viii) Ensure personal information of Uber Users and Driver are safely stored and appropriately encrypted and password protected;

- (l) Pre-judgment interest and post-judgment interest;
 - (m) The costs of this action on a substantial indemnity basis;
 - (n) The costs of administering the plan of distribution of the recovery in this action;
92. Such further and other relief as may be required and as this Honourable Court deems to be just and appropriate in the circumstances.

NOTICE TO THE DEFENDANT(S)

You only have a short time to do something to defend yourself against this claim:

20 days if you are served in Alberta

1 month if you are served outside Alberta but in Canada

2 months if you are served outside Canada.

You can respond by filing a statement of defence or a demand for notice in the office of the clerk of the Court of Queen's Bench at CALGARY, Alberta, AND serving your statement of defence or a demand for notice on the plaintiff's(s') address for service.

WARNING

If you do not file and serve a statement of defence or a demand for notice within your time period, you risk losing the law suit automatically. If you do not file, or do not serve, or are late in doing either of these things, a court may give a judgment to the plaintiff(s) against you.