C A N A D A

(Class Action)

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

SUPERIOR COURT

Nº : 500-06-001152-210

T S [redacted]

Plaintiff

v.

AUDI CANADA INC., legal person having its elected domicile at 900-1000, De La Gauchetière West, in the City and District of Montréal, Province of Québec, H3B4W5

-and-

VOLKSWAGEN GROUP CANADA INC., legal person having its elected domicile at 900-1000, De La Gauchetière West, in the City and District of Montréal, Province of Québec, H3B4W5

Defendants

CORRECTED AND AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION
(Art. 574 C.C.P. and following)

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:

INTRODUCTION

1. Plaintiff wishes to institute a class action on behalf of the following group, of which Plaintiff is a member, namely:

> All persons in Canada:
>
> (i) whose personal or financial information held by Volkswagen Canada Inc. or Audi Canada Inc. was compromised in a data breach which occurred on or before March 10, 2021, or
>
> (ii) who received an email or letter from Volkswagen Canada Inc. or Audi Canada Inc., dated on or about June 11, 2021, informing them of such data breach;
>
> or any other Group(s) or Sub-Group(s) to be determined by the Court;
>
> (hereinafter Class Members are collectively referred to as "**Class Member(s)**", "**Group Member(s)**", the "**Group**", the "**Class**", **"Customer(s)"** or "**Client(s)**").

2. Defendant Audi Canada Inc, which also does business under the names Automobiles Lamborghini Canada, Automobili Lamborghini Canada, and Audi Canada (hereinafter "**Audi Canada**" or "**Audi**"), is a Canadian corporation having an elected domicile in the City of Montreal, Province of Quebec, the whole as appears more fully from a copy of the *Registre des enterprises* (CIDREQ) report communicated herewith as **Exhibit R-1**.

3. Defendant Volkswagen Group Canada Inc., which also does business under the names Volkswagen Canada Inc., Volkswagen Canada, Groupe Volkswagen Canada, and Audi Canada (hereinafter "**Volkswagen Canada**" or "**VW**"), is also a Canadian corporation having an elected domicile in the City of Montreal, Province of Quebec, the whole as appears more fully from a copy of the *Registre des enterprises* (CIDREQ) report communicated herewith as **Exhibit R-2**.

4. Defendants, directly and/or through their related companies or parents in the Volkswagen family of companies worldwide, are well known for manufacturing, marketing, and selling automotive vehicles under various brands including without limitation the Volkswagen and Audi brands.

5. As appears from the R-1 and R-2 CIDREQ reports, Audi Canada Inc. is the wholly owned subsidiary of Volkswagen Group Canada Inc. and both entities do business under the

name “Audi Canada”.

The Situation

6. On or about March 10, 2021, Defendants were made aware that an unauthorized third party had accessed and obtained Customer information. Indeed, between August 2019 and May 2021, Defendants and/or one of their vendors/dealers/agents had apparently left unsecured certain electronic data and/or databases containing the private information of over 3.3 million customers and/or potential customers and/or past customers which had done business with VW or Audi between 2014 and 2019 (hereinafter the “**Data Breach**”), the whole as more fully appears from the Audi of America Notice of Data Breach (the “**Notice**”) dated June 11, 2021, communicated herewith as **Exhibit R-3**, and the letter addressed to the Attorney General of the State of Maine, Aaron Frey, dated June 10, 2021, communicated herewith as **Exhibit R-4**.

7. As appears from the Notice, the database and information which was accessed and stollen by the unauthorized third party includes some or all of the following:

- First and last name;
- Personal mailing address
- Business mailing address;
- Email address;
- Phone number;
- Driver’s license numbers;
- Date of Birth;
- Social Security or Social Insurance Numbers;
- Credit information (“eligibility for a purchase, loan, or lease”);
- Account or loan numbers,
- Tax identification numbers),
- Information about a vehicle purchased, leased, or inquired about, such as: Vehicle Identification Number (VIN), Make, Model, Year, Color, and Trim packages.

8. Defendants, who required the personal and financial information of its Customers in the context of a vehicle lease or finance, had the obligation to protect that information and to ensure by all proper and required means that this information is safeguarded from compromise, theft or loss.

9. When a data breach affecting approximately 3.3 million Consumers occurs, Defendants had the obligation to immediately and accurately notify its Customers in order to help

them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience.

10. This lawsuit stems from Defendants' failure to follow these obligations.

11. Defendants claim that on March 10, 2021, they were first made aware that their database had been breached by unknown parties. Plaintiff is presently not aware of the exact date(s) on which the Data Breach occurred nor on which date Defendants knew or should have known about the Data Breach.

12. Defendants also claim that the Data Breach and the type of information accessed were confirmed on May 24, 2021. However, Audi and VW inexplicably waited from March 10, 2021, namely at least 93 days, before publicly announcing the Data Breach on June 11, 2021.

13. The Data Breach was reported by multiple media outlets, as appears from the various articles reporting the issue communicated herewith as **Exhibit R-5**, *en liasse*.

14. Despite the fact that the Data Breach was announced in multiple media outlets, Defendants never published the link to the Notice on their websites or social media accounts. This decreased the likelihood that the Consumers would read the Notice and was surely intended to minimize the adverse effects of the Data Breach on VW and Audi sales.

15. Defendants were negligent in choosing to wait before actually notifying the affected Customers (Class Members), leaving them at greater risk of fraud and identity theft, although Defendants have and had the proper contact information and financial means in order to quickly reach the Class Members.

16. Moreover, Defendants failed to confirm that it would indemnify and hold the Class Members harmless of any losses or damages suffered as a result of the Data Breach.

17. Although Defendants (…) have offered 24 months of credit monitoring and $1,000,000 of insurance reimbursement policy to US residents through IDX Privacy Platform, Defendants failed to provide any protection to Canadian residents, the whole as more fully appears from the IDX information document titled "Recommended Steps to help Protect your Information", communicated herewith as **Exhibit R-6**.

18. The 24 months period is also inadequate since fraud can occur well after the first two year following the Data Breach, especially in instances were such a large number of

Customers are affected.

19. Defendants failed to mandate (and pay for) TransUnion Canada and Equifax Canada to automatically activate credit monitoring serviced or fraud alerts for Class Members, putting these Class Members at greater risk of fraud.

20. Defendants were negligent and committed faults in this regard since they failed to activate the TransUnion and Equifax services for their Canadian Customers, and many Class Members are not even aware of the Data Breach.

21. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class Members, Defendants clearly chose to save money instead of helping protect the Class Members. Indeed, there is a fee payable to TransUnion and Equifax Canada for activating credit monitoring services and/or to post a fraud alert but Defendants are not offering this and have not paid to automatically activate these services.

22. VW and Audi sought to impart a false sense of security to the Class Members by deceptively downplaying the Data Breach which involves the private information of approximately 3.3 million Customers in North America. Indeed, VW and Audi have falsely represented that only 90,000 Customers had "sensitive information" accessed and stollen.

23. After becoming aware of the Data Breach, VW and Audi waited more than twelve (12) weeks, namely until June 2021, before starting to contact some but not all of the Class Members in order to inform them of Data Breach.

24. Accordingly, Defendants failed to promptly and quickly disclose the Data Breach to the Class Members/victims of the Data Breach.

25. Personal information is a valuable commodity. There is a "cyber black-market" available for criminals to openly post personal information on a number of Internet websites in what is known as the "dark web". This demand increases the likelihood of Class Members falling victim to identity theft.

26. As a result of Defendants' inadequate data security, unauthorized third parties / cyber-criminals now possess the private information of Plaintiff and the Class Members.

27. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting more than twelve (12) weeks pass before starting to notify Class Members (with many not even informed yet), VW and Audi failed

to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class Members.

28. VW and Audi Customers have been and/or will be exposed to fraud and/or identity theft and these Customers have been harmed as a result. Harm to victims of the Data Breach includes without limitation fraudulent charges on their accounts, disbursements incurred such as for purchasing extra insurance, placing a fraud alert on their credit file, loss time and expenses related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards or bank accounts; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; and (e) the general nuisance and annoyance of dealing with all these issues resulting from the Data Breach;

29. On top of actual monetary losses related to fraud and identity theft, Plaintiff and the Class Members have already and/or will continue to experience stress, anxiety, fear, inconvenience and/or loss of time due to the loss of their personal information, which has made Plaintiff and the Class Members potential targets for fraud and/or identity theft.

30. The Plaintiff and the Class Members have suffered or will suffer certain additional inconveniences and damages including but not limited to the following:

a) Delays in the processing of any future requests or applications for credit in the future;

b) The obligation to closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, for many months or years;

c) The obligation to be even more attentive than normally necessary concerning the communication of their personal information since they are at threat of social engineering and phishing, due to the higher possibility of fraudulent activity caused by Defendants' loss of the information;

d) The obligation to inform their financial institutions of the loss of the information by the Defendants and to deal with said financial institutions in order to reduce risk of fraud as much as possible. In this regard, certain Class Members have and/or will close their accounts and open new accounts in order to protect themselves, which will cause further loss of time, inconvenience and costs;

e) Obtaining and reviewing their credit reports, regularly, in order to look for unauthorized transactions or fraud;

f) A negative effect on their credit score.

31. Many Class Members have also paid or will pay certain fees or costs in order to further protect themselves, such as in order to activate a credit monitoring service or in order to purchase fraud insurance or alerts, title or other insurance, to change their personal information such as requesting new driver's licence numbers or Social Insurance Numbers, for credit protection consulting services, etc. Defendants are solely responsible for these costs or fees paid by the Class Members and for the inconvenience caused to Class Members in this regard.

32. Plaintiff invokes *inter alia* the following sections of provincial and federal legislation which apply under the circumstances and Plaintiff respectfully submits that the mere fact that the personal information was entrusted to the Defendants and subsequently lost by Defendants as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which makes Defendants liable to pay compensatory, moral and punitive damages:

a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, S.Q. 1991, c. 64*;*

b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, CQRL, c. C-12;

c) Sections 1, 2, 10, 13 and 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c. P-39.1;

d) Sections 2, 3, 5 and 11 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5, as well as its sections 4.1, 4.3, 4.7 to 4.7.4 of its Schedule 1;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF

33. Plaintiff reiterates the above allegations in the present section, as though recited at length.

34. At the end of 2015, Plaintiff leased a new 2016 Audi A3 from the Audi Prestige dealership located in Saint-Laurent, Quebec, and provided her personal and financial information to the dealership and Defendant Audi Canada Inc. (and/or its related entities)

35. Plaintiff read the TechCrunch.com article contained in R-5 titled "Volkswagen Says a Vendor's Security Lapse Exposed 3.3 Million Drivers' Details" published on June 11,

2021, and contacted undersigned attorney to mandate them to institute the present class action proceedings on her behalf and on behalf of the Class Members.

36. In order to help protect herself from fraud and identity theft, Plaintiff (…) purchased the recurring monthly subscription of the Equifax Canada Complete Premier credit monitoring services, at a price of $21.94 per month (namely $19.95 plus taxes), which amounts she claims from Defendants as damages stemming directly from the Data Breach, the whole as more fully appears from her Equifax Canada email confirmation dated June 14, 2021, communicated herewith as **Exhibit R-7**. Plaintiff also activated the Equifax Canada 6-year fraud alert on her credit file on June 14, 2021, the whole in order to further protect her credit files and identity.

37. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Defendants would properly safeguard their personal and financial information, which Defendants clearly did not.

38. As a result of learning that her personal information was lost by Defendants, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information.

39. In order to save money, Defendants have failed or refused to mandate and pay for TransUnion and Equifax Canada to immediately and automatically activate credit monitoring and fraud alerts for all affected Class Members such as Plaintiff.

40. All fees payable to TransUnion or Equifax Canada in order to activate these alerts are hereby claimed by Plaintiff and the Class Members from Defendants as damages.

41. TransUnion and Equifax Canada are the two (2) only credit agencies in Canada, both of which Defendants failed to contact immediately about the Data Breach affecting Plaintiff and other Class Members.

42. In addition, considering that the personal information of over 3.3 million VW and Audi Customers have been accessed and stollen by unauthorized third parties, it will take much longer that 1 to 2 years for the thieves to use and/or sell all of the stollen client information. Defendants are clearly responsible to indemnify and hold the Class Members harmless of all losses and damages suffered since the Data Breach.

43. Defendants had the obligation to ensure, by the most technologically sophisticated means possible and available, that said information was protected and could not be accessed. Defendants failed in this regard and failed to secure this private and highly sensitive information and their negligence and carelessness facilitated the Data Breach, making

Defendants liable to pay compensatory, moral and punitive damages.

44. Indeed, the R-3 Notice and R-4 letter confirms that the Class Members' personal and financial information was left "unsecured" for almost two (2) years, namely from August 2019 to May 2021.

Punitive Damages:

45. For all of the reasons more fully detailed above, which are reiterated as though recited at length in the present section, Plaintiff respectfully submits that Defendants were grossly and/or intentionally negligent and are liable to pay punitive damages to the Class Members.

46. In fact, without limiting the generality of the forgoing, Defendants were grossly negligent and/or intentionally negligent when they:

a. did not follow or properly implement an effective data security industry standard to protect the Class Members' highly sensitive personal and financial information, which information VW and Audi allowed to be accessed and/or downloaded/stollen by unauthorized third parties;

b. failed to promptly and clearly notify the Plaintiff and the Class Members of the Data Breach;

c. failed to properly ensure that Plaintiff and Class Members are protected by credit monitoring services by both Equifax Canada and TransUnion and failing to post fraud alerts on the Class Members' credit files immediately after the Data Breach;

d. failed to timely detect and prevent the Data Breach itself until on or about March 10, 2021 whereas it apparently occurred from August 2019 to May 2021 (leaving the Class Members' information at risk and "unsecured" for almost two (2) years);

e. failed to even provide protection (Equifax or TransUnion) to Class Members;

f. failed to offer indemnification for losses suffered by Class Members.

47. Considering the above and considering the fact that Defendants have violated various laws which have been enacted in order to protect the Class Members' personal and/or financial information, Defendants are liable to pay punitive damages to all of the Class

Members due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class Members.

48. Defendants' above detailed actions qualify the fault as intentional which is a result of wild and foolhardy recklessness in disregard for the rights of the Class Members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class Members.

49. Defendants' negligence has shown a malicious, oppressive and high-handed conduct that represents a marked departure from ordinary standards of decency. In that event, punitive damages should be awarded to Class Members.

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE CLASS MEMBERS

50. Plaintiff reiterates the above allegations in the present section, as though recited at length.

51. Class Member had their personal information lost by Defendants as described hereinabove, including without limitation first and last name, personal or business mailing address, email address, phone number, driver's license numbers, date of birth, social Security or Social Insurance Numbers, credit information ("eligibility for a purchase, loan, or lease"), account or loan numbers, tax identification numbers, vehicle Identification Number (VIN), Make, Model, Year, color, and trim packages.

52. Every Class Member has or will experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information.

53. Every Class Member had and has to closely monitor his or her accounts looking for possible fraud from now on and for all periods subsequent to the loss of information.

54. Every Class Member will be inconvenienced by any safety measures that may become necessary in order to prevent further fraud exposure, such as signing up for credit monitoring service, posting an alert on their accounts or credit files, changing their personal information or account numbers, transferring money from one account to another, closing and opening accounts, paying for and dealing with NSF or other bank charges or interest, etc.

55. Furthermore, every Class Member may be required to pay costs or fees in order to sign up for such credit monitoring, to post an alert on their accounts or credit files, to change

their personal information, to purchase insurance, or in order to otherwise protect themselves from further fraud exposure.

56. The Class Members' credit score has and/or will be negatively affected.

57. Moreover, as mentioned above, it is likely that many Class Members have not been notified of the loss of their information, making them still at great risk of fraud or identity theft.

58. Every Class Member can still fall victim to fraud or identity theft, in the future, due to Defendants' negligence in the safekeeping of their personal information and negligence in the way it handled itself after being made aware of this Data Breach.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

59. The composition of the Group makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (Article 575 (3) C.C.P.) for the following reasons.

60. Plaintiff is unaware of the specific number of persons included in the Class but, as mentioned above, it appears that the personal and/or financial information (including first and last name, personal mailing address, business mailing address, email address, phone number, driver's license numbers, date of birth, social Security or Social Insurance Numbers, credit information ("eligibility for a purchase, loan, or lease"), account or loan numbers, tax identification numbers, vehicle Identification Number (VIN), Make, Model, Year, color, and trim packages) of 3.3 million of Defendants'(…) Customers in Canada and the U.S.A. has been lost, stolen or otherwise compromised as a result of the Data Breach.

61. Plaintiff estimates that hundreds of thousands of Canadian Class Members have been impacted by the Data Breach.

62. Class Members are numerous and are scattered across the entire province and country since Defendants lease and finance automotive vehicles across the country, including Quebec.

63. In addition, given the costs and risks inherent in an action before the Courts, many people will hesitate to institute an individual action against the Defendants. Even if the Class Members themselves could afford such individual litigation, the Court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues

raised by the conduct of the Defendants would increase delay and expense to all parties and to the Court system;

64. Moreover, a multitude of actions instituted risks leading to contradictory judgments on issues of fact and law that are similar or related to all Class Members;

65. These facts demonstrate that it would be impractical, if not impossible, to contact each and every Class Member to obtain mandates and to join them in one action;

66. In these circumstances, a class action is the only appropriate procedure for all of the Class Members to effectively pursue their respective rights and have access to justice;

67. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely Defendants'(…) negligence, and fault;

68. The claims of the Class Members raise identical, similar or related issues of law and fact (Article 575 (1) C.C.P.), namely:

(a) Did Defendants commit a fault regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendants commit a fault by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendants commit a fault due to the deficiencies of the notices given to Class Members about the Data Breach?

(d) Are Defendants liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

69. The interests of justice favour that this application be granted in accordance with its conclusions.

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

70. The action that Plaintiff wishes to institute for the benefit of the Class Members is an action in damages.

71. The facts alleged herein appear to justify the conclusions sought by the Plaintiff (Article 575 (2) C.C.P.), namely the following conclusions that Plaintiff wishes to introduce by way of an originating application:

> **GRANT** the Class Action of Plaintiff on behalf of all the Class Members against Defendants;
>
> **CONDEMN** Defendants to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendants to pay to the Class Members punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;
>
> **THE WHOLE** with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

72. Plaintiff suggests that this class action be exercised before the Superior Court in the District of Montreal for the following reasons:

a) Plaintiff resides in the District of Montreal;

b) A great number of Class Members reside in the judicial District of Montreal and/or provided their personal and financial information to Defendants in the District of Montreal;

c) Defendants carries on business, including the leasing and financing of vehicles, in the District of Montreal;

d) Defendants have elected domicile in the District of Montreal (Exhibits R-1 and R-2);

e) The undersigned attorneys representing the Plaintiff and the proposed Class practice in the District of Montreal;

73. Plaintiff, who is requesting to be appointed as Representative Plaintiff, is in a position to

properly represent the Class Members (Article 575 (4) C.C.P.), since:

a) Her personal information was lost by Defendants as described hereinabove;

b) She has already and will continue to suffer anxiety, inconvenience, stress, loss of time, and fear, as well as out of pocket expense, as a result of said loss of information;

c) She may in the future fall, victim to fraud and/or identity theft because of Defendants' loss of her personal information;

d) She understands the nature of the action and has the capacity and interest to fairly and adequately protect and represent the interest of the Class Members;

e) She is available to dedicate the time necessary for the present action before the Courts of Quebec and to collaborate with Class Counsel in this regard and Plaintiff is ready and available to manage and direct the present action in the interest of the Class Members that Plaintiff wishes to represent;

f) Plaintiff is determined to lead the present file until a final resolution of the matter, the whole for the benefit of the Class Members;

g) Her interests are not antagonistic to those of other Class Members;

h) She has given the mandate to the undersigned attorneys to obtain all relevant information to the present action and intends to keep informed of all developments;

i) She has given the mandate to the undersigned attorneys to post the present matter on their firm website in order to keep the Class Members informed of the progress of these proceedings and in order to more easily be contacted or consulted by said Class Members.

j) She, with the assistance of the undersigned attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other Class Members and to keep them informed;

74. The present application is well founded in fact and in law;

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the present Application;

AUTHORIZE the bringing of a class action in the form of an Application to institute proceedings in damages in the District of Montreal;

APPOINT the Plaintiff as the Representative Plaintiff representing all persons included in the Class herein described as:

All persons in Canada:

(i) whose personal or financial information held by Volkswagen Canada Inc. or Audi Canada Inc. was compromised in a data breach which occurred on or before March 10, 2021, or

(ii) who received an email or letter from Volkswagen Canada Inc. or Audi Canada Inc., dated on or about June 11, 2021, informing them of such data breach;

or any other Group(s) or Sub-Group(s) to be determined by the Court;

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

(a) Did Defendants commit a fault regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendants commit a fault by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendants commit a fault due to the deficiencies of the notices given to Class Members about the Data Breach?

(d) Are Defendants liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

IDENTIFY the conclusions sought by the class action to be instituted as being the following:

GRANT the Class Action of Plaintiff on behalf of all the Class Members against Defendants;

CONDEMN Defendants to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendants to pay to the Class Members punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;

THE WHOLE with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

DECLARE that all Class Members who have not requested their exclusion from the Class in the prescribed delay to be bound by any Judgment to be rendered on the class action to be instituted;

FIX the delay of exclusion at 30 days from the date of the publication of the notice to the Class Members;

ORDER the publication or notification of a notice to the Class Members in accordance with Article 579 C.C.P., within sixty (60) days from the Judgment to be rendered herein in digital edition of the LaPresse, the Journal de Montreal, the Journal de Quebec, The National Post, the Globe and Mail, and the Montreal Gazette, and **ORDER** Defendants solidarily to pay for all said publication/notification costs;

ORDER that said notice be posted and available on the home page of Defendants' various websites, Facebook page(s), and Twitter account(s), including without limitation the Audi and Volkswagen websites, and **ORDER** Defendants to send the notice by email with proof of receipt and by direct mail to all Class Members;

THE WHOLE with costs including without limitation the Court filing fees herein and all costs related to preparation and publication of the notices to Class Members.

MONTREAL, June 14, 2021

(S) Lex Group Inc.

Lex Group Inc.
Per: David Assor and Joanie Lévesque
Class Counsel / Attorneys for Plaintiff
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7
Telephone: 514.451.5500 ext. 321
Fax: 514.940.1605

Nº.: 500-06-001152-210

(Class Action Division)
SUPERIOR COURT

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

T[redacted] S[redacted]

Plaintiff

v.

AUDI CANADA INC.

-and-

VOLKSWAGEN GROUP CANADA INC.

Defendants

CORRECTED AND AMENDED
APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION

ORIGINAL

Me David Assor

BL 5606

Lex Group Inc.
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7

T: 514.451.5500
F: 514.940.1605
@: davidassor@lexgroup.ca