

CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

N°: 500-06-000902-185

(Class Action Division)

SUPERIOR COURT

PIERRE-OLIVIER FORTIER, 


Plaintiff

v.

UBER CANADA INC., legal person with an establishment at 1751 Richardson Street, suite 7120, Montreal, Quebec, H3K 1G6

– and –

UBER TECHNOLOGIES INC., legal person (...) with its principal establishment at 1455 Market Street, suite 400, in San Francisco, in California, United States 94103

– and –

UBER B.V., legal person with an establishment at Mr. Treublaan 7, 1097 DP, Amsterdam, Netherlands

– and –

RASIER OPERATIONS B.V., legal person with an establishment at (...) Mr. Treublaan 7, 1097 DP, Amsterdam, Netherlands

– and –

UBER PORTIER B.V., legal person with an establishment at Mr. Treublaan 7, 1097 DP, Amsterdam, Netherlands

Defendants

AMENDED APPLICATION FOR AUTHORIZATION TO EXERCISE A CLASS ACTION AND TO BE APPOINTED AS REPRESENTATIVE PLAINTIFF
(Articles 574 and following of the *Code of Civil Procedure*)

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT OF QUEBEC, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PLAINTIFF STATES THE FOLLOWING:

I. INTRODUCTION

1. The Plaintiff seeks from this Honourable Court the authorization to exercise a class action on behalf of all people who are part of the two subclasses described below (together, the “**Class Members**”):

“All persons residing in Quebec that, as users, provided personal information to Uber that was collected, held, retained and used by Uber and disclosed without authorization to a third party in October 2016.”

-and-

“All persons residing in Quebec that, as drivers, provided personal information to Uber that was collected, held, retained and used by Uber and disclosed without authorization to a third party in October 2016.”

2. This Application is in response to events that occurred in October 2016 when personal information provided by the Class Members (hereinafter, “**Personal Information**”) collected, held, retained and used by Uber (as defined below at para. 20) was made accessible to unauthorized persons, namely, hackers (collectively, the “**Hackers**”).
3. In support of his Application, the Plaintiff alleges that the Defendants are solidarily liable towards the Class Members for the following faults:
 - i) Failing to previously inform the Class Members of the fact that their Personal Information was communicated to others, namely, an unauthorized third party and kept in a manner not provided for in the contract binding them to Uber;
 - ii) Having disclosed to an unauthorized third party the Personal Information of the Class Members for an unauthorized purpose, without having previously obtained their consent;

- iii) Failing to have taken the necessary and adequate security measures to protect the Personal Information provided by the Class Members, given the sensitivity and the mass of Personal Information;
 - iv) Having intentionally concealed the hacking of the Personal Information for over a year, preventing the Class Members from taking the means necessary in order to avoid their Personal Information from being compromised again or having their identity stolen;
 - v) Having put their own interests before the rights and interests of the Class Members to their private lives and the confidentiality of their Personal Information;
 - vi) Having breached their obligations and failed in their general duty of prudence and diligence;
 - vii) Having breached the applicable legal obligations relating to the collection, holding, retention, use and communication of Personal Information of the Class Members;
 - viii) Having breached the *Consumer Protection Act (...)* by making false representations to Uber users;
 - ix) Having violated the fundamental right to a private life protected by the *Charter of Human Rights and Freedoms*;
4. The Plaintiff seeks, in his name and on behalf of the Class Members, the collective recovery of the following damages:
- i) a sum in moral damages, to be detailed at trial;
 - ii) a sum in pecuniary damages, to be detailed at trial;
 - iii) \$10,000,000 in punitive damages for the unlawful and intentional interference with the Class Members' rights by the Defendants, to be detailed;
 - iv) interest at the legal rate and the additional indemnity provided for at article 1619 of the *Civil Code of Québec*;
 - v) legal costs, including expert fees, if applicable, and fees related to the publication and notice, in an amount to be determined at the hearing.

II. THE PARTIES

A) THE PLAINTIFF

5. The Plaintiff is an actor who lives and works in Montreal.
6. He is also very involved in the *Union des artistes*, as a representative in the negotiation of collective agreements.
7. The Plaintiff does not have a car and uses exclusively public transit, bicycle, car-sharing and taxi services to travel around the city.
8. On November 17, 2013, the Plaintiff signed up for the transportation services offered by Uber and downloaded the Uber mobile application, as a user.
9. As of his registration as a user, the Plaintiff was required, pursuant to Uber's user terms of use, to provide his name, address, telephone number, email address as well as his payment information, namely, his credit card number.
10. Following his registration as a user, the Plaintiff was also required by Uber, in case of any changes, to regularly update this information, in order to continue to use the transportation services and the Uber application.
11. Since he began using the Uber application, other Personal Information of the Plaintiff's has also been collected by Uber.
12. The Plaintiff had the right to expect that his Personal Information would be collected, held and retained by Uber in a secure manner, namely given the terms of use of the Uber service, including Uber's privacy policy in force at the time, as well as Uber's articles and by-laws.
13. On or around November 21, 2017, the Plaintiff became aware for the first time that his Personal Information had been communicated by Uber, and retained and held by an unauthorized third party, and that Uber had been hacked in 2016, when this hack was reported in various media outlets.
14. In fact, before November 21, 2017, he had absolutely no knowledge of these facts, not having been advised of either the hack that Uber experienced in 2016 nor the fact that any of his Personal Information that he provided was at all compromised.
15. What is more, the Plaintiff was not, at any time to this date, informed by Uber of the (...) situation relating to his Personal Information.
- 15.1. It is only on March 12, 2018 that the Plaintiff finally received notice from Uber that his Personal Information had been hacked in 2016.

B) THE DEFENDANTS

16. The defendant *Uber Canada Inc.* is a company duly incorporated under the *Canada Business Corporations Act*, RSC 1985, c C-44, and whose offices are located at 100 King Street West, suite 6200, Toronto, Ontario carrying on its activities in Quebec under the name Uber Canada Inc. and having a principal establishment in Quebec at 1751 Richardson Street, suite 7120, Montreal, Quebec, H3K 1G6, as appears from an extract of the Quebec corporate register, disclosed in support hereof as **Exhibit P-1**.
- 16.1. *Uber Canada Inc.* is responsible for marketing and administrative support for Uber B.V. for the Uber applications in Canada as well as technical support offered to Uber users and drivers in Canada and in Quebec.
17. The defendant Uber Technologies Inc. is a company duly incorporated under the laws of (...) Delaware, whose head office is located in San Francisco in the United States and is the company that developed, distributed and operated the Uber applications for smartphones, which put Uber users and drivers in contact. It also operates the site www.uber.com, which is accessible from Quebec.
18. The defendant Uber B.V. is a company duly incorporated under the laws of the Netherlands, with its head office located in Amsterdam and is the company that makes available the smartphone applications to Uber users and drivers allowing them to be in contact in the province of Quebec, as well as the company that holds and uses the intellectual property relating to these applications. It is also the entity that controls the Personal Information at issue.
19. The defendant Rasier Operations B.V. is a company duly incorporated under the laws of the Netherlands, with its head office also located in Amsterdam and is the company that grants the limited access licenses for the Uber applications in Canada. Rasier Operations B.V. has an individual contract with each user and driver, including those in Quebec.
- 19.1. Uber Portier B.V. is also a company duly incorporated under the laws of the Netherlands and whose head office is located in Amsterdam and is the company that grants the limited access licenses for the UberEATS application.
20. At all times relevant to the period of this class action, the defendants Uber Canada Inc., Uber Technologies Inc., Uber B.V. (...), Rasier Operations B.V. and Uber Portier B.V. (collectively, “Uber”), acted jointly in the carrying out of their activities and the conduct of their business.

III. THE FACTS GIVING RISE TO THIS APPLICATION

- 20.1. Personal information is a valuable commodity for identity thieves. Once this information has been compromised, criminals can sell it on the “cyber black market” for several years. Following recent large-scale data breaches, identity

thieves and cybercriminals have shared personal information directly on various websites on the “dark web”, making this information public.

21. This action is being undertaken by the Plaintiff who, as is the case with all Class Members, provided his Personal Information to Uber.
22. Uber, due to its carelessness and negligence, made this Personal Information accessible to unauthorized third parties around October 2016.
23. Making the situation worse, Uber voluntarily concealed this unauthorized disclosure for more than a year, choosing instead to transact with the Hackers instead of advising the Plaintiff and the Class Members that their Personal Information had been compromised, thus increasing the risk that the Plaintiff and Class Members are once again subject to a theft of their Personal Information in the future.
- 23.1. Uber’s conduct is offensive, immoral, unethical and unscrupulous and has caused and continues to cause injury to the Plaintiff and the Class Members.

A) THE SERVICES OFFERED BY UBER

24. Uber is a multinational corporation which offers transportation services in 83 countries as well as more than 673 cities around the world.
25. Uber’s transportation services are offered in Canada and, namely, in Quebec since at least 2013.
26. In Quebec, Uber’s transportation services are offered in the cities of Montreal and Quebec.
27. Once registered as a user, anyone, after downloading the Uber application, can use it anywhere in the world where Uber services are offered.
28. The transportation services offered by Uber in Quebec include, without limitation, UberEATS, UberX, UberXL and UberSelect.
29. UberEATS is a delivery service through which a user can order food from a participating restaurant.
30. UberX is a transportation service that can accommodate up to four people in a standard vehicle, such as a sedan with four or five doors.
31. UberXL is a similar service to that offered by UberX, but offers larger vehicles, such as SUVs.
32. Finally, UberSelect is a transportation service that resembles the other services, but offers high-end vehicles.

33. The services in this vast transportation network are provided through the same mobile application, except UberEATS which is provided through its own application. (For the purposes of this Application, we refer collectively to all of these services as the “**Uber Application**”).

B) THE COLLECTION OF PERSONAL INFORMATION BY UBER

34. In order to access all of these services, a person must first download the Uber Application and accept Uber’s terms of use.
35. Uber operates three mobile Applications:
- i) The Uber Application for users;
 - ii) The Uber Application for drivers;
 - iii) The UberEATS Application.
36. Uber users use the first of these applications to plan and order a ride, check on their ride on their smartphone and facilitate the payment of the ride and evaluate the Uber drivers.
37. With respect to Uber drivers, they use their Uber Application in order to be notified of a request for a ride, obtain payment and to evaluate the passengers at the end of the ride.
38. Finally, as mentioned previously, Uber users can also, through UberEATS, order food from a participating restaurant.
39. In order to become a user, Uber requires that the person:
- i) be at least 18 years old;
 - ii) respect the conditions provided (...) in its Terms of Use, including obtaining an access and use license from the Uber Application for passengers;
 - iii) provide to Uber their name, mobile telephone number and email address as well as their payment information, namely, their credit card number;
40. The user, in accepting Uber’s terms of use, contractually binds himself to Rasier Operations B.V. to respect these terms.
41. In order to have access to the Uber Application for drivers, a person must satisfy certain conditions, that is, namely, to be 21 years old or older, (...) provide a valid driver’s license number, provide proof of registration and (...) proof of insurance.

42. In the case of Uber drivers, they must also provide proof of eligibility to work in Canada and pass a criminal background check performed by a third party for Uber, as well as a security inspection of their vehicle.
43. If the conditions are satisfied, the driver must then accept Uber's terms of use and in doing so, contractually binds himself to Rasier Operations B.V. to respect these terms.
44. The same conditions or similar conditions must also be satisfied in order to become a user or driver for UberEATS and to obtain a limited access license from Uber Portier B.V.
45. Uber's terms of use provide the obligations of the Uber Application user – user or driver – to provide Personal Information that is accurate and up-to-date. It is a continuous obligation:

In order to use most aspects of the Services, you must register for and maintain an active personal user Services account (“Account”). You must be at least 18 years of age, or the age of legal majority in your jurisdiction (if different than 18), to obtain an Account. 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 a 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, complete, and 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.

[underlining added]

as appears from the conditions applicable to users and drivers, disclosed in support hereof as **Exhibit P-2**;

46. The Defendants could collect, hold, retain and use the Personal Information of the Plaintiff and the Class Members on their own network, in accordance with Uber's terms of use, including Uber's privacy policy applicable during the relevant periods.
47. However, Uber decided to hold and retain the Personal Information on a “Cloud”-type network owned by a third party, thus contravening its own privacy policies.
48. At no time did Uber advise the Plaintiff or the Class Members of its intention to proceed this way, and even less request their permission to do so.
- 48.1. Further, at no time did Uber advise the Plaintiff or the Class Members of the fact that it had already been subject to a hack in May 2014 affecting the names and license plate numbers of approximately 100,000 drivers, as well as certain of their account numbers and their social insurance numbers and other information similar to the information to which the Hackers had access in this case (the “2014 Hack”).

48.2. At no time did Uber advise the Plaintiff or the Class Members that it was the subject of a complaint and a consent order by the Federal Trade Commission in 2017, requiring it to establish, implement and maintain a complete program for protection of personal information, due to its failure to have a satisfactory program in place, as appears from a copy of the complaint and the decision of the Federal Trade Commission in 2017 against Uber, disclosed in support hereof as **Exhibit P-5**, *en liasse*.

C) THE HACK OF PERSONAL INFORMATION

49. Around the month of October 2016, two individuals, the Hackers, illegally accessed through the “Cloud”-type network belonging to the unauthorized third party, the Personal Information provided by approximately 57,000,000 individuals throughout the world (the “**Hack**”).
50. Uber was notified of the Hack shortly after it happened (in November 2016) and deliberately chose to hide it from the Class Members and other persons affected – as it had done previously for the 2014 Hack –, as well as from the relevant regulatory authorities in the jurisdictions in which it operates, in order to avoid the repercussions associated with such a disclosure.
51. Rather than informing the Plaintiff and other Class Members of the Hack, thereby providing them with the opportunity to take the necessary measures to respond and to ensure the protection and surveillance of their Personal Information, Uber chose to pay the Hackers \$100,000 USD, in exchange for a promise of silence and the purported destruction of the Personal Information to which they had access.
- 51.1. Initially, Uber maintained that the payment of \$100,000 USD was a “bug bounty”, a legitimate payment to third parties to test its IT systems, a statement which was false and intentionally misleading.
52. The Uber Hack was in fact never voluntarily disclosed by Uber and was made public only by the media, one year later, on or about November 21, 2017.
- 52.1. The same day, Uber finally publicly admitted that it had been the subject of a hack in October 2016 wherein the hackers had access to the Personal Information held by Uber on the cloud server of a third party.
53. On December 11, 2017, the Office of the Privacy Commissioner of Canada announced that it was opening a formal investigation on the Uber Hack.
54. The same day, Uber announced that 815,000 Canadian drivers or users were affected by the Hack, as appears from a copy of the article published on the Radio-Canada website, disclosed in support hereof as **Exhibit P-3**.
- 54.1. On February 28, 2018, the Alberta Privacy Commissioner rendered a decision with respect to the Hack, concluding that the Hack posed a real risk of significant harm

to Uber users, and ordering Uber B.V. to notify the users of the Hack, as appears from the February 28, 2018 decision by the Alberta Privacy Commissioner, disclosed in support hereof as **Exhibit P-6.**

54.2. On March 12, 2018, approximately eighteen (18) months after the Hack, and after being ordered to do so by the Alberta Privacy Commissioner, Uber at last notified the Canadian users and drivers affected by the Hack that it had occurred, as appears from a copy of the email sent to the Plaintiff, disclosed in support hereof as **Exhibit P-7.**

54.3. This email dated March 12, 2018 exhibit P-7 confirms that the Hack lasted for over one (1) month, and included information used by Uber to operate their services, including users' name, email address, and mobile phone number and, in some cases, Uber internal user IDs, locational information, user tokens, user ratings and scores, notes by Uber personnel, passwords protected through a technical process called "hashing and salting" and drivers' payment statements.

D) THE DEFENDANTS' LIABILITY

55. The Defendants are solidarily liable for the damages that the Plaintiff and the Class Members suffered as a result of their fault, that is, all of the damages described hereinafter and other damages that will be proven at the hearing.

a) The Civil Liability of the Defendants

56. Upon accepting the terms of use established by Uber, sending their Personal Information and using the Uber services, users and drivers entered into a contractual relationship with Uber.

57. In both cases, these contracts are contracts of adhesion as set out at Article 1379 of the *Civil Code of Québec*, insofar as it is clear that the essential stipulations were imposed and drawn up by Uber and were not negotiable.

58. The terms of use, Exhibit P-2, refer specifically to Uber's privacy policy as an integral part of the contract between Uber, its drivers and its users:

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.

[underlining added]

59. Between July 2015 and November 2017, Uber had two (2) privacy policies in place, one for its users and one for its drivers, as appears from the two (2) privacy policies in place, disclosed in support hereof as **Exhibit P-4, en liasse**.
60. The privacy policy applicable to users provides the breadth of the Personal Information that could be collected by Uber directly from users, which includes a considerable quantity of Personal Information:

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.
61. The privacy policy also provides the five (5) circumstances in which Uber has the right to use the Personal Information provided by its users :
- 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.
62. Regarding the storing of the Personal Information, this same policy provides that Uber must take the “appropriate” measures in order to ensure that the Personal Information of users is not compromised or, to use the words of the policy, “protect” this Personal Information.

63. Finally, the privacy policy also provides the circumstances in which the Information provided can be communicated to a third party:

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.

[underlining added]

64. The privacy policy for Uber drivers in place between July 2015 and November 2017, Exhibit P-4, includes stipulations the contents of which are the same or extremely similar to those above relevant to this litigation.
65. Further, just as is the case with the privacy policy applicable to users between July 2015 and November 2017, it provides for Uber's obligation to take the appropriate measures in order to ensure that the drivers' Personal Information is held and retained without being compromised.
66. It also provides that this information cannot be disclosed to a third party that is not mentioned without the driver having previously been notified, given his consent and that the Information be provided to the third party in an anonymous fashion.
67. These two aspects are, by reference, explicit stipulations contained in the contracts between Uber and the Plaintiff and the Class Members.
68. Pursuant to these contracts, Uber was contractually obligated to:
 - i) treat the Personal Information provided by the Plaintiff and the Class Members in a confidential manner;
 - ii) collect, hold, retain, use and disclose this Personal Information in accordance with the privacy policy in force and solely for the reasons expressly provided therein;
 - iii) hold, retain, use and disclose this Personal Information in accordance with all applicable legislation and regulations;

- iv) not disclose the Personal Information of the Class Members without their consent, other than in the specific cases provided in the contract or the privacy policy;
 - v) ensure that the Personal Information is not compromised by any means, including by being lost or stolen;
 - vi) take the means necessary in order to ensure that the Personal Information is not at risk in any way through the fault of Uber;
 - vii) all other obligations that will be proven at trial.
69. In transferring such a significant quantity of Personal Information on a third party's online network, Uber violated the terms and conditions of the aforementioned contracts as well as its obligation under the applicable privacy policies.
70. At no moment did Uber obtain the consent of the Plaintiff or the other Class Members in order to transfer their Personal Information to a third party nor did they consent to it being transferred in such a way.
71. The transfer and retention of the Personal Information on the "Cloud"-type online server of a third party was done *en masse* and without relation to the provision of services to Uber users or drivers.
72. This transfer was also not done in an anonymous fashion or in the context where measures were taken to protect the identity of Uber users and drivers, which could have prevented their Personal Information from being compromised.
73. Moreover, the transfer of Personal Information and its continued retention on the online server of a third party were also not done for one of the reasons provided in the policy.
74. This transfer was not at all justified and was done in flagrant disregard of the rights and interests of the Plaintiff and the Class Members in respect of their private lives.
75. At the outset, the Defendants' conduct constitutes an illegal and unauthorized disclosure of the Personal Information of Class Members to a third party in violation of the terms of use of the Uber Application, including the Defendants' privacy policies applicable at the time of the event.
76. Further, this unauthorized transfer of Personal Information by Uber rendered this Personal Information inherently vulnerable to hacking, which Uber should have known or anticipated, especially considering the 2014 Hack.
- 76.1. The Plaintiff and the Class Members were never informed of this risk.

77. Technology, digital programs or tools used by the Defendants, namely the use of a “Cloud”-type online server operated by a third party to retain the Personal Information of the Class Members, were inadequate and insufficient and eventually permitted that this same Personal Information end up in the hands of the Hackers.
- 77.1. Uber hired IT employees and sub-contractors that were not qualified to ensure the safety of the Personal Information belonging to the Plaintiff and the Class Members.
78. The Defendants failed in their obligation to hold, retain and use this Personal Information in a secure fashion and to protect it against loss, theft or access by unauthorized third parties.
79. The Defendants were extremely negligent by not acting as a reasonable person in the circumstances, namely by failing to respect industry standards, and by not taking the means necessary to protect the Personal Information that was entrusted to them by the Plaintiff and the Class Members.
- 79.1. As a result of this negligence and a lack of appropriate security measures, it took the Defendants one month to detect the Hack.
- 79.2. The Defendants’ conduct allowed cybercriminals to illegally access the Plaintiff and the Class Members’ Personal Information for at least one (1) month.
80. The Defendants, by their carelessness and recklessness, made possible the Hack of the Personal Information by the Hackers.
81. Further, the response of the Defendants to the Uber Hack and to the theft of the Personal Information of the Class Members also constitutes negligent conduct that exposed the Plaintiff and the Class Members to additional prejudice.
82. In attempting to avoid the bad publicity that would have followed the disclosure of the Uber Hack, and which would have exposed the Defendants’ inability to protect the Personal Information of Uber users and drivers, the Defendants chose to pay criminals in order to hide the theft, prioritizing their interests over those of the Plaintiff and the Class Members.
83. In so doing, the Defendants were accomplices to the criminals that stole the Personal Information belonging to the Plaintiff and the Class Members and demonstrated their wanton and reckless disregard in respect of the Plaintiff and Class Members’ interests and right to a private life.
- 83.1. In so doing, the Defendants also increased the risks that the Plaintiff’s and Class Members’ Personal Information would be the subject of a future hack due to its decision to pay the Hackers \$100,000 USD, which legitimized the Hack and deprived the Plaintiff and the Class Members of the opportunity to mitigate their damages in this regard.

83.2. The Defendants thus acted in bad faith.

b) The Defendants' Obligations Pursuant to *PIPEDA*, (...) *PPIPS* and the *Civil Code of Québec*

84. The Personal Information provided by the Class Members collected, retained, used and ultimately disclosed by Uber constitutes Personal Information under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, (hereinafter "***PIPEDA***") and the *Act Respecting the Protection of Personal Information in the Private Sector*, (hereinafter "***PPIPS***"), CQLR c P-39.1.
85. In so doing, the Defendants were subject to the obligations provided by both *PIPEDA* and *PPIPS* regarding the collection, retention, use and disclosure of the Class Members' Personal Information.
86. Both pursuant to *PIPEDA* and *PPIPS*, the Defendants had a legal obligation to protect the Personal Information obtained from the Plaintiff and the Class Members and limit its use to the purposes provided in the contract between the Defendants and its users and drivers.
87. The Defendants failed in their obligation to protect this Personal Information in failing to put in place policies, practices, procedures, as well as appropriate security measures in the circumstances given the sensitive nature of the Personal Information communicated, and ensuring that they were followed.
- 87.1. The Defendants also failed in their obligation to protect this Personal Information by failing to put in place appropriate security measures that would have allowed the detection of the Hack in a timely manner.
88. More specifically, in disclosing the Personal Information of the Plaintiff and the Class Members and in retaining them on the online server of a third party, without obtaining the consent of the Class Members, the Defendants failed in their obligations pursuant to sections 6.1 and 7 of *PIPEDA*, which provide that the initial consent given by the Plaintiff and the Class Members to the collection of their Personal Information was given only for the purpose provided.
- 88.1. The Defendants failed in their obligations pursuant to section 5 and Schedule 1 of *PIPEDA*, including without limitation sections 4.7 to 4.7.4 which provide that "[p]ersonal information shall be protected by security safeguards appropriate to the sensitivity of the information".
- 88.2. The Defendants also failed in their obligation of openness pursuant to sections 4.8 to 4.8.3 of Schedule 1 of *PIPEDA*.
89. The Defendants further had the obligation to ensure, at all times, that the Plaintiff and the Class Members understood the nature, purpose and consequences of the collection, use and disclosure of the Personal Information to which they consented.

90. In the case of a change, the Defendants were obligated to notify the Plaintiff and the Class Members in order to obtain their consent again, except in the cases specifically provided.
91. However, the use and disclosure made by the Defendants herein of the Personal Information provided does not qualify in any of the categories specifically enumerated in *PIPEDA* as exceptions.
92. The failure or inability of the Defendants to set up and apply policies and procedures and use the technological means that would have permitted the protection of the Class Members' Personal Information and detection of unauthorized access also constitute a violation of section 10 *PPIPS* in that "[a] person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored."
93. The Defendants also violated sections 13 and 17 *PPIPS* in sending this Personal Information to a third party without first obtaining the Plaintiff and the Class Members' consent.
94. Furthermore, after being advised of the Uber Hack, the Defendants should have notified the Plaintiff and the Class Members of same in order to comply with their legal obligations.
95. In failing to notify the Plaintiff and the Class Members of the Hack in a timely manner, the Defendants, practically speaking, rendered ineffective the legislative and regulatory protections provided to the Plaintiff and the Class Members by the legislator.
- 95.1. Finally, this conduct also constitutes a violation of sections 35 to 37 of the *Civil Code of Québec*, including the obligation to only gather information relevant to the stated objective and not to communicate such information to third parties or use it for other purposes without the consent of the person concerned.

c) The Defendants' Obligations under the *Consumer Protection Act*

96. (...) The Defendants also failed in their obligations under section 219 of the *Consumer Protection Act*, CQLR c P-40.1, in making false and misleading representations (...) to the Plaintiff and the Class Members regarding the way in which their Personal Information would be kept.
97. In fact, the Defendants failed to disclose to the Plaintiff and the Class Members the real location where their Personal Information would be kept and the manner in which it would be kept.

97.1. Further, they made false representations regarding the level of surveillance and protection that would be exercised over the Personal Information provided by the Class Members.

97.2. Finally, in not disclosing the Hack immediately in 2016, and in characterizing the ransom paid to the Hackers as a bug bounty, when this was not at all the case, the Defendants failed to disclose an important fact regarding the safety of the Personal Information belonging to the Plaintiff and the Class Members.

98. Because of these failures, the Plaintiff and the Class Members are justified in seeking punitive damages under section 272 of the *Consumer Protection Act*.

d) The Defendants' Obligations under the *Charter of Human Rights and Freedoms*

99. The Defendants have also infringed the Plaintiff and the Class Members' right to a private life, which right is protected under section 5 of the *Charter of Human Rights and Freedoms*.

100. The Defendants did not simply fail in their contractual and legal obligations, they were grossly negligently in keeping the highly sensitive Personal Information on an unsecured online server, without taking any measures to ensure the anonymous nature of the Personal Information provided.

101. (...) The Defendants sent this Personal Information to a third party without notifying the Plaintiff or the Class Members.

102. After having learned that the Personal Information had been illegally obtained by the Hackers, the Defendants knowingly concealed this fact from the Plaintiff and the Class Members.

103. Rather than advise the Plaintiff and the Class Members that their Personal Information had been compromised, Uber instead paid the Hackers an amount of \$100,000 USD in order to avoid the embarrassment of the publicity around its own failure to protect the Personal Information and the theft of data.

104. Uber thus chose to prioritize its own corporate, economic and reputational interests to the detriment of the interests of the Plaintiff and the Class Members.

105. Ultimately, a year later, it was the media who disclosed the Uber Hack to the Plaintiff and the Class Members.

105.1. By legitimizing the Hackers' actions and making them financially profitable, Uber also increased the risk that the Personal Information belonging to the Plaintiff and the Class Members would again be the subject of a hack.

106. All of the Defendants' actions evidence their illicit and intentional interference with the Plaintiff's and the Class Members' right to a private life.
107. It also denotes a profound disregard for their rights and interests.
108. In concealing the Hack and the theft of the Personal Information of approximately 57 million users and drivers across the world in October 2016, including the Plaintiff and the Class Members, the Defendants intentionally and illegally violated the Plaintiff's and Class Members' right to a private life, giving rise to punitive damages pursuant to section 49 of the *Charter of Human Rights and Freedoms*.
- 108.1. This conduct is part of a larger intentionally wanton pattern by the Defendants in that Uber chose to conceal the 2014 Hack, preferring to hide this highly relevant information from its users and drivers, depriving them of the possibility of appreciating the risk they ran in disclosing their Personal Information to Uber.
- 108.2. Further, in its complaint in 2017, Exhibit P-5, the Federal Trade Commission chastises Uber for having falsely led people to believe that it had in place adequate safety practices, whereas in fact Uber had not put in place such adequate practices, protocols or procedures in a timely manner.

E) THE DAMAGES SUFFERED BY THE PLAINTIFF AND THE CLASS MEMBERS

109. The Plaintiff and the Class Members put forward that the Defendants are solidarily liable for the damages suffered or that resulted from their failures regarding the maintaining of the confidentiality of the Plaintiff and the Class Members' Personal Information (...), and the numerous violations of their right to a private life.
110. Due to the Defendants' acts and omissions as set out above, proof of which will be made at the hearing, the Plaintiff and the Class Members suffered moral damages as well as pecuniary damages in addition to the harm caused to their interests and their right to a private life, stemming directly from the unauthorized disclosure by Uber of their Personal Information to a third party, from the theft of this Information by the Hackers as well as the concealment of the Hack by the Defendants.
111. As a consequence of the Defendants' acts and omissions, the Plaintiff and the Class Members were continuously and are still today exposed to an abnormally high risk of phishing, identity theft and the financial losses that could result therefrom.
- 111.1. These risks are even greater considering that Hackers had access to this Personal Information for more than one (1) month and because of Uber's decision to give the Hackers a ransom that legitimized their actions and gave them a valid reason to try again.
112. Recall that the Personal Information herein was not only lost or made available unknowingly.

113. This Personal Information was rendered accessible to Hackers who chose to profit from this theft in extorting Uber further for an amount of \$100,000 USD.
114. The risk of identity theft is increased and the measures that the Plaintiff and the Class Members have to take in order to counter this risk are also greater than in the context of disclosure of Personal Information to an unauthorized third party or loss of Personal Information.
115. The amount of Personal Information provided originally and made accessible to the Hackers, that is, the name, email address, cell phone number, payment information of Uber users and, in the case of drivers, information relating to their driver's license (...), registration, profile photos and sensitive geolocation data, as well as the period of time during which the unauthorized access lasted, also increase the risk and necessarily the measures that have to be taken in order to counteract that risk.
116. This situation, namely the fact of knowing that their sensitive Personal Information is currently or was at one time or another in the hands of Hackers willing to extort, has caused the Plaintiff and the Class Members great stress.
117. The intentional concealment by Uber of the Hack also caused the Plaintiff and the Class Members to lose confidence, not only in Uber, but also in other private businesses to whom (...) they provided Personal Information over the course of the last several years which may have been disclosed to third parties and then concealed.
- 117.1. Indeed, the knowledge that their Personal Information was at risk and that Uber had already in the past been subject to a hack in 2014 was highly relevant information for the Plaintiff and the Class Members in their decision of whether to accept to disclose their Personal Information.
118. This situation also caused the Plaintiff a great deal of anxiety. He has a modest revenue and it took several years to build his good credit; an identity theft would have a significantly harmful impact on him.
119. Importantly, at no time did the Defendants inform the Plaintiff or the Class Members regarding whether measures were put in place after the Hack in order to secure the Personal Information made accessible to the Hackers, choosing instead to intentionally conceal this information until March 12, 2018.
120. In fact, irrespective of whether their identity has been stolen or not, the Plaintiff and the Class Members will be, due to the fault of the Defendants, forced to invest time in order to obtain this information themselves, to investigate the theft of their Personal Information and to take measures necessary in order to diminish or control the loss and risks that are associated therewith.

121. These inconveniences largely surpass the normal inconveniences associated with sending Personal Information to a third party and the risks that come with it.
 - 121.1. The Plaintiff and the Class Members should not today have to incur fees to manage the damages that were caused by the Defendants' negligence.
 - 121.2. The significance of the inconveniences associated with sending Personal Information was in this case directly increased by the Defendants, namely by its past conduct, including the continued absence of putting in place adequate protective measures, despite a warning from the American regulatory authorities – not disclosed to the Plaintiff and the Class Members – and the payment of a ransom that increased the risk that their Personal Information would once again be compromised.
 - 121.3. Finally, a major part of the risk was not related to the mere sharing of Personal Information, but to the fact that the Defendants knowingly hid from the Plaintiff and the Class Members the very existence of the Hack concerning them, after having been informed thereof, preventing them from mitigating their damages.
122. The Plaintiff and the Class Members suffered and will continue to suffer damages, namely the unauthorized disclosure and use of their Personal Information which includes extremely sensitive financial information, and the loss of control over this Information.
123. This situation will thus continue to generate additional significant stress for the Plaintiff and the Class Members whose Personal Information is likely still in the hands of the Hackers or to have been communicated to other criminals.
124. The Plaintiff asserts that these moral damages are the direct result of the Defendants' conduct.
125. In addition to these moral damages, the Plaintiff and the Class Members will also suffer a pecuniary loss stemming from the facts, acts and omissions of the Defendants.
126. In fact, Uber never offered any measure to mitigate the Plaintiff's and the Class Members' damages nor their risk of identity theft, by offering, for example, easy access to monitoring programs on their credit file or, at a minimum, providing information in this regard.
127. Due to the conduct of the Defendants and the delays caused by the concealment of the Hack, the Plaintiff and the Class Members are today obliged to take draconian measures, going beyond the usual routine checks in order to counteract the eventual prejudice related to the disclosure of their Personal Information to an unauthorized third party as well as the fact that the Hackers obtained this Personal Information.

128. The Plaintiff and the Class Members must themselves incur fees in order to obtain advice regarding protection against and prevention of identity theft, instruct a credit evaluation agency, get a re-evaluation of their credit file, ask an agency to monitor their credit file and, in certain cases, investigate an identity theft and take measures to remediate it.
129. More particularly in the case of the Plaintiff, these steps and measures that must be taken surpass largely the normal inconveniences, and are exceptional in the circumstances and directly due to the Defendants' acts and omissions, the Defendants refusing to this day to disclose the extent of the Personal Information hacked, which would have allowed the Plaintiff to take the necessary measures more efficiently and at a lower cost.
130. Uber also did not inform the Plaintiff nor any other Class Member of the measures taken in order to limit the prejudice suffered, to the point that their increased vigilance will have to continue over time, thereby increasing the associated costs.
131. In paying the Hackers an amount of \$100,000 USD, Uber also increased the risk that the Plaintiff and the Class Members' Personal Information be subjected to a future hack by persons also tempted to extort money from Uber.
132. The acts and omissions of the Defendants, their faults, their failures to meet their legal and contractual and other obligations, are the cause of the Plaintiff's and Class Members' damages, including their moral damages and economic losses.
133. Finally, the Plaintiff and the Class Members assert that the conduct of the Defendants as described above was not a first, was intentional, deliberate, demonstrated carelessness and recklessness, a high degree of negligence and was a flagrant disregard for the security, privacy and (...) rights of the Plaintiff and the Class Members, and in doing so, expose the Defendants to punitive and exemplary damages.
134. It is imperative in the circumstances that the Defendants be condemned to pay punitive damages in an amount that is sufficiently high in order to incite them to change their behavior, their policies and procedures and way of doing things regarding the collection, holding, retention, use and disclosure of Personal Information as well as in regards to informing the persons concerned by data theft.
- 134.1. The fact that the Defendants, despite previously having been the subject of such a hack, still failed to modify their behaviour, policies, procedures and ways of functioning in this respect is also demonstrative of the Defendants' recklessness.
- 134.2. Even the Federal Trade Commission's decision exhibit P-5 did not cause the Defendants to disclose this second Hack to those concerned.

135. In light of the foregoing, the Plaintiff is within his rights to ask for moral damages, in an amount to be detailed, in order to compensate for the stress and inconvenience caused by the faults of the Defendants, as is the case for the other Class Members.
136. In light of the foregoing, the Plaintiff is also within his rights to ask for pecuniary damages, in an amount to be detailed, in order to compensate for the fees and expenses incurred due to the faults of the Defendants, as is the case for the other Class Members.
137. In light of the foregoing, the Plaintiff is also within his rights to ask for punitive damages, given the reprehensible conduct of the Defendants, incompatible with the objectives sought by the legislator in the *Consumer Protection Act* and the Defendants' intentional interference with the Plaintiff and the Class Members' right to a private life, contrary to the Quebec *Charter of Human Rights and Freedoms*.
138. The severity of the Defendants' faults, their patrimonial situation, estimated at about \$70 billion USD, and the relatively minimal extent of the damages that Uber would be obligated to pay if the Plaintiff is successful regarding moral and pecuniary damages, justifies that the Plaintiff and the Class Members claim \$10,000,000 in punitive damages, amount to be detailed.

IV. THE COMPOSITION OF THE CLASS MAKES IT DIFFICULT OR IMPRACTICABLE TO APPLY THE RULES FOR MANDATES TO TAKE PART IN JUDICIAL PROCEEDINGS ON BEHALF OF OTHERS OR FOR CONSOLIDATION OF PROCEEDINGS

139. The determination of the identical, similar or related issues of law or fact presented in this Application will allow the advancement of the proceedings even if individual questions should remain to be decided.
140. The Group is composed of an indeterminate number of user and driver Members who provided their Personal Information to Uber.
141. The identity of these Members is known to the Defendants. Thus, it would be easy to identify them using the Defendants' records.
142. The Class Members, as individuals, do not have the resources of the Defendants. Individual actions by each Group Member would not be economical and would not be an adequate or efficient use of judicial resources.
143. Without this class action, the Class Members would effectively be deprived of access to justice.
144. Deterrence of the Defendants in order for them to modify their behaviours, policies and procedures also militates in favour of an action of this nature.

145. This action is the appropriate means for resolving efficiently and equitably the current litigation without excessively bogging down the Court and the justice system with a multitude of individual actions, as well as to avoid the risk of contradictory decisions on the same facts and questions.
146. All of the Class Members have in common the fact that they suffered damages resulting from the omission or negligence of the Defendants to protect their Personal Information and their failure to inform them in a timely manner that their Personal Information had been compromised.
147. The Class Members are so numerous that the consolidation of proceedings in one would simply not be practical.
148. Thus, the condition provided at paragraph 575(3) of the *Code of Civil Procedure*, regarding the composition of the class in order for the Court to authorize the class action, is met.

V. **THE CLASS MEMBERS' CLAIMS RAISE IDENTICAL, SIMILAR OR RELATED ISSUES OF LAW OR FACT**

149. The identical, similar or related questions raised in this Application for a class action are the following :
- a) Did the Defendants fail in their contractual obligations to protect the Personal Information provided by the Class Members?
 - b) Did the Defendants' conduct constitute a failure of their obligation of diligence and prudence?
 - c) Did the Defendants fail in their obligation under *PIPEDA* to protect the Personal Information of the Class Members?
 - d) Did the Defendants fail in their obligation under *PPIPS* to protect the Personal Information of the Class Members?
 - e) Did the Defendants fail in their more general obligation to inform the Class Members that their Personal Information had been compromised once they learned of the Uber Hack?
 - e.1) Does the Defendants' conduct constitute a failure of their obligation to act in good faith?
 - f) Did the Defendants fail in their obligation under the *Civil Code of Québec* and the *Consumer Protection Act* to not conduct disloyal commercial practices, including the obligation not to make false and misleading representations to Class Members regarding the collection, holding, retention, use and disclosure of their Personal Information?

- g) Did the Defendants illegally and intentionally interfere with the fundamental rights and freedoms of the Class Members, protected by the Quebec *Charter of Human Rights and Freedoms*?
 - h) If it is demonstrated that the Defendants failed in their obligations and duties, do the Class Members have the right to be compensated for the damages suffered?
 - i) What is the appropriate amount of moral, pecuniary and punitive damages to which the Class Members have right?
 - j) Are the Defendants solidarily liable for the damages caused to the Class Members?
150. Given the nature of the questions raised and their relatedness, the condition provided at paragraph 575(1) of the *Code of Civil Procedure* is also satisfied herein.

VI. THE NATURE OF THE ACTION THAT THE PLAINTIFF INTENDS TO EXERCISE ON BEHALF OF THE CLASS MEMBERS

151. An action in civil liability for general damages as well as punitive and exemplary damages against the Defendants.

VII. THE CONCLUSIONS SOUGHT BY THE PLAINTIFF (...)

151.1. The conclusions sought by the Plaintiff are:

GRANT the Plaintiff's Application;

CONDEMN the Defendants, solidarily, to pay the Plaintiff an amount for non-pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay the Plaintiff an amount for pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

GRANT the Plaintiff's class action for all Class Members;

CONDEMN the Defendants, solidarily, to pay each Class Member an amount for non-pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay each Class Member an amount for pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay to the Plaintiff and the Class Members the amount of \$10,000,000 as punitive damages, to be detailed, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

ORDER collective recovery of the claims for non-pecuniary and punitive damages for all Class Members and individual liquidation of the claims of Class Members in accordance with articles 595 to 598 of the *Code of Civil Procedure*;

ORDER collective recovery of the claims for pecuniary damages for all Class Members and individual liquidation of the claims of Class Members in accordance with articles 595 to 598 of the *Code of Civil Procedure*, and, alternatively, order the individual recovery of claims for pecuniary damages for all Class Members in accordance with articles 599 to 601 of the *Code of Civil Procedure*;

THE WHOLE with judicial costs, including fees for notices and experts.

152. The facts alleged appear to justify the conclusions sought, thus satisfying the condition provided at paragraph 575(2) of the *Code of Civil Procedure*.

VIII. THE PLAINTIFF IS IN A POSITION TO PROPERLY REPRESENT THE CLASS MEMBERS

153. The Plaintiff is available to invest all the time and effort required in order to accomplish all of the formalities and tasks necessary for the advancement of this class action.
154. The Plaintiff mandated the undersigned lawyers who have significant experience in class action matters.
155. The Plaintiff collaborated and is prepared to collaborate with the undersigned counsel in all steps of the process and to provide information necessary to ensure the advancement of this class action.
156. While the Plaintiff could have filed an individual application, he prefers to bring this class action in order to help the other Class Members.
157. The Plaintiff seeks to facilitate access to justice for the Class Members.

158. The Plaintiff is acting in good faith for the sole objective of asserting his rights as well as those of the Class Members.

159. The Plaintiff is thus able to ensure adequate representation of the members in the sense of paragraph 575(4) of the *Code of Civil Procedure*.

IX. THIS CLASS ACTION SHOULD BE BROUGHT IN THE DISTRICT OF MONTREAL

160. The district of Montreal is the most appropriate considering that Class Members are located all over the province of Quebec, with a majority in Montreal including the Plaintiff.

161. Further, the undersigned attorneys have their offices in Montreal.

FOR THESE REASONS, MAY IT PLEASE THE COURT TO:

GRANT this Amended Application for Authorization to Exercise a Class Action and to be Appointed as Representative Plaintiff.

AUTHORIZE the class action in civil liability and moral, pecuniary, punitive and exemplary damages against the Defendants.

APPOINT the Plaintiff Pierre-Olivier Fortier as representative of the group herein described as:

“All persons residing in Quebec that, as users, provided personal information to Uber that was collected, held, retained and used by Uber and disclosed without authorization to a third party in October 2016.”

APPOINT the Plaintiff Pierre-Olivier Fortier as representative of the group herein described as:

“All persons residing in Quebec that, as drivers, provided personal information to Uber that was collected, held, retained and used by Uber and disclosed without authorization to a third party in October 2016.”

IDENTIFY the principle questions of fact and law to be treated collectively as the following:

- a) Did the Defendants fail in their contractual obligations to protect the Personal Information provided by the Class Members?
- b) Did the Defendants’ conduct constitute a failure of their obligation of diligence and prudence?

- c) Did the Defendants fail in their obligation under *PIPEDA* to protect the Personal Information of the Class Members?
- d) Did the Defendants fail in their obligation under *PPIPS* to protect the Personal Information of the Class Members?
- e) Did the Defendants fail in their more general obligation to inform the Class Members that their Personal Information had been compromised once they learned of the Uber Hack?
- e.1) Does the Defendants' conduct constitute a failure of their obligation to act in good faith?
- f) Did the Defendants fail in their obligation under the *Civil Code of Québec* and the *Consumer Protection Act* to not conduct disloyal commercial practices, including the obligation not to make false and misleading representations to Class Members regarding the collection, holding, retention, use and disclosure of their Personal Information?
- g) Did the Defendants illegally and intentionally interfere with the fundamental rights and freedoms of the Class Members, protected by the Quebec *Charter of Human Rights and Freedoms*?
- h) If it is demonstrated that the Defendants failed in their obligations and duties, do the Class Members have the right to be compensated for the damages suffered?
- i) What is the appropriate amount of moral, pecuniary and punitive damages to which the Class Members have right?
- j) Are the Defendants solidarily liable for the damages caused to the Class Members?

IDENTIFY as follows the conclusions sought in relation thereto:

GRANT the Plaintiff's Application;

CONDEMN the Defendants, solidarily, to pay the Plaintiff an amount for non-pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay the Plaintiff an amount for pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*;

Québec, from the date of service of the Application for Authorization to Exercise a Class Action;

GRANT the Plaintiff's class action for all Class Members;

CONDEMN the Defendants, solidarily, to pay each Class Member an amount for non-pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay each Class Member an amount for pecuniary damages, to be determined at trial, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

CONDEMN the Defendants, solidarily, to pay to the Plaintiff and the Class Members the amount of \$10,000,000 as punitive damages, to be detailed, as well as interest at the legal rate and the additional indemnity provided at article 1619 of the *Civil Code of Québec*, from the date of service of the Application for Authorization to Exercise a Class Action;

ORDER collective recovery of the claims for non-pecuniary and punitive damages for all Class Members and individual liquidation of the claims of Class Members in accordance with articles 595 to 598 of the *Code of Civil Procedure*;

ORDER collective recovery of the claims for pecuniary damages for all Class Members and individual liquidation of the claims of Class Members in accordance with articles 595 to 598 of the *Code of Civil Procedure*, and, alternatively, order the individual recovery of claims for pecuniary damages for all Class Members in accordance with articles 599 to 601 of the *Code of Civil Procedure*;

THE WHOLE with judicial costs, including fees for the notices and experts.

DECLARE that, unless they have been excluded, the Class Members will be bound by any judgment to be rendered on the class action in the manner provided for by law;

FIX the deadline for exclusion at thirty (30) days after the date of the notice to members, at the expiry of which Class Members that have not requested their exclusion will be bound by any judgement to be rendered;

ORDER the publication of a notice to members (in accordance with article 576 of the *Code of Civil Procedure*) on the conditions that will be determined by the Court;

REFER the file to the Chief Justice for determination of the district in which the class action will be exercised and designation of the judge to hear it;

(...)

THE WHOLE with judicial costs, including expert fees and notice publication fees.

Montreal, March 15, 2018

WOODS LLP

Counsel for the Plaintiff Pierre-Olivier Fortier

Mtres. James A. Woods, Sarah Woods

and Jessy Héroux

2000 McGill College Avenue, suite 1700

Montreal, Quebec H3A 3H3

Tel : (514) 982-4545 Fax : (514) 284-2046

Email: notification@woods.qc.ca

jwoods@woods.qc.ca

swoods@woods.qc.ca

jheroux@woods.qc.ca

SUMMONS
(Articles 145 and following of the *Code of Civil Procedure*)

Filing of a judicial application

Take notice that the plaintiff has filed this originating application in the office of the court of Montreal in the judicial district of Montreal.

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal situated at 1 Notre-Dame Street East, within 15 days of service of the application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the plaintiff's lawyer or, if the plaintiff is not represented, to the plaintiff.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgement may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the plaintiff in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Québec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Change of judicial district

You may ask the court to refer the originating application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

Transfer of application to Small Claims Division

If you qualify to act as a plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

Calling to a case management conference

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the originating application, the plaintiff intends to use the following exhibits:

EXHIBIT P-1	Extract of the Corporate Register for Uber Canada Inc.
EXHIBIT P-2	Copy of the terms of use applicable to Uber users and drivers
EXHIBIT P-3	Copy of an article published on the Radio-Canada website dated December 12, 2017 on the topic of the Uber hack
EXHIBIT P-4	<u>En liasse</u> , copy of the <u>two (2)</u> privacy policies in force from July 2015 to November 2017 for Uber users and drivers
EXHIBIT P-5	<u>En liasse</u> , copy of the <u>complaint and the order of the Federal Trade Commission</u>
EXHIBIT P-6	<u>Copy of the February 28, 2018 decision by the Alberta Privacy Commissioner</u>
EXHIBIT P-7	<u>Copy of the email sent to the Plaintiff on March 12, 2018</u>

These exhibits are available on request.

Notice of presentation of an application

If the application is an application in the course of a proceeding or an application under Book III, V, excepting an application in family matters mentioned in article 409, or VI of the Code, the establishment of a case protocol is not required; however, the application must be accompanied by a notice stating the date and time it is to be presented.

Translation