SUPERIOR COURT

CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

No: 500-06-001152-210

DATE: August 1, 2022

PRESIDING THE HONOURABLE THOMAS M. DAVIS, J.S.C.

TANIA SCISCENTE

Plaintiff

v.

AUDI CANADA INC.
and
VOLKSWAGEN GROUP CANADA INC.

Defendants

JUDGMENT

OVERVIEW

[1] Plaintiff Tania Sciscente seeks the Court's authorization for a pan-Canadian class action, following an alleged data breach of personal information in relation to clients or

potential clients of Defendants, Audi Canada Inc. **(Audi)** and Volkswagen Group Canada Inc. **(VW)**. The breach is believed to have occurred sometime prior to March 2021.

[2] She sets out the proposed class as follows:

> 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;

1. THE ALLEGED DATA BREACH

[3] Ms. Sciscente describes the breach as follows:

> 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")...

[4] Her description of the breach must be put into the proper context, both given the evidence that Ms. Sciscente adduced, as well as the evidence authorized by the Court.

[5] The 3.3 million customers whose data may have been compromised were located throughout North America.

[6] The authorization application was filed in the immediate wake of notices having been disseminated in the United States of America as of June 10, 2021 by Volkswagen Group of America, Inc. and its operating divisions, Audi of America and Volkswagen of America. The security incident affected certain customers and interested buyers in the United States of America and attracted media attention there as of June 11, 2021. These notices include the Audi of America Notice,[1] a letter addressed to the Attorney General of the State of Maine,[2] and an IDX information document titled "Recommended Steps to Help Protect Your Information.[3]

---

1 Exhibit R-3.
2 Exhibit R-4.
3 Exhibit R-6.

[7] As explained in the affidavit of Douglas Black, authorized by the Court, it appears that the data security incident was different, from a Canadian and Quebec perspective:

> a) On March 10, 2021, Audi was alerted that an unauthorized third party "may" have obtained certain customer information;
>
> b) An investigation was immediately commenced and the source of the incident was identified in May 2021;
>
> c) The data security incident relates to information in support of sales and marketing, from 2014 and 2019 and include:
>
> > i. First and last names, personal or business mailing addresses, email addresses or phone numbers;
> >
> > ii. In some instances, vehicle identification number (VIN), make, model, year, colour, and trim packages.
>
> d) The data security incident affected certain Audi customers and interested buyers, but did not affect individuals who purchased or leased a Volkswagen-branded vehicles, nor interested buyers of Volkswagen vehicles in Quebec or Canada.

[8] This information was confirmed by Mr. Black when he was examined on his affidavit.

[9] Audi sent a letter to the affected Canadians, including Ms. Sciscente. Here are the highlights:

> **What happened?**
>
> On March 10, 2021, we were alerted that an unauthorized third party may have obtained certain customer information.
>
> We immediately commenced an investigation to determine the nature and scope of this event. The investigation confirmed that the third party obtained limited personal information received from or about customers and interested buyers from a vendor used by Audi, Volkswagen, and some authorized dealers in the United States and Canada. This included information gathered for sales and marketing purposes from 2014 to 2019. We believe the data was obtained when the vendor left electronic data unsecured at some point between August 2019 and May 2021, when we identified the source of the incident.
>
> **We have confirmed that your personal information was included in this incident.**
>
> **What information was included?**

> The data included some or all of the following contact information about you: first and last name, personal or business mailing address, email address, or phone number. In some instances, the data also included information about a vehicle purchased, leased, or inquired about, such as the Vehicle Identification Number (VIN), make, model, year, color, and trim packages.[4]

[10] The letter was not sent to VW customers, as Defendants concluded that the incident only affected Audi customers in Canada.

[11] Ms. Sciscente denies receiving the letter and says that she learned about the breach in a TechCrunch.com article titled *"Volkswagen Says a Vendor's Security Lapse Exposed 3.3 Million Drivers' Details"* published on June 11, 2021.[5]

[12] In order to help protect herself from fraud and identity theft, she purchased a recurring monthly subscription of the Equifax Canada Complete Premier credit monitoring services, at a price of $21.94 per month including taxes and 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.

[13] During the examination authorized by the Court Ms. Sciscente stated that she purchased the protection following her reading of the article and a discussion with her lawyer, who advised her that it was one way to protect herself. The conversation and decision to purchase it occurred on Sunday June 13, 2021.

[14] She tried to complete the purchase but had issues with a verification code such that she could only complete it on Monday June 14 at the end of the day. With respect to the purchase of the protection purchased from Equifax, she notes that the Modified Authorization Application was only filed on June 15, 2021, after the purchase of the additional protection.

[15] Ms. Sciscente claims that she was not notified of the breach on a timely basis and that when notification did occur, it was deficient. Furthermore, Canadians victimized by the breach have not been offered appropriate protection against the potential damages of the breach, such as fraud or identity theft.

[16] She claims compensatory and punitive damages alleging a failure of Audi and VW to respect the following laws:

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;

---

4 Douglas Black confirms in his affidavit that this was the information that was breached in relation to Canadian customers.

5 Exhibit R-5.

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;[6]

2. ANALYSIS

2.1 Introduction

[17] The Court's role at the authorization stage is to filter out frivolous applications. This is well explained by the Supreme Court of Canada in *L'Oratoire Saint-Joseph du Mont-Royal c. J.J.*:

> [56] Article 575(2) *C.C.P.* provides that the facts alleged in the application must "appear to justify" the conclusions being sought. This condition, which was not included in the original bill on class actions, was added in response to pressure from certain companies [translation] "that feared it would give rise to a significant volume of frivolous actions": V. Aimar, "L'autorisation de l'action collective: raisons d'être, application et changements à venir", in C. Piché, ed., *The Class Action Effect* (2018), 149, at p. 156 (emphasis added); P.-C. Lafond, "Le recours collectif: entre la commodité procédurale et la justice sociale" (1998-99), 29 *R.D.U.S.* 4, at p. 24. It is now well established that at the authorization stage, the role of the judge is to screen out *only* those applications which are "frivolous", "clearly unfounded" or "untenable": *Sibiga*, at paras. 34 ("the judge's function at the authorization stage is only one of filtering out untenable claims" (emphasis added)), 52 ("[a] motion judge should only weed out class actions that are frivolous or have no prospect of success" (emphasis added)) and 78 ("it was enough to show that the appellant's claim was not a frivolous one and that, at trial, she would have an arguable case to make on behalf of the class" (emphasis added)); see also *Charles*, at para. 70; Lafond (2006), at pp. 112 ([translation] "the purpose of [art. 575(2) *C.C.P.*] is first, 'to immediately eliminate actions that are *prima facie* frivolous' and, second, to 'dispose in the same way of actions that, although not frivolous, are clearly unfounded'") and 116 ("the authorization stage exists solely to screen out applications that are frivolous or clearly unfounded in fact or in law, as the legislature originally intended"); see also *Fortier*, at para. 70; *Oubliés du viaduc de la Montée Monette v. Consultants SM Inc.*, 2015 QCCS 3308, at para. 42 (CanLII). As this Court explained in *Infineon*, "the court's role is merely to filter out frivolous motions", which it does "to ensure that parties are not being subjected unnecessarily to litigation in which they must defend against untenable claims": para. 61 (emphasis added); see also paras. 125 ("a judge hearing a motion for authorization is responsible for weeding

---

[6] Modified Authorization Application, par. 32.

out frivolous cases") and 150 ("the purpose of the authorization stage is merely to screen out frivolous claims").[7]

2.2 Paragraph 575(1) C.C.P.

[18] The purpose of article 575(1) C.C.P. is to ensure that the members of the proposed class are united by one or more identical, similar or related issues of law or fact.[8] The members of the proposed class must share a common interest in at least one question. The answer to the common question should be capable of resolving a significant portion of the dispute. Finally, the common interest is to be interpreted generously and flexibly.[9]

[19] It is also important to note that only common questions are required (even just one). The answers need not be identical for all class members.[10] Nor, as the Supreme Court of Canada said in *Infineon Technologies AG* v. *Option consommateurs*, do the experiences and circumstances of all class members need to be perfectly identical:

> [73] There is no requirement that each member of a group be in an identical or even a similar position in relation to the defendant or to the injury suffered. Such a requirement would be incompatible with the concern for judicial economy which the class action serves by avoiding duplicated or parallel proceedings (see *Western Canadian Shopping Centres Inc. v. Dutton*, 2001 SCC 46, [2001] 2 S.C.R. 534, at para. 27). The Court of Appeal summarized this as follows in *Guilbert v. Vacances sans Frontière Ltée*, 1991 CanLII 2869 (QC CA), [1991] R.D.J. 513:
>
> > [translation] The fact that the situations of all members of the group are not perfectly identical does not mean that the group does not exist or is not uniform. To be excessively rigorous in defining the group would render the action useless . . . in situations in which claims are often modest, there are many claimants and dealing with cases on an individual basis would be difficult. [p. 517][11]

[20] Ms. Sciscente proposes the following common questions:

(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?

---

7 2019 CSC 35.

8 L'Oratoire Saint-Joseph du Mont-Royal v. J.J., supra, note 2, par. 44; Infineon Technologies AG v. Option consommateurs, 2013 SCC 59, par. 72-73.

9 L'Oratoire Saint-Joseph du Mont-Royal v. J.J., supra note 2, par. 44; Vivendi Canada Inc. v. Dell'Aniello, 2014 SCC 1, par. 37, 52-56; Infineon Technologies AG v. Option consommateurs, supra, note 4, par. 72-73; Baratto c. Merck Canada inc., 2018 QCCA 1240, par. 70.

10 Vivendi Canada Inc. v. Dell'Aniello, par. 51.

11 Infineon Technologies AG v. Option consommateurs, par. 73.

(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?

[21] In the Court's view, the facts alleged do give rise to these proposed common questions, limited to Audi, as the Court will consider later.

[22] This said, Audi argues the nature of the remedies sought will require that: "For each class member, a multifold analysis will be required to determine if they have sustained damages and to which extent...".

[23] With respect, that some people may have been affected differently by the fault committed by Audi is not a bar to a class action being authorized. The judgment of Justice Hamilton, then in this Court, in *Zuckerman c. Target Corporation*, provides an example:

> [50] Based on the arguments set out above, Target argues that this condition is not met because there is no identical, similar or related issue with respect to damages.
>
> [51] Even assuming that the damages issue is not common, Target overstates the burden on the petitioner under Article 575(1) C.C.P. Article 575(1) requires only one question of law or fact that is identical, similar or related, not all the questions.[12]
>
> [Reference omitted]

[24] Even though Justice Hamilton acknowledged that the damages for each member could be different, he provided for collective recovery of same in the conclusions that he authorized.

2.3 Paragraph 575(2)

[25] The real issue in the present matter is whether the facts alleged appear to justify the conclusions sought.

2.3.1 Is Volkswagen Group Canada Inc. Properly Named as a Defendant

[26] For VW to be the object of the action, there needs to be a factual demonstration that it committed a fault related to the data breach.

[27] Ms. Sciscente argues that paragraph 6 of her Modified Application provides the necessary factual basis for the action to move forward against VW. She relies on two internal documents, being the Audi of America Notice of Data Breach, dated June 11,

---

[12] 2017 QCCS 110.

2021[13] and the letter addressed to the Attorney General of the State of Maine, Aaron Frey, dated June 10, 2021.[14]

[28] Ms. Sciscente also produced a number of internet media articles, which describe the data breach affecting 3.3 million Audi and VW customers in the US and Canada.[15] However, these do not distinguish between the two countries, so the Court must rely on the un-contradicted statement of Mr. Black, to get a full understanding of the Canadian situation.

[29] The Court acknowledges that if the questions for which authorization is sought will advance the claims of people who are in a similar situation in relation to VW, then the person seeking to advance those claims is entitled to do so on behalf of other people who would either benefit from or be bound by a judgment on the common issues.[16] However, minimally, there must be a factual allegation that would allow the Court to conclude that VW's Canadian customers suffered the same fate as Audi's. Ms. Sciscente only presents documentary evidence in relation to the situation in the USA insofar as VW is concerned.

[30] Moreover, in its judgement on the production of evidence, the Court allowed Mr. Black to be examined on the following issue:

> • the basis for the affirmation that the Data Security Incident did not affect individuals who purchased or leased a Volkswagen-branded vehicles or interested buyers of Volkswagen vehicles in Quebec or in Canada.[17]

[31] Ms. Sciscente's lawyer chose to question him and this is what Mr. Black said:

> Q. You just said that it's also -- and in your 18 affidavit, at 9c), you referred to Audi and Volkswagen. So both those dealers or those brands were impacted by the data breach, correct?
>
> A. Dealers, yes. Brands, no. There was no trace of anything related to Volkswagen vehicles that we were able to find in the investigation.
>
> Q. So are you saying that the data breach only included people who were either purchasing, leasing, or interested in an Audi branded vehicle? Nothing else?
>
> A. That is what I'm saying for the Canadian market, yes.
>
> Q. Okay, so notwithstanding what you say at 9c), you're saying if someone is interested in anything but an Audi vehicle, they were not impacted in Canada?

---

13 Exhibit R-3.
14 Exhibit R-4.
15 Exhibit R-5.
16 *Bank of Montreal* v. *Marcotte* 2014 SCC 55.
17 *Sciscente c. Audi Canada inc.*, 2022 QCCS 1087.

A. That is correct.

[32] Having chosen to question Mr. Black on the scope of the breach, Ms. Sciscente cannot now ask the Court to ignore this evidence. The Court will only consider the application as against Audi. It does not suffice to provide documents related solely to the US breach to support an authorization application in Canada.

2.3.2 The Cause of Action against Audi

[33] Audi correctly posits that the occurrence of a data security incident does not, in and of itself, mean that a fault has been committed in the safeguarding of the personal information. However, in the present matter, there are elements of Audi's conduct that provide a clear road to making a reasoned argument that a fault was committed. One is the amount of time that the breach went unnoticed, another is the time that Audi took to advise its customers following its knowledge of the breach.

[34] Audi then argues that Ms. Sciscente has not demonstrated that she suffered any real damages.

[35] Justice Morrison considered a similar situation recently, in *Fortier c. Uber Canada Inc.*[18] Uber had argued that the facts alleged were too vague to demonstrate that the applicant had suffered prejudice as a result of the breach. Justice Morrison did not agree:

> *[41] En appliquant une approche similaire, la Cour d'appel du Québec dans l'arrêt Sofio confirme le refus de la Cour supérieure d'autoriser une action collective liée à la perte de renseignements personnels pour cause d'absence d'allégations factuelles suffisantes pour soutenir l'existence d'un préjudice.*
>
> *[42] La Cour confirme que dans de tels cas, l'usurpation ou la tentative d'usurpation de l'identité ne constitue pas une condition sine qua non d'un préjudice indemnisable.*
>
> *[43] Par contre, les allégations de la demande en autorisation doivent révéler un minimum factuel au soutien de l'existence d'un préjudice. La Cour d'appel dans Sofio s'exprime ainsi:*
>
> *[25] [...] Le problème, en l'espèce, tient cependant au fait que les allégations de la requête en autorisation, tenues pour avérées, ne révèlent tout simplement pas de préjudice, même simplement moral : on invoque un stress dont la nature, l'ampleur, l'intensité ou les effets ne sont nullement détaillés et l'on décrit comme un préjudice des activités de vérification tout à fait routinières et habituelles, voire banales, chez la personne raisonnable qui est titulaire d'un compte bancaire ou détient une carte de crédit ou de débit. S'il y a plus, la requête ne le dit pas. Certes, il ne s'agit pas d'inviter ici les requérants ou les demandeurs à dramatiser la*

---

[18] 2021 QCCS 4053.

présentation de leurs allégations ou gonfler le descriptif de leur préjudice, mais il faut néanmoins un minimum factuel, qui n'est pas présent ici.

[44] Donc, l'analyse de la question de l'existence d'un préjudice est faite au cas par cas, sur la base des allégations factuelles contenues dans la demande en autorisation, lesquelles sont tenues pour avérées.[19]

[36] So, what are the facts alleged by Ms. Sciscente?

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.

[...]

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.

[...]

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.

---

19 *Id.*

> [...]
>
> 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.

[37] As was the case in the Uber matter, the Court finds the allegations to be somewhat vague. On the other hand, the facts in the present matter can be distinguished from those in *Bourbonnière c. Yahoo! Inc.*,[20] where Justice Chantal Tremblay refused to authorize the action. She found the following as a finding of fact:

> [35] As a matter of fact, Plaintiff's discovery demonstrates that she has no reason to believe that she has been the victim of identity theft or fraud as she has not identified any suspicious charges on either her debit or credit cards and she has not received a bad credit report. She continues using her Yahoo account and she admitted not having purchased any identity protection services such as credit monitoring: [...]

[38] Ms. Sciscente did purchase credit monitoring, and while given her examination out of court, there may be legitimate questions around her motivation for doing so, these can only be fully fleshed out on the merits. There is also sufficient evidence in the record to allow a cogent argument that her personal information was accessed; she was advised of same by Audi. The situation is different than the one considered by Justice Bisson in *Li c. Equifax inc*:[21]

[39] The Court also considers it to be different from the situation in *Homsy c. Google*.[22] As was the situation in that matter, the allegations around the data breach are general and do not point specifically to Ms. Sciscente. However, unlike the *Homsy* matter, we know that she was affected by the breach, given that Audi sent her a letter advising her of its occurrence.

[40] On the sufficiency of the allegations and on whether there is an arguable case for an award of punitive damages, the Court likens the factual situation raised by Ms. Sciscente to that considered by the Court of Appeal in *Levy c. Nissan Canada inc.*:

> [34] While the allegations in such regard may be perfunctory, which may be inevitable prior to full discovery, they are nevertheless sufficient at this stage. Indeed, Appellant alleged that Respondent's behaviour was unlawful and intentional and Appellant presented an arguable case that Respondent's failure to implement proper steps and required IT security measures could give rise to the

---

20 2019 QCCS 2624.
21 2019 QCCS 4340.
22 2022 QCCS 722.

award of punitive damages. In such regard, Appellant alleged in paragraph 29 of the re-amended Application that Nissan experienced at least two other prior data breaches which raise the deterrent aspect of punitive damage awards. The tribunal can certainly draw inferences from the allegations of fact in the Application and deduce that Respondent had to know that a failure to implement proper measures could lead to the violation of the class members' right to privacy as Appellant alleges in paragraphs 51 and 52 of the re-amended Application.

[35] Moreover, the more than one-month delay between the breach and the web posting and sending of the letters could potentially be viewed as conduct undertaken (or abstained from) in full knowledge of the prejudicial consequences that could be suffered by Respondent's customers during such period. This may be the case notwithstanding Respondent's explanation that there was an investigation of the incident ongoing at the time, which will be an issue for the merits. Nevertheless, the failure is alleged by Appellant, which is sufficient at this stage of the proceedings. Indeed, the judge acknowledges that the delay appears to be "excessive" even when considered in light of the *Act respecting the protection of personal information in the private sector*. Conduct after the breach can potentially give rise to punitive damages. Here, Nissan's delay perpetuated and aggravated the violation of its customers' right to privacy. The violation did not end when the data was breached. Rather, the violation commenced with the breach and continued, as alleged, while the information was in the hands of the perpetrators and Respondent did not act to protect its customers or enable them to protect themselves.

[36] At the present stage of the proceedings, where we are only considering the allegations, delays in the management of the incident can potentially be the source of damages in addition to the conduct of Respondent in failing to protect personal information prior to the breach.[23]

[41] In sum, while the allegations are indeed concise, the Court considers that Ms. Sciscente has presented an arguable case, that she might be entitled to compensatory, moral and even punitive damages as a result of the data breach.

2.4 Paragraph 575(3)

[42] In the matter of *Rozon* c. *Les Courageuses*, the Court of Appeal sets out the role of the Court as follows:

[43] Dans l'analyse de l'article 575(3) C.p.c., le juge doit évaluer si la composition du groupe rend difficile ou peu pratique l'application des règles sur le mandat d'ester en justice pour le compte d'autrui ou sur la jonction d'instances.

[44] Le juge a retenu que les critères applicables sont les suivants : 1) le nombre probable de membres; 2) la situation géographique des membres; 3) l'état physique et mental des membres; 4) la nature du recours entrepris; 5) les aspects

---

[23] 2021 QCCA 682.

> financiers du recours; et 6) les contraintes pratiques et juridiques inhérentes à l'utilisation du mandat et de la jonction des parties en comparaison avec l'action collective.[24]
>
> [References omitted]

[43] In the Court's view, the criteria of article 575(3) are satisfied in the present matter. The group is potentially large and certainly geographically dispersed. The financial gain for each member is likely modest, which underscores that a class action is an appropriate procedural vehicle.

2.5 Article 575(4)

[44] The bar for an individual to be an appropriate representative is not high:

> [97] Article 1003(d) C.C.P. directs that the member seeking the status of representative be "in a position to represent the class adequately / en mesure d'assurer une représentation adéquate des membres". As the judge correctly observed, this is generally said to require the consideration of three factors: a petitioner's interest in the suit, his or her qualifications as a representative, and an absence of conflict with the other class members. These factors should, says the Supreme Court, be interpreted liberally: "No proposed representative should be excluded unless his or her interest or qualifications is such that the case could not possibly proceed fairly".[25]

[45] In the Court's view, Ms. Sciscente has taken a sufficient interest, in the matter and the proceeding, to be an adequate representative, and that is all that is required. The fact that she may have been guided by class counsel in some of the steps that she took, does not change this.

3. THE SCOPE OF THE ACTION

[46] Ms. Sciscente proposes a national class. For Audi this makes the proposed action too broad in scope.

[47] The Supreme Court of Canada allowed a national class in *Vivendi Canada Inc. v. Dell'Aniello*:

> [61] The group proposed by the respondent includes 250 retirees or surviving spouses of employees who worked in six provinces: Quebec (134 members), Ontario (82 members), Alberta (3 members), British Columbia (16 members), Saskatchewan (2 members) and Manitoba (13 members). Since no applicable law was designated in the contracts of employment of the various employees, the law of the province where each employee worked would have to

---

[24] 2020 QCCA 5.
[25] *Sibiga c. Fido Solutions inc.*, 2016 QCCA 1299.

> apply to that employee's case (art. 3118 of the *Civil Code of Québec*, S.Q. 1991, c. 64 ("*C.C.Q.*")). According to the motion judge, the multitude of legal schemes applicable to the individual claims is an additional difficulty that demonstrates the proposed group's lack of homogeneity.
>
> [62] However, the fact that the employees worked in six different provinces is not in itself a bar to the authorization of the class action. In a class action, the court can accept proof of the law applicable in the common law provinces or take judicial notice of that law: art. 2809 *C.C.Q.* Only substantial differences between the applicable legal schemes would cause a class action to lose its collective nature: *Union des consommateurs* (2012), at paras. 120 and 123.
>
> [63] In the case at bar, the fact that members of the group live in different Canadian provinces should not prevent the court from authorizing the class action. There are common questions in the claims of the members of the proposed group with respect to the legality or the validity of the 2009 amendments.[26]

[48] However, it is important to note that the Court did not discuss the criteria of article 3148 C.p.c., likely because the trial judge had held the following:

> [44] À la lumière des faits qui nous occupent, la Cour supérieure a compétence en vertu de l'article 3148 (3) C.c.Q. qui indique que les autorités québécoises sont compétentes lorsqu'une faute a été commise au Québec, qu'un préjudice y a été subi, qu'un fait dommageable s'y est produit ou que l'une des obligations découlant d'un contrat devait y être exécutée.
>
> [45] En effet, un recours collectif peut être exercé pour le compte de personnes non domiciliées au Québec pourvu que chacune d'elles démontre que la cause d'action quant à elle a pris naissance au Québec ou que son contrat y a été conclu.
>
> [46] En l'espèce, la Requête est fondée sur un contrat de travail liant tous les membres du groupe et un successeur de Seagram (Vivendi), dont le siège social à l'époque était situé à Montréal.[27]
>
> [Reference omitted]

[49] A national class was also found to be appropriate in *Benamor c. Air Canada*,[28] but Air Canada had agreed that one was appropriate and, considering article 3148 C.C.Q., its head office is in Quebec.

[50] The article reads as follows:

---

26 2014 SCC 1.
27 *Dell'Aniello c. Vivendi Canada inc.*, 2010 QCCS 3416.
28 2020 QCCA 1597.

> 3148. In personal actions of a patrimonial nature, Québec authorities have jurisdiction in the following cases:
>
> (1) the defendant has his domicile or his residence in Québec;
>
> (2) the defendant is a legal person, is not domiciled in Québec but has an establishment in Québec, and the dispute relates to its activities in Québec;
>
> (3) a fault was committed in Québec, injury was suffered in Québec, an injurious act or omission occurred in Québec or one of the obligations arising from a contract was to be performed in Québec;
>
> (4) the parties have by agreement submitted to them the present or future disputes between themselves arising out of a specific legal relationship;
>
> (5) the defendant has submitted to their jurisdiction.
>
> However, Québec authorities have no jurisdiction where the parties have chosen by agreement to submit the present or future disputes between themselves relating to a specific legal relationship to a foreign authority or to an arbitrator, unless the defendant submits to the jurisdiction of the Québec authorities.

[51] Audi is not domiciled here. The CIDREQ does show that Audi has an elected domicile here, but this does not suffice to bring the proposed action under the ambit of article 3148:

> [84] However, the Court agrees with the Respondents that the Quebec Superior Court does not have jurisdiction over a national class based on the facts as pleaded.
>
> [85] Firstly, art. 3148 (1) is not met because neither Respondent has their domicile or residence in Quebec: the so-called "election of domicile" in the CIDREQ does not create legal domicile under art. 3148 (1) and Apple Canada has only "establishments in Quebec". There are no allegations that the alleged wrongs suffered by out of province consumer/owners (a) "relate to activities in Quebec" or (b) arise from "any contract that was to be performed in Quebec".[29]

[52] Audi does have establishments here, but as for the dispute relating to activities in Quebec, that is only potentially the case for the members of the proposed class who reside in Quebec. The same reality relates to the injury being suffered in Quebec. This only links the dispute to Quebec residents and there is no factual allegation that would allow the Court to conclude that the fault was committed here. In short, there is nothing

---

[29] *Charbonneau c. Apple Canada Inc.*, 2016 QCCS 5770 (CanLII), Application for leave to appeal dismissed, 2018 QCCA 2089; see also *Walid c. Compagnie nationale Royal Air Maroc*, 2019 QCCS 597, pars. 52-54.

in the allegations that would allow the Court to assume jurisdiction over the claims of the residents of other Canadian provinces.[30]

[53] The Court concludes that the class should be limited to Quebec residents.

4. CONCLUSIONS

[54] The Court will authorize the class action for the following group:

> 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;

FOR THESE REASONS, THE COURT:

[55] **GRANTS** the Applicant's application in part;

[56] **AUTHORIZES** the bringing of a class action in the form of an Application to institute proceedings in damages in the District of Montreal;

[57] **APPOINTS** the Plaintiff as the Representative Plaintiff representing all persons included in the Class herein described as:

> 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;

[58] **IDENTIFIES** the principle issues of law and fact to be treated collectively as follows:

- 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?

---

[30] *Holcam c. Retaurants Brands International Inc.*, 2022 QCCS 2168, par. 21-25.

- (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?

[59] **IDENTIFIES** 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 Audi Canada Inc.;
>
> **CONDEMN** Audi Canada Inc. to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Audi Canada Inc.'s loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Audi Canada Inc. 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;

[60] **DECLARES** 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;

[61] **CONVENES** the parties to a further hearing at a date to be determined for the purpose of determining the content of the notice to class members, the plan of communication, and the delay for class members to exclude themselves from the class action;

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

THOMAS M. DAVIS, J.S.C.

Mtres David Assor and Joanie Lévesque
LEX GROUP INC.
Lawyers for Plaintiff

Mtres Vincent de l'Étoile, Caroline Deschênes and Justine Brien
LANGLOIS LAWYERS L.L.P.
Lawyers for Defendants

Hearing date: May 5, 2022