CANADA

(Class Action Division)

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

SUPERIOR COURT

Nº : 500-06-000902-185

PIERRE-OLIVIER FORTIER, [redacted]

Plaintiff

– and –

ALL PERSONS RESIDING IN QUEBEC WHO, AS USERS, PROVIDED UBER WITH PERSONAL INFORMATION THAT WAS COLLECTED, HELD, RETAINED AND USED BY UBER AND DISCLOSED AND/OR MADE ACCESSIBLE WITHOUT AUTHORIZATION TO A THIRD PARTY IN OCTOBER OF 2016

Sub-class of users / Plaintiffs

– and –

ALL PERSONS RESIDING IN QUEBEC WHO, AS DRIVERS, PROVIDED UBER WITH PERSONAL INFORMATION THAT WAS COLLECTED, HELD, RETAINED AND USED BY UBER AND DISCLOSED AND/OR MADE ACCESSIBLE WITHOUT AUTHORIZATION TO A THIRD PARTY IN OCTOBER OF 2016

Sub-class of drivers / Plaintiffs

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, the Netherlands

– and –

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

– and –

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

Defendants

AMENDED ORIGINATING APPLICATION
(Articles 100, 141-141 and 583 of the *Code of Civil Procedure*)

IN SUPPORT OF HIS ORIGINATING APPLICATION, THE PLAINTIFF PIERRE-OLIVIER FORTIER SUBMITS:

I. INTRODUCTION

1. The Plaintiff, Mr. Pierre-Olivier Fortier ("**Mr. Fortier**") was authorized to proceed with the class action and was given the status of the representative of the persons included in the following sub-classes (collectively, the "**Class**"; individually, the "**Class Members**"):

> *All persons residing in Quebec who, as users, provided Uber with personal information that was collected, held, retained and used by Uber and disclosed and/or made accessible without authorization to a third party in October of 2016 (the "**Sub-class of users**")*

and

*All persons residing in Quebec who, as drivers, provided Uber with personal information that was collected, held, retained and used by Uber and disclosed and/or made accessible without authorization to a third party in October of 2016 (the "**Sub-class of drivers**")*

as it appears from the authorization judgment in the Court record dated September 28, 2021 (the "**Authorization judgment**").

2. This proceeding (the "**Class Action**") is in response to events that occurred in October 2016 when personal information of the Class Members (hereinafter, "**Personal Information**") that was collected, held, retained and used by Uber (as defined in sub-section B of section III below) and communicated without authorization to a third party was made accessible to two hackers (collectively, the "**Hackers**").

3. This occurred all the while the Defendants have known, since 2014, that their system of storing Personal Information was defective.

4. Even worse, the Defendants withheld this critical information from their users and drivers until a year later when the media exposed them.

5. As will be detailed below, the Defendants are liable to the Members for the following faults:

a) 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;

b) Disclosing to an unauthorized third party the Personal Information of the Class Members for an unauthorized purpose, without having previously obtained their consent;

c) Failing to take 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;

d) Intentionally concealing the hacking of the Personal Information for over a year, thereby preventing the Class Members from taking the measures necessary to avoid having their Personal Information being compromised again or having their identity stolen;

e) Putting their own interests before the Class Members' rights and interests to their private lives and the confidentiality of their Personal Information;

f) Breaching their obligations and failing in their general duty of prudence and diligence;

g) Breaching the applicable legal obligations relating to the collection, holding, retention, use and communication of Personal Information of the Class Members;

h) Breaching the *Consumer Protection Act*, CQLR c. P-40.1 ("**CPA**") by making false representations to Uber users and omitting to disclose important facts;

i) Violating the fundamental right to a private life protected by the *Charter of Human Rights and Freedoms*;

6. Mr. Fortier seeks, in his name and on behalf of the Class Members, the collective recovery of the following damages:

(i) moral damages in an amount *à parfaire* at trial;

(ii) pecuniary damages in an amount *à parfaire* at trial;

(iii) $10,000,000 in punitive damages for the Defendants' unlawful and intentional interference with the Class Members' rights, *à parfaire*;

(iv) interest at the legal rate and the additional indemnity provided for at article 1619 of the *Civil Code of Québec* ("**CCQ**");

(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, MR. FORTIER

7. The Plaintiff is an actor who lives and works in Montreal.

8. He is also very involved in the *Union des artistes*, as a representative in the negotiation of collective agreements.

9. The Plaintiff does not have a car and uses exclusively public transit, a bicycle, car-sharing and taxi services to move around.

10. On November 17, 2013, the Plaintiff signed up for the transportation services offered by Uber and downloaded the Uber mobile application, as a user.

11. 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.

12. 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 using the transportation services and the Uber application.

13. Since he began using the Uber application, other Personal Information of the Plaintiff has also been collected by Uber.

14. The Plaintiff had the right to expect that his Personal Information would be collected, held, retained and used by Uber in a secure manner, notably 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.

15. On or around November 21, 2017, when the October 2016 hacking was reported in different media, the Plaintiff first became aware of the fact that his Personal Information had been communicated and/or rendered accessible in an unauthorized fashion by Uber to a third party.

16. In fact, before November 21, 2017, he had absolutely no knowledge of these facts, not having been advised of either the hacking Uber had been subjected to, or of the fact that any Personal Information he had provided had been compromised.

17. It was only on March 12, 2018, that the Plaintiff finally received a notice from Uber that his Personal Information had been hacked in 2016, 17 months after the incident.

B. THE DEFENDANTS

18. The Defendants are companies acting jointly in the development and operation of mobile applications for connecting drivers providing transportation services (Uber) and food deliveries (UberEATS).

19. The Defendant Uber Canada Inc. is a company duly incorporated under the *Canada Business Corporations Act*, RSC 1985, c C-44, the offices of which are located at 100 King Street West, suite 6200, Toronto, Ontario. It carries on its activities in Quebec under the name Uber Canada Inc. and has a principal establishment in Quebec at 1751 Richardson Street, suite 7120, Montreal, Quebec, H3K 1G6, as it appears from an extract of the Quebec corporate register, disclosed in support hereof as **Exhibit P-1**.

20. Uber Canada Inc. is responsible for marketing and administrative support for Uber B.V. for the Uber applications in Canada as well as for technical support offered to Uber users and drivers in Quebec and elsewhere in Canada.

21. The Defendant Uber Technologies Inc. is a company duly incorporated under the laws of Delaware, with its head office located in San Francisco, in the United States of America. It developed, distributed and operated the Uber applications for smartphones, which connect Uber users to drivers in Quebec. It also operates the site www.uber.com, which is accessible in Quebec.

22. The Defendant Uber B.V. is a company duly incorporated under the laws of the Netherlands, with its head office located in Amsterdam. It is the company that holds and uses the Uber applications' intellectual property for smartphones and, incidentally, connects users to Uber drivers in Quebec. It is also the entity that controlled the Personal Information of users and drivers that was hacked in 2016.

23. 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. It is the company that grants the limited access licenses for Uber applications in Canada. Rasier Operations B.V. has an individual contract with each user and driver.

24. Uber Portier B.V. is also a company duly incorporated under the laws of the Netherlands, with its head office located in Amsterdam. It is the company that grants the limited access licenses for the UberEATS application.

25. At all times relevant to the period covered by 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 businesses.

III. FACTS GIVING RISE TO THIS APPLICATION

26. Personal information of physical and legal persons is coveted by identity thieves for illegal ends. Once this information has been compromised, criminals can, notably, 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", a network known for its illegal content, making this information public and potentially destined for criminal activities.

27. This Class Action is being undertaken by the Plaintiff who, as all Class Members, provided his Personal Information to Uber.

28. Uber decided to hold and retain the Personal Information on a third-party Cloud network in an unauthorized manner.

29. Due to its carelessness and negligence, Uber made this Personal Information accessible to the Hackers around October 2016.

30. To make matters worse, Uber voluntarily concealed this unauthorized disclosure for more than one year, choosing rather to transact with the Hackers and to buy their silence.

31. Hence, Uber did not notify the Plaintiff and the Class Members that their Personal Information had been compromised, preventing them from protecting themselves against identity theft and all other illicit and prejudicial use of their Personal Information, and increasing the risks of them falling victim to such illegal behaviour again in the future.

32. 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

33. Uber is a multinational corporation which offers transportation services in 83 countries as well as more than 673 cities around the world.

34. Uber's transportation services have been offered in Canada, including in Quebec since at least 2013.

35. In Quebec, Uber's transportation services are notably offered in the cities of Montreal, Quebec, Gatineau, Saguenay, Sherbrooke, Trois-Rivières and other cities and municipalities in the Laurentian region.

36. Once registered as a user after downloading the Uber application, anyone can use it anywhere in the world where Uber services are offered.

37. The transportation services offered by Uber in Quebec include, without limitation, UberEATS, UberX, UberXL and Premier.

38. UberEATS is a delivery service through which a user can order food from a participating restaurant.

39. 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.

40. UberXL is a similar service to that offered by UberX, but offers larger vehicles, such as SUVs.

41. Finally, Premier is a transportation service that resembles the other services, but offers high-end vehicles.

42. The services in this vast transportation network are provided through the same mobile application, except for 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

43. In order to access all of these services, a person must first download the Uber Application and accept Uber's terms of use.

44. Uber operates three mobile Applications:

(i) The Uber Application for users;

(ii) The Uber Application for drivers;

(iii) The UberEATS Application.

45. Uber users use the first of these applications to plan and order a ride, check on their ride on their smartphones and facilitate the payment of the ride and rate the Uber drivers.

46. 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 rate the passengers at the end of the ride.

47. Finally, as mentioned previously, Uber users can also, through UberEATS, order food from a participating restaurant.

48. 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, including their credit card number;

49. The user, in accepting Uber's general terms of use, is contractually bound to Uber B.V. to respect these terms.

50. In the case of Uber drivers, in order to have access to the Uber Application they must satisfy certain conditions, notably, be at least 21 years old, provide a valid driver's license, proof of registration and proof of insurance.

51. The latter 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.

52. If the conditions are satisfied, the driver must then accept Uber's terms of use and in doing so, is contractually bound to Rasier Operations B.V. to respect these terms.

53. 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.

54. Uber's terms and conditions of use stipulate the Uber Application user's – user or driver – obligations 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 (the "*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.
>
> [Our translation and emphasis]

as it appears from the terms of use applicable to users and drivers, disclosed in support hereof as **Exhibit P-2**.

55. 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 and conditions of use, including Uber's privacy policy applicable during the relevant periods.

56. However, Uber decided to hold and retain the Personal Information on a "Cloud"-type network owned by a third party, thereby contravening its own privacy policies.

57. At no point in time did Uber advise the Plaintiff or the Class Members of its intention to proceed this way, let alone request their permission to do so.

58. Further, at no point in 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 regarding 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**").

59. At no point in 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 comprehensive and appropriate program for the protection of personal information, due to its failure to have a satisfactory program in place, as it appears from a copy of the complaint and the decision of the Federal Trade Commission rendered in 2017 against Uber, disclosed in support hereof as **Exhibit P-3**, *en liasse*, as well as the complaint and the revised decision from October 2018, disclosed in support hereof as **Exhibit P-4**, *en liasse*.

C) THE HACK OF PERSONAL INFORMATION

60. 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**").

61. Uber was notified of the Hack shortly after it happened, that is, in November 2016, and deliberately chose to hide it from the Class Members, including the Plaintiff, 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.

62. Rather than inform the Plaintiff and the 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 USD100,000, in exchange for a promise of silence and the purported destruction of the Personal Information to which they had access.

63. Initially, Uber claimed that the USD100,000 payment was a « bug bounty », a legitimate payment made to a third party to test its information technology systems, a statement which Uber fully knew to be false and intentionally misleading.

64. In fact, the Hackers were fundamentally different from legitimate recipients of a "bug bounty", since instead of simply identifying a vulnerability in Uber's systems and disclosing it in a reasonable manner, the Hackers exploited it in a malicious way in order to gain access to the Personal Information of the Class Members.

65. 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.

66. The same day, Uber was forced to publicly admit that it had been the subject of a hack in October 2016 wherein hackers had had access to the Personal Information held by Uber on the Cloud server of a third party.

67. On December 11, 2017, the Office of the Privacy Commissioner of Canada announced that it was opening a formal investigation into the Uber Hack.

68. The same day, Uber announced that 815,000 Canadian drivers or users were affected by the Hack, as it appears from a copy of the article published on the Radio-Canada website, disclosed in support hereof as **Exhibit P-5**.

69. On February 28, 2018, the Information and Privacy Commissioner of Alberta rendered a decision with respect to the Hack, concluding that the Hack posed a real risk of significant harm to Uber users, especially when personal information was compromised by a deliberate and unauthorized intrusion by the Hackers, and ordering Uber B.V. to notify the users of the Hack, as it appears from the February 28, 2018 decision by the Information and Privacy Commissioner of Alberta, disclosed in support hereof as **Exhibit P-6**.

70. On March 12, 2018, approximately eighteen (18) months after the Hack, and after being ordered to do so by the Information and Privacy Commissioner of Alberta and despite having had continuous access to the users' data which would have enabled Uber to notify them without delay, Uber finally notified the Canadian users and

drivers affected by the Hack that it had occurred, as it appears from a copy of the email sent to the Plaintiff, disclosed in support hereof as **Exhibit P-7**.

71. This email dated March 12, 2018 (Exhibit P-7) confirms that the Hack lasted for over one (1) month, and included Personal Information used by Uber to operate its services, including notably users names, email addresses, and mobile phone numbers and, in some cases, Uber internal user IDs, location information, user tokens, user ratings and scores, notes by Uber personnel, encrypted passwords and drivers' payment statements.

72. In the Netherlands, on November 6, 2018, the Dutch Protection Authority rendered a decision following an investigation concerning the Hack, in which it fined Uber € 600,000 for having omitted to notify users and drivers about the Hack within 72 hours, as it appears from a copy of the said decision delivered in Dutch and an English translation, disclosed in support hereof as **Exhibit P-8**, *en liasse*.

73. Moreover, in the United Kingdom, on November 26, 2018, the Information Commissioner's Office also conducted an investigation and fined Uber € 385,000 for having omitted to protect the personal information of users during the Hack, as it appears from the monetary penalty notice and the press release issued by the commissioner that accompanied the notice, copies of which are disclosed in support hereof as **Exhibit P-9**, *en liasse*.

74. In France, on December 19, 2018, the *Commision nationale de l'informatique et des Libertés* also rendered a decision in which it fined Uber € 400,000 for having failed to ensure the security and confidentiality of the data, as it appears from the Deliberation of the restricted panel nº SAN-2018-011, a copy of which is disclosed in support hereof as **Exhibit P-10**.

75. Furthermore, on August 20, 2020, the former chief of Uber's security, Mr. Joe Sullivan, was accused of attempting to conceal the Hack. More specifically, Mr. Sullivan was charged with obstruction of justice and misprision of a felony, as it appears from a press release of the Department of Justice, Northern District of California, an article in the newspaper *La Presse*, and the criminal complaint, which are disclosed in support hereof as **Exhibits P-11**, **P-12** and **P-13** respectively.

D) THE DEFENDANTS' LIABILITY

76. The Defendants are 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 trial.

a) The Civil Liability of the Defendants

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

78. In both cases, these contracts are contracts of adhesion as set out at article 1379 of the CCQ, insofar as it is clear that the essential stipulations were imposed and drawn up by Uber and were not negotiable.

79. 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.
>
> [Our translation and emphasis]

80. Between July 2015 and November 2017, Uber had two (2) privacy policies in place, one for its users and one for its drivers, as it appears from the two (2) privacy policies of July 2015 and November 2017, disclosed in support hereof as **Exhibit P-14**, *en liasse*.

81. 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.

[Our translation]

82. The privacy policy also sets out the five (5) circumstances in which Uber has the right to use the Personal Information shared 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.

[Our translation]

83. Regarding the storing of the Personal Information, this same policy provides that Uber must take the "appropriate" measures in order to ensure that users' Personal Information is not compromised or, to use the words of the policy, to "protect" this Personal Information.

84. Finally, the privacy policy also sets out the circumstances in which the Personal 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;

- <u>If we otherwise notify you and you consent to the sharing; and</u>

- <u>In an aggregated and/or anonymized form which cannot reasonably be used to identify you</u>.

[Our translation and emphasis]

85. The privacy policy for Uber drivers, applicable between July 2015 and November 2017 (Exhibit P-14), includes similar conditions.

86. Further, just as is the case with the privacy policy applicable to users between July 2015 and November 2017, Uber must take appropriate measures in order to ensure that the drivers' Personal Information is held and retained without being compromised.

87. It also provides that this information cannot be disclosed to a third party that is not mentioned without the driver having previously been notified, consent to same and that the Personal Information be provided to the third party in an anonymous fashion.

88. These two aspects are express stipulations included by reference in the contracts between Uber and the Plaintiff and the Class Members.

89. 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 in any way, 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.

90. By transferring such a significant quantity of Personal Information on a third party's Cloud network, Uber violated the aforementioned contracts' terms and conditions of use as well as its obligations under the applicable privacy policies.

91. At no point in time 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 to it being transferred in such a way.

92. 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.

93. 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.

94. 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.

95. This transfer was not at all justified and was done in flagrant disregard of the Plaintiff and the Class Members' rights and interests with regards to their private lives.

96. 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.

97. Further, this unauthorized transfer of Personal Information by Uber rendered this Personal Information inherently vulnerable to hacking, which Uber should have known or anticipated, notably considering the 2014 Hack.

98. The Plaintiff and the Class Members were never informed of this risk.

99. The technology, programs or digital tools used by the Defendants, including the use of a "Cloud"-type online server operated by a third party to retain the Plaintiff and the Class Members' Personal Information, were inadequate and insufficient and eventually permitted that this same Personal Information end up in the hands of the Hackers.

100. Uber hired information technology employees and sub-contractors who were not qualified to ensure the safety of the Plaintiff and the Class Members' Personal Information.

101. 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.

102. The Defendants were extremely negligent by not acting as a reasonable person in the circumstances, including 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.

103. More specifically, the Hackers managed to access Uber's GitHub private account by using username and password pairs that had been exposed in the course of previous hacks. The Hackers informed Uber that they had managed to identify passwords for

GitHub accounts belonging to 12 Uber employees, as it appears from the decision rendered in the UK, Exhibit P-9.

104. The access keys having enabled the Hackers to access the online Cloud service housing the Personal Information were stored, unencrypted, in Uber's GitHub account, contrary to the recommended security practices in the industry.

105. Moreover, contrary to a common security practice, Uber never prohibited engineers from reusing credentials, and never required engineers to enable multi-factor authentication, which would have needed an additional authentication such as a security token, an ID number or a biometric factor when accessing Uber's GitHub repositories, as it appears notably from the decision rendered in the UK (Exhibit P-9) and the revised American complaint (Exhibit P-4).

106. GitHub already had a two-factor identification security process in place at the time, but Uber voluntarily chose not to avail itself of it.

107. Despite the 2014 Hack, Uber failed to put in place training, policy or procedure to ensure that its personnel was […] adequately informed of the directives and practices with respect to the protection of personal data and did not implement the necessary measures enabling it to verify whether the said policies were respected by the personnel.

108. As a result of this negligence and the lack of appropriate security measures, it took the Defendants one (1) month to detect the existence of the Hack.

109. The Defendants' conduct also allowed cybercriminals to illegally access the Plaintiff and the Class Members' Personal Information for at least one (1) month.

110. The Defendants, by their carelessness and recklessness, made the Hackers' Hack of the Personal Information possible.

111. Further, the Defendants' response to the Uber Hack and to the theft of the Class Members' Personal Information also constitutes negligent conduct that exposed the Plaintiff and the Class Members to additional prejudice.

112. By 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 Uber users and drivers' Personal Information, the Defendants chose to pay cybercriminals in order to hide the theft, prioritizing their interests over those of the Plaintiff and the Class Members.

113. 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 the Class Members' interests and right to a private life.

114. The Defendants also increased the risks that the Plaintiff and the Class Members' Personal Information would be the subject of a future hack due to its decision to pay the Hackers USD 100,000, which legitimized the Hack and deprived the Plaintiff and the Class Members of the opportunity to mitigate their damages in this regard.

115. The Defendants thus acted in bad faith.

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

116. The Personal Information provided by the Plaintiff and the Class Members collected, held, 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. The *PPIPS* was recognized in Quebec as being essentially similar to *PIPEDA*.

117. As such, the Defendants were subject to the obligations set out in both *PIPEDA* and *PPIPS* regarding the collection, retention, holding, use and disclosure of the Class Members' Personal Information.

118. Pursuant to both *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, and always in a safe manner in order to preserve the confidentiality of the Personal Information.

119. The Defendants failed in their obligation to protect this Personal Information by failing to put in place and enforce 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.

120. 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.

121. More specifically, in disclosing the Plaintiff and the Class Members' Personal Information and retaining it on a third party's online server 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 solely for the intended purpose.

122. The Defendants also 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."

123. The Defendants also failed in their obligation of openness pursuant to sections 4.8 to 4.8.3 of Schedule 1 of *PIPEDA*.

124. 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.

125. In 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.

126. However, the use and disclosure made by the Defendants of the Personal Information provided does not fall in any of the categories specifically enumerated in *PIPEDA* as being exceptions.

127. The failure or inability of the Defendants to put in place and apply policies and procedures and use the technological means that would have permitted the protection of the Class Members' Personal Information and the 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, among other things, 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."

128. The Defendants also violated sections 13 and 17 *PPIPS* by communicate this Personal Information to a third party without first obtaining the Plaintiff and the Class Members' consent and by omitting to ensure that Personal Information was not accessible to unauthorized third parties, such as the Hackers.

129. Furthermore, after being advised of the Uber Hack, the Defendants should have notified the Plaintiff and the Class Members of same without delay in order to comply with their legal obligations.

130. By failing to notify the Plaintiff and the Class Members of the Hack in due course, the Defendants, practically speaking, rendered ineffective the legislative and regulatory protections provided to the Plaintiff and the Class Members by the legislator.

131. Finally, this conduct also constitutes a violation of sections 35 to 37 of the […] CCQ, including the obligation to only gather information relevant to the stated objective and not to communicate such information to third persons or use it for purposes that are inconsistent with the purpose for which the information was gathered without the consent of the person concerned.

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

132. The Defendants also failed in their obligations under article 219 of the CPA by making false and misleading representations to the Plaintiff and the Class Members about the collection, conservation, use and communication of their Personal Information.

133. They also failed to mention an important fact, thereby contravening article 228 of the CPA.

134. 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.

135. They also chose to conceal the 2014 Hack, opting not to disclose these highly relevant facts to the users and drivers, depriving them of the possibility of appreciating the risk they ran in disclosing their Personal Information to Uber.

136. 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.

137. Finally, by not disclosing the Hack immediately in 2016, and by 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.

138. Because of these failures, the Plaintiff and the Class Members are justified in seeking punitive damages under section 272 of the CPA.

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

139. 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*.

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

141. The Defendants sent this Personal Information to a third party in an unauthorised manner, without notifying the Plaintiff or the Class Members of same.

142. Moreover, the Defendants made this Personal Information accessible to third parties, that is, the Hackers, in an unauthorised manner.

143. 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.

144. Rather than advise the Plaintiff and the Class Members that their Personal Information had been compromised, Uber instead paid the Hackers an amount of USD 100,000 in order to avoid the embarrassment that would have been caused by the publicity concerning its own failure to protect the Personal Information and the data theft.

145. 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.

146. Ultimately, one year later, it was the media that disclosed the Uber Hack to the Plaintiff and the Class Members.

147. 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.

148. All of the Defendants' actions evidence their illicit and intentional interference with the Plaintiff and the Class Members' right to a private life.

149. It also denotes a profound contempt for their rights and interests.

150. By 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 and the Class Members' right to a private life, giving rise to punitive damages pursuant to section 49 of the *Charter of Human Rights and Freedoms*.

151. 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 these highly relevant facts from its users and drivers, depriving them of the possibility of appreciating the risk they ran in disclosing their Personal Information to Uber.

152. Further, in its complaint in 2017 (Exhibit P-3), the *Federal Trade Commission* chastises Uber for having falsely led people to believe that it had in place adequate security 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

153. The Plaintiff and the Class Members suffered damages caused by the Defendants' faulty management and protection of the Personal Information provided by them, and by the multiple violations of their right to a private life.

154. Due to the Defendants' acts and omissions set out above, proof of which will be made at trial, 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 and unsecured 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.

155. As a consequence of the Defendants' acts and omissions, the Plaintiff and the Class Members have been continuously and are to this day exposed to an abnormally high risk of phishing, identity theft and usurpation and resulting financial loss.

156. The Plaintiff and the Class Members learned of the Hack more than one year after it had happened. The Defendants chose to hide this information from the Plaintiff and the Class Members, preventing them from protecting themselves against identity theft and all other illicit and prejudicial use of their Personal Information, thereby increasing their risks of becoming victims of such illegal behaviour in the future.

157. It should be remembered that the Personal Information was stolen by malicious persons, and that certain stolen data can be used by hackers months, if not years, after the hack.

158. That was the case with the hack of LinkedIn in 2012, following which a hacker started selling information gathered during the hack on a clandestine forum four (4) years later, that is, in 2016, as it appears from articles published in *La Presse* and *Le monde*, copies of which are disclosed […] in support hereof as **Exhibit P-15**, *en liasse*.

159. These risks are even greater considering that the Hackers had access to this Personal Information for more than one (1) month and exacerbated by Uber's decision to give the Hackers a ransom that had the effect of legitimizing their actions and giving them a valid reason to try again.

160. By way of reminder, the Personal Information in question was not simply lost or made available without knowing who had access to it.

161. This Personal Information was rendered accessible to the Hackers who chose to profit from this theft by extorting straight away USD100,000 from Uber.

162. The risk of identity theft and usurpation is thus increased and the measures that the Plaintiff and the Class Members had to take in order to counter this risk are also greater than in the case of disclosure of Personal Information to an unauthorized third party or loss of Personal Information.

163. The amount of Personal Information originally provided and made accessible to the Hackers, that is, the name, email address, cell phone number, encrypted passwords, payment information of Uber users and, in the case of drivers, information relating to their driver's license, registration, as well as profile photos and sensitive geolocation data, in addition to the duration of this unauthorized access, also increase the risk and thereby necessarily increase the measures that had to be taken to remedy that risk.

164. This situation, notably the fact of knowing that their sensitive Personal Information is currently or was at one time or another in the hands of the Hackers willing to extort, has caused the Plaintiff and the Class Members great stress.

165. Furthermore, other hackers can take advantage of the opportunity and the concerned users' vulnerabilit and use the Hack as a ruse to phish them. Some Uber users have since been targeted with phishing maneuvers following the Hack, as it appears from newspaper articles disclosed […] in support hereof as **Exhibit P-16**, *en liasse*.

166. It appears from these articles that hackers took advantage of the Uber users' concerns and worries following the Hack and Uber's tardy reaction to send them phishing emails in order to obtain information that would allow them to access their accounts.

167. More specifically, if the users clicked on the link mentioned in the phishing email and provided information about their password, the opportunistic hackers could access their Uber accounts and, in some cases, some of their other online accounts, considering that many people use the same password for multiple platforms.

168. The Hack has therefore significantly increased the Plaintiff and the Class Members' vulnerability and their chances of becoming targets of such fraudulent practices.

169. 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.

170. Indeed, the knowledge that their Personal Information was at risk and that Uber had already been subject to a hack in 2014 was highly relevant information for the Plaintiff and the Class Members in their decision whether or not to accept to disclose their Personal Information.

171. Moreover, it is now recognized that client data has commercial value for companies, as it appears notably from an article published in the Journal of Direct, Data and Digital Marketing Practice, a copy of which is disclosed in support hereof as **Exhibit P-17**.

172. Due to Uber's fault, the Plaintiff and the Class Members are deprived of the choice whether or not to communicate this information and to select the persons to whom they wish to communicate it.

173. Through its conduct, Uber allowed the Hackers to appropriate data that has significant commercial value.

174. This situation also caused the Plaintiff, who makes a modest living and built his good credit over years, and for whom an identity theft and usurpation would have a significantly harmful impact, a great deal of anxiety.

175. Importantly, at no point in time did the Defendants inform the Plaintiff or the Class Members regarding whether measures had been put in place in order to secure the Personal Information made accessible to the Hackers following the Hack, choosing instead to intentionally conceal this information until March 12, 2018.

176. In fact, irrespective of whether their identity has been stolen or not, the Plaintiff and the Class Members, due to the Defendants' fault, were forced to invest time and money 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.

177. These inconveniences largely surpass the normal inconveniences associated with sharing Personal Information with a third party and the risks that accompany it.

178. The Plaintiff and the Class Members should not have to incur fees today to manage the damages that were caused by Uber's negligence.

179. The significance of the inconveniences associated with sharing of Personal Information was in this case directly increased by the Defendants, notably by their 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.

180. Finally, the fact that the Defendants knowingly hid from the Plaintiff and the Class Members the very existence of the Hack which concerned them, despite having been informed thereof, prevented them from mitigating their damages.

181. 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 Personal Information.

182. 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 Hackers' hands or has been communicated to other criminals.

183. The Plaintiff considers that these moral damages are the direct result of the Defendants' conduct, as illustrated notably in the article published in the *La Presse* newspaper, entitled "Identity theft: 'One should not underestimate the psychological

harm'" (original: Vol d'identité: *"Il ne faut pas sous-estimer le prejudice psychologique"*) dated August 1, 2019, a copy of which is disclosed in support hereof as **Exhibit P-18**.

184. In addition to moral damages, the Plaintiff and the Class Members also suffered pecuniary loss arising from the acts and omissions of the Defendants.

185. Indeed, at no point in time did Uber offer any assistance to the Plaintiff and the Class Members in order to help them mitigate damages and decrease the risk of identity theft or usurpation by, for example, providing easier access to programs for monitoring their credit file or at least furnishing information about it.

186. Due to the Defendants' conduct and the delays caused by the concealment of the Hack, the Plaintiff and the Class Members had to take draconian measures, going beyond the usual routine checks in order to remedy any actual or 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.

187. The Plaintiff and the Class Members had to incur fees in order to obtain advice regarding protection against and prevention of identity theft and usurpation, 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 remedy it.

188. More particularly in the case of the Plaintiff, these steps and the measures which had to be taken go well beyond normal inconveniences, and are totally 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 necessary measures to be taken more efficiently and at a lower cost.

189. To this end, on May 24, 2018, the Plaintiff took the necessary steps in order to obtain his Equifax credit file and score, spending $19.95 on account of fees, as it appears from the order confirmation, a copy of which is disclosed in support hereof as **Exhibit P-19**, and from the order history a copy of which is disclosed in support hereof as **Exhibit P-20**.

190. Uber also did not inform the Plaintiff nor any of the Class Members of the measures taken in order to limit the prejudice suffered, if any, and thus their increased vigilance will have to continue over time, thereby increasing the associated costs.

191. By paying the Hackers an amount of $100,000 USD, Uber also increased the risk of the Plaintiff and the Class Members' Personal Information being subjected to a future hack by persons also tempted to extort money from Uber.

192. The Defendants' acts and omissions, their faults, their failures to meet their legal and contractual and other obligations, are the cause of the Plaintiff and the Class Members' damages, including their moral and pecuniary damages.

193. Finally, the Defendants' conduct, as previously described, was not a first, was intentional and deliberate and demonstrated reckless and wanton disregard, a high degree of negligence and a blatant contempt for the safety, privacy and rights of the Plaintiff and the Class Members, justifying an order for punitive damages against them.

194. In these circumstances, it is imperative that the Defendants be required to pay punitive damages, the quantum of which must be high enough to cause them to change their behaviour, policies, procedures and practices in relation to the collection, holding, conservation, use and disclosure of Personal Information, as well as with respect to the notification of persons concerned in case of data theft.

195. The Defendants' recklessness is also demonstrated by the fact that they had already been the subject of a hack in 2014 and did not change their behaviour, policies, procedures and ways of doing things in that respect.

196. Even the *Federal Trade Commission*'s decision (Exhibit P-3) did not cause the Defendants to disclose this second Hack to those concerned.

197. In light of the foregoing, the Plaintiff is within his rights to ask for moral damages, in an amount *à parfaire*, in order to compensate for the stress and inconvenience caused by the Defendants' faults, as is the case for the other Class Members.

198. In light of the foregoing, the Plaintiff is also within his rights to ask for pecuniary damages, in an amount *à parfaire*, in order to compensate for the fees and expenses incurred due to the Defendants' faults, as is the case for the other Class Members

199. In light of the foregoing, the Plaintiff is also within his rights to ask for punitive damages, given the Defendants' reprehensible conduct which is incompatible with the objectives sought by the legislator in the […] CPA 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.*

200. The seriousness of the Defendants' faults, their patrimonial situation, estimated at about USD120 billion, as it appears from an article published on March 15, 2019 on the CNBC website, a copy of which is disclosed in support hereof as **Exhibit P-21**, and the relatively minimal extent of the damages that Uber would be have to pay if the Plaintiff and the Class Members succeed with their claims for moral and pecuniary damages, justifies that the Plaintiff and the Class Members claim $10,000,000 in punitive damages, amount *à parfaire*.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the Plaintiff's Originating Application;

CONDEMN the Defendants, solidarily, to pay the Plaintiff non-pecuniary damages, in an amount *à parfaire* 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 pecuniary damages, in an amount *à parfaire* 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 non-pecuniary damages, in an amount *à parfaire* 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 pecuniary damages, in an amount *à parfaire* 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 to pay to the Plaintiff and the Class Members the amount of $10,000,000 as punitive damages, in an amount *à parfaire*, 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.

Montreal, February 25, 2022

Woods s.e.n.c.r.l./LLP

WOODS LLP
Attorneys for the Plaintiff Pierre-Olivier Fortier
Mtre. Sarah Woods
Mtre. Carolan Villeneuve
2000, avenue McGill College, suite 1700
Montreal (Quebec) H3A 3H3
Tel. : 514 982-4545 | Fax. : 514 284-2046
Email : notification@woods.qc.ca
swoods@woods.qc.ca
cvilleneuve@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:	The complain and the 2017 decision of the Federal Trade Commission against Uber;
Exhibit P-4:	The complain and the revised decision dated October 2018;
Exhibit P-5:	Article published on Radio-Canada website;
Exhibit P-6:	Decision of the Office of the Information and Privacy Commissioner of Alberta dated February 28, 2018;
Exhibit P-7:	Email from Uber Canada inc. transmitted to the Plaintiff;
Exhibit P-8:	Copy of a decision dated November 6, 2018 in Dutch and the English translation thereof;
Exhibit P-9:	Notice of pecuniary sanction;
Exhibit P-10:	Deliberation of the restricted panel n^{o} SAN-2018-011;
Exhibit P-11:	Communication of the Department of Justice of the Northern District of California;
Exhibit P-12:	Article published in *La Presse*;

Exhibit P-13:	Criminal complaint;
Exhibit P-14:	Two privacy policies put in place between July 2015 and November 2017;
Exhibit P-15:	Articles published in *La Presse* and *Le Monde*;
Exhibit P-16:	Newspaper articles;
Exhibit P-17:	Article published in the Journal of Direct, Data and Digital Marketing Practice;
Exhibit P-18:	Article entitled *Vol d'identité : « Il ne faut pas sous-estimer le préjudice psychologique »*, published in *La Presse* on August 1, 2019;
Exhibit P-19:	Order confirmation;
Exhibit P-20:	Order confirmation history;
Exhibit P-21:	Article published on the CNBC website on March 15, 2019.

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.

Montreal, February 25, 2022

Woods s.e.n.c.r.l./LLP

WOODS LLP
Attorneys for the Plaintiff Pierre-Olivier Fortier
Mtre. Sarah Woods
Mtre. Carolan Villeneuve
2000, avenue McGill College, suite 1700
Montreal (Quebec) H3A 3H3
Tel. : 514 982-4545 | Fax. : 514 284-2046
Email : notification@woods.qc.ca
swoods@woods.qc.ca
cvilleneuve@woods.qc.ca

Nº : 500-06-000902-185

(Class Action Division)

SUPERIOR COURT
DISTRICT OF MONTREAL
PROVINCE OF QUEBEC

Pierre-Olivier Fortier, [redacted]

Plaintiff

– and –

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

Sub-class of users / Plaintiffs

– and –

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

Sub-class of drivers / Plaintiffs

v.

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

– et –

UBER TECHNOLOGIES INC., legal person with its principal establishment at 455 Market Street, suite 400, in San Francisco, in California, United States 941031

– et –

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

– et –

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

– et –

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

Defendants

AMENDED ORIGINATING APPLICATION

Nature : Class Action
Amount in dispute : 10 000 000 $

ORIGINAL

Mtre Sarah Woods
Mtre Carolan Villeneuve
Dossier nº : 6235-1

Woods LLP
Barristers & Solicitors
2000 McGill College Avenue, Suite 1700
Montréal, Québec H3A 3H3
T 514 982-4545 F 514 284-2046
Notification : notification@woods.qc.ca
Code BW 0208

Woods