CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

Nº : 500-06-001152-210

(Class Action)

SUPERIOR COURT

TANIA SCISCENTE

Plaintiff

v.

AUDI CANADA INC.

Defendant

ORIGINATING CLASS ACTION APPLICATION

IN SUPPORT OF HER AUTHORIZED CLASS ACTION, THE REPRESENTATIVE PLAINTIFF RESPECTFULLY STATES THE FOLLOWING:

INTRODUCTION

1. By way of the Superior Court of Quebec's Authorization Judgment dated August 1, 2022 (the "**Authorization Judgment**"), the class action herein has been authorized against the Defendant and Plaintiff was appointed as the Representative Plaintiff representing all persons included in the Class described as follows:

> All Quebec residents:
>
> (i) whose personal or financial information held by 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 Audi Canada Inc., dated on or about June 11, 2021, informing them of such data breach.

2. The main issues of fact and law to be treated collectively have been identified by this Honorable Court in the Authorization Judgment as follows:

   a) Did Audi Canada Inc. commit a fault regarding the storage and the safe-keeping of the personal information of the Class Members?

   b) Did Audi Canada Inc. commit a fault by delaying the notification to Class Members that a Data Breach had occurred?

   c) Did Audi Canada Inc. commit a fault due to the deficiencies of the notices given to Class Members about the Data Breach?

   d) Is Audi Canada Inc. liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

3. 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 P-1**.

4. Audi, directly and/or through its related companies, is well known for manufacturing, marketing, selling, and leasing automotive vehicles under various brands.

5. Audi, 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.

6. When a data breach affecting approximately 3.3 million Consumers occurs, Audi 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.

7. This authorized class action lawsuit stems from Audi's failure to follow these obligations.

The Data Breach

8. On or about March 10, 2021, Defendant (and/or one of its related compagnies) was made aware that an unauthorized third party had accessed and obtained

Customer information. Indeed, between August 2019 and May 2021, Defendant and/or its related compagnies/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 Audi (and/or its related compagnies) 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 P-2**, and the letter addressed to the Attorney General of the State of Maine, Aaron Frey, dated June 10, 2021, communicated herewith as **Exhibit P-3**.

9. The database and information which was accessed and stollen included some or all of the following information, regarding "Audi" and Volkswagen ("**VW**") clients in Canada and the USA:

- 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.

10. Audi claims that it was only on March 10, 2021, it was first made aware that its database had been breached by unknown parties.

11. Defendant also claims that it was apparently not able to ascertain the exact date(s) on which the Data Breach occurred.

12. Defendant also claims that the Data Breach and the type of information accessed were confirmed on May 24, 2021. However, Audi inexplicably waited 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 P-4**, *en liasse*.

14. Despite the fact that the Data Breach was announced in multiple media outlets, Defendant 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 Audi sales.

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

16. Moreover, Defendant 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. Defendant (together with its related US companies) offered 24 months of "IDX" credit monitoring services and a $1,000,000 insurance reimbursement policy to US resident clients which were included in the Data Breach, the whole as confirmed in Exhibit P-2 and as also appears from the IDX information document titled "Recommended Steps to help Protect your Information", communicated herewith as **Exhibit P-5**.

18. That being said, Defendant abusively refused to provide any similar protections to Canadian resident clients who were also included in the very same Data Breach.

19. Defendant therefore refused to mandate (and pay for) TransUnion Canada and Equifax Canada to automatically activate credit monitoring services and fraud alerts for Class Members, putting these Class Members at greater risk of fraud.

20. Defendant was negligent and committed faults in this regard since it failed and/or refused to activate the TransUnion and Equifax services for their Canadian customers, and many Class Members are not even aware of the Data Breach.

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

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

23. 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.

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

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

26. Harm, inconveniences and damages suffered by victims of the Data Breach includes without limitation the following:

    a) Fraud and/or identity theft, including fraudulent charges on their accounts and/or unreimbursed fees;

    b) Professional fees disbursed;

    c) Disbursements incurred such as for purchasing extra insurance or signing up for and paying for credit monitoring services;

    d) Placing a fraud alert on their credit file, and costs related thereto;

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

f) The obligation to closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, which will be much longer than 24 months;

g) 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 Defendant's loss of the information;

h) The obligation to inform their financial institutions of the loss of the information by the Defendant and to deal with said financial institution 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;

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

j) A negative effect on their credit score;

k) Loss of time and expenses related to (i) finding fraudulent charges; (ii) cancelling and reissuing cards or bank accounts; (iii) credit monitoring and identity theft prevention; (iv) imposition of withdrawal and purchase limits on compromised accounts; and (vi) the general nuisance and annoyance of dealing with all these issues resulting from the Data Breach.

27. In addition, 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.

28. Plaintiff and many Class Members have also paid certain fees or costs in order to further protect themselves, such as in order to activate a more advanced credit monitoring service and for a longer period than the one offered by Defendant, or in order to purchase fraud insurance, title insurance, to change their personal information such as requesting new driver's licence numbers or Social Insurance Numbers. Defendant is solely responsible for these costs or fees paid by the Plaintiff and/or other Class Members and for the inconvenience caused to Class Members in this regard.

29. Plaintiff and the Class Members are justified in claiming and have also been authorized to claim punitive damages against Defendant, as confirmed in the Authorization Judgment.

The Representative Plaintiff

30. 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 (and/or its related entities).

31. Plaintiff read a TechCrunch.com article titled "Volkswagen Says a Vendor's Security Lapse Exposed 3.3 Million Drivers' Details" published on June 11, 2021 (included in P-4).

32. Accordingly, in the case of Plaintiff and many other Class Members, these Class Members remained uninformed of the Data Breach and highly vulnerable to fraud and identity theft for over two (2) years, namely from August 2019 to at least May/June 2021 (if not longer).

33. Audi completely failed to notify Plaintiff at all of the Data Breach which included her personal information. Indeed, it was only during the pre-authorization process in the present proceedings that Audi confirmed that Plaintiff's personal information was indeed included in the Data Breach.

34. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Defendant would properly safeguard their personal information as part of their vehicle lease or finance contract, which Defendant clearly did not.

35. Since being made aware of the Data Breach involving her personal information, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear.

36. Although Defendant has offered 24 months of credit monitoring services and $1,000,000 of insurance reimbursement policy to US residents included in the Data Breach (as detailed above), Audi never mandated (and never paid for) TransUnion Canada and/or Equifax Canada to automatically activate credit monitoring services or fraud alerts for the Plaintiff and Class Members, putting them at greater risk of fraud.

37. In order to help protect herself and her credit file from fraud and identity theft, and as a direct result of the Data Breach herein, Plaintiff purchased the recurring monthly subscription of the Equifax Canada Complete Premier credit monitoring services, as of June 14, 2021, at a price of $21.94 per month

(namely $19.95 plus taxes), which amounts she claims from Defendant 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 P-6**.

38. 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 file and identity.

39. Plaintiff spent many hours on the telephone with Equifax Canada representatives (multiple calls) in order to activate these protective services. A loss of time Defendant is liable to compensate.

40. In order to save money, Defendant has 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.

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

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

43. In addition, considering that the personal information of over 3.3 million customers have been accessed and stollen by unauthorized third parties, it will take much longer than 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.

44. Defendant had the obligation to ensure, by the most technologically sophisticated means possible and available, that said information was protected and could not be accessed. Defendant failed in this regard and failed to secure this private and highly sensitive information and their negligence and carelessness facilitated the Data Breach, making Defendant liable to pay compensatory, moral and punitive damages.

Punitive Damages

45. For all of the reasons more fully detailed above, including those contained in the Superior Court's August 1, 2022 Authorization Judgment herein, which are reiterated as though recited at length in the present section, Plaintiff respectfully submits that Defendant was grossly and/or intentionally negligent and is liable to pay punitive damages to the Class Members.

46. In fact, without limiting the generality of the forgoing, Defendant was grossly negligent and/or intentionally negligent when it:

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 Audi allowed to be accessed and/or downloaded/stollen by unauthorized third parties;

b. 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);

c. failed to promptly and clearly notify the Plaintiff and the Class Members of the Data Breach. Indeed, Defendant never notified Plaintiff;

d. 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;

e. failed to provide insurance protection to Class Members;

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

g. failed to provide any updates to the Class Members after its investigation into the Data Breach.

47. Defendant's decision not to provide Plaintiff and Class Members with credit monitoring services and insurance (as was offered to Americans) and Defendant's decision not to post fraud alerts on the Class Members' credit files, further warrant and support a condemnation for punitive damages herein.

48. Defendant's excessive delays, faults and failures in the investigation and notification process after the Data Breach also further warrant and support a condemnation for punitive damages herein.

49. Considering the above and considering the fact that Defendant has violated various laws which have been enacted in order to protect the Class Members' personal and/or financial information, Defendant is liable to pay punitive damages to all of the Class Members due to the loss of private information itself, aside from any other compensatory damages suffered by the Class Members.

50. Defendant's 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.

51. Defendant's 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.

The Class Members

52. Class Member had their personal and financial information lost by Defendant 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.

53. Some Class Members incurred out of pocket expenses as a result of the Data Breach and/or as a result of receiving a notification letter, which expenses are claimed herein.

54. Class Members have experienced stress, anxiety, inconvenience, loss of time, and/or fear as a result of the Data Breach and/or as a result of receiving a notification letter (if they received such a letter at all).

55. Class Members had to and have to closely monitor their accounts looking for possible fraud for all periods subsequent to the loss of information.

56. Class Members have been inconvenienced by the safety measures that became 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.

57. Furthermore, Class Members who paid 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 claim the reimbursement of these costs and fees from Defendant.

58. Class Members' credit score has and/or will be negatively affected as a result of the Data Breach, a further damage claimed herein.

59. 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 greater risk of fraud or identity theft.

60. Class Members can still fall victim to fraud or identity theft, in the future, due to Defendant's negligence in the safekeeping of their personal information.

61. The Representative Plaintiff and the Class Members are therefore justified and entitled to claim compensatory, moral and punitive damages against the Defendant.

62. The present action is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

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

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

CONDEMN Defendant 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.

MONTREAL, October 26, 2022

Lex Group Inc.

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

SUMMONS

(Articles 145 and following C.C.P.)

Filing of a judicial application

Take notice that the Plaintiff(s) has filed this application in the office of the Superior Court of Quebec 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 Est, Montréal, Québec 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 judgment 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 application, the Plaintiff intends to use the following exhibits:

Exhibit P-1: Copy of the *Registraire des entreprises* CIDREQ reports regarding Defendant Audi Canda Inc.;

Exhibit P-2: Notice of Data Breach, dated June 11, 2021;

Exhibit P-3: Letter addressed to the Attorney General of the State of Maine, Aaron Frey, dated June 10, 2021;

Exhibit P-4: Various news articles, *en liasse;*

Exhibit P-5: IDX information document titled "Recommended Steps to help Protect your Information;

Exhibit P-6: Equifax Canada confirmation email to the Plaintiff, dated June 14, 2021;

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.

DO GOVERN YOURSELF ACCORDINGLY.

MONTREAL, October 26, 2022

Lex Group Inc.

Lex Group Inc.
Per: David Assor and Sarah Rasemont
Class Counsel / Attorneys for Representative Plaintiff

№.: 500-06-001152-210

SUPERIOR COURT
(CLASS ACTION)

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

TANIA SCISCENTE

Plaintiff

-vs-

AUDI CANADA INC.

Defendant

ORIGINATING CLASS ACTION APPLICATION

ORIGINAL

Me David Assor

LEX GROUP
AVOCATS · ATTORNEYS
WWW.LEXGROUP.CA

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

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

BL 5606