CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL
N°: 500-06-000907-184

(Class Action Division)
SUPERIOR COURT

K[redacted] L[redacted]

Representative Plaintiff

-vs-

NISSAN 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 Court of Appeal of Quebec's Judgment dated April 28, 2021, and the Superior Court of Quebec's Judgment dated September 19, 2019, the class action herein has been authorized against the Defendant and K[redacted] L[redacted] was appointed as the Representative Plaintiff representing all persons included in the Class described as:

Toutes les personnes au Québec: (i) dont les renseignements personnels ou financiers détenus par Nissan Canada ont été compromis dans une intrusion informatique dont l'intimée a été informée par les auteurs par courriel le 11 décembre 2017, ou (ii) qui ont reçu une lettre de Nissan Canada le ou vers le mois de janvier 2018 les informant de cette intrusion informatique;	All persons in Québec: (i) whose personal or financial information held by Nissan Canada was compromised in a data breach of which Respondent was advised by the perpetrators by email on December 11, 2017, or (ii) who received a letter from Nissan Canada on or about January 2018 informing them of such data breach;

2. The main issues of fact and law to be treated collectively have been identified as the following:

a) Nissan Canada inc. a-t-elle commis une faute relativement à l'entreposage et à la conservation des renseignements personnels et/ou économiques des membres du groupe?	(a) Did Nissan Canada Inc. commit a fault regarding the storage and the safe-keeping of the financial and/or personal information of the Class Members?
b) Nissan Canada inc. a-t-elle commis une faute en tardant à aviser les membres du groupe de la survenance d'une intrusion informatique?	(b) Did Nissan Canada Inc. commit a fault by delaying the notification to Class Members that a data breach had occurred?
c) Nissan Canada inc. a-t-elle commis une faute en raison des déficiences dans les avis aux membres du groupe concernant l'intrusion informatique?	(c) Did Nissan Canada Inc. commit a fault due to the deficiencies of the notices given to Class Members about the data breach?
d) Nissan Canada inc. a-t-elle commis une faute en raison de son omission d'aviser les membres du groupe des résultats de son enquête?	(d) Did Nissan Canada Inc. commit a fault due to its failure to inform the Class Members of the outcome of its investigation?
e) comme résultat, Nissan Canada inc. est-elle obligée de payer des dommages-intérêts compensatoires ou des dommages punitifs aux membres du groupe ? Et si oui, de quels montants?	(e) Is Nissan Canada Inc. liable to pay compensatory damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

3. Nissan Motor Company is one of the world's largest automobile manufacturers. It is headquartered in Japan, with national branches around the globe. Worldwide, its estimated annual profits exceed $72 billion;

4. Defendant Nissan Canada Inc. is a Canadian corporation, headquartered in Mississauga, Ontario but has elected domicile in the District of Montreal, Province of Quebec, the whole as more fully appears from the *Registraire des entreprises* (CIDREQ) reports regarding Defendant, communicated herewith, *en liasse*, as **Exhibit P-1** (hereinafter "**Defendant**" or "**Nissan Canada**");

5. As the Canadian branch of Nissan Motor Company, Nissan Canada sells over 100,000 motor vehicles per year in Canada and is considered a market leader in automotive sales;

6. As appears from the R-1 CIDREQ reports, Nissan Canada also operates under the following names: Mitsubishi Motors Services Financiers, Services Financiers Mitsubishi Motors, Mitsubishi Motors Financial Services, Infiniti, Infiniti Financial Services, Nissan Canada Finance and Services Financiers Infiniti (hereinafter collectively "**NCF**");

7. At the relevant times, Defendant's customers could finance the purchase or lease of new or used vehicle through NCF at Nissan, Infiniti or Mitsubishi dealerships across Canada, including Quebec. The purchased or leased vehicles in question were not necessarily Nissan, Infiniti or Mitsubishi branded vehicles (for example, if a used Ford vehicle was sold or leased from a Nissan dealership, it would have been financed through Defendant);

8. On or before December 11, 2017, the NCF database was breached by unknown parties, resulting in the compromise, loss and theft of personal and financial information pertaining to approximately 1.13 million past and/or present customers of the Defendant (hereafter the "**Data Breach**");

9. This stolen personal and financial information included without limitation the name, address, vehicle make and model, vehicle identification number (VIN), Social Insurance Number, loan amount, amount of monthly payments and the credit scores of these approximate 1.13 million customers who had financed or leased a vehicle through Defendant;

10. Defendant, who requires the personal and financial information of its customers in the context of a vehicle lease or finance, has 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;

11. When a data breach affecting approximately 1.13 million clients occurs, Defendant 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;

12. This authorized class action lawsuit stems from Defendant's failure to follow these obligations;

The Data Breach

13. Nissan Canada claims that on December 11, 2017, it was first made aware that its database of NCF consumers had been breached by unknown parties;

14. Even after completing its own investigations following the Data Breach in question, Defendant was not able to ascertain the exact date(s) on which the Data Breach occurred, nor how or from where the Data Breach was accomplished;

15. Indeed, on December 11, 2017, three (3) Nissan Canada executives received an email from the thief with an extortion demand, the whole as more fully appears from a copy of December 11, 2017, extortion demand email, communicated herewith as **Exhibit P-2**;

16. As appears from the extortion demand email (P-2), the thief confirmed *inter alia* that he or she had stolen **all** of Defendant's "customers and proprietary information" and confirmed that he was providing a "sample" of the stolen information to Defendant, a copy of said sample document provided to Defendant through the Exhibit P-2 extortion demand email is filed herewith, *under seal*, as **Exhibit P-3**;

17. The "sample" document provided by the extortionist (Exhibit P-3) contained the actual client information which was stored on Defendant's servers regarding 278,450 of Defendant's active customers in Canada as at December 2016 to January 2017;

18. The P-3 Sample also included valid Social Insurance Numbers (SINs);

19. Defendant's servers are very large and can hold hundreds of thousands of files. The unencrypted client information which was stolen and included in the Sample document provided by the thief was in the same location on the Defendant's servers as other private and financial information concerning the Class Members (information which was also unencrypted and readily available to the thief who had gained access to the servers);

20. As mentioned, P-3 represents a mere "sample" of the information which was stolen, since the December 11, 2017 extortion demand email (P-2) confirmed that the thief had stolen **all** of Defendant's "customers and proprietary information";

21. Indeed, the thief was able to extricate and steel the unencrypted information from Defendant's servers and Defendant's inadequate IT "security" systems did not alert Defendant that the breach had occurred and obviously did not prevent the breach. In fact, were it not for the P-2 extortion demand email being sent by the thief, Defendant would not have even known that the information had been accessed and stolen at all;

22. Nissan Canada inexplicably waited at least 10 days before publicly announcing the Data Breach on December 21, 2017. On that date, Defendant announced that the names, addresses, vehicle makes and models, vehicle identification numbers (VIN), loan amounts, amounts of monthly payments and the credit scores of its approximate 1.13 million Customers had been lost, stolen or otherwise compromised, the whole as more fully appears from the Nissan Canada Finance Notice to Customers, communicated herewith as **Exhibit P-4** (hereafter the "**Notice**");

23. However, Nissan Canada published the link to the Notice on the bottom left corner of the front page of the Nissan Canada Finance corporate website, under an unassuming title, and where it could be easily overlooked, rather than posting the Notice on Nissan Canada's general customer website or social media accounts. This decreased the likelihood that the customers would read the Notice and was surely intended to

minimize the adverse effects of the Data Breach on Nissan sales during the holiday season and end-of-year sales, the whole as appears from a copy of Defendant's (Nissan Canada Finance) website and a copy of the Nissan.ca website, both dated February 12, 2018, communicated herewith as **Exhibit P-5**, *en liasse*;

24. Nissan Canada failed and neglected to mention that valid Social Insurance Numbers were also contained in the sample file provided by the thief;

25. Nissan Canada 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;

26. The Notice clearly indicated that Nissan Canada was and remains uncertain of exactly what was lost during the Data Breach, who is affected by the loss of personal information, and the extent of the risks the Class Members now face. Indeed, Nissan Canada has since completed its internal investigation and is still unable to confirm the date on which the Data Breach occurred, how the thief gained access to its networks, the identity of the thief/thieves, nor what information, files or documents were accessed and/or stolen by the thief. That being said, the thief did have access to the other information and documents that were stored in the same location (servers) as the data represented in the "sample" document that the thief provided to Defendant;

27. Moreover, Nissan Canada 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;

28. Furthermore, although Defendant had offered an inadequate 12 months of TransUnion (credit agency) credit monitoring to Class Members (who had to jump through many hoops and provide private information in order to hopefully activate said service), this service could not prevent fraud and Defendant delayed, and in some cases completed failed, to send certain Class Members the proper activation code in order to activate said service;

29. The 12 months period is also inadequate since fraud can occur well after the first year following the Data Breach, especially in instances were such a large number of customers are affected and Defendant is not even able to determine when the breach had occurred (and for how long it occurred);

30. Defendant chose to only offer TransUnion's credit monitoring, instead of credit monitoring by both Canadian credit agencies TransUnion and Equifax Canada;

31. Defendant failed to mandate (and pay for) TransUnion and Equifax Canada to automatically activate the said credit monitoring;

32. Defendant was negligent and committed faults in this regard since it was asking the affected customers to jump through hoops (and provide private information) in order to hopefully activate the TransUnion service - that is if the Class Member were even aware of the Data Breach which is not the case for many Class Members for various reasons;

33. Furthermore, Defendant failed to have fraud alerts posted on the Class Members' credit files with TransUnion and Equifax Canada, which would have further helped, although not guaranteed, that the Class Members were better protected;

34. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class Members, Defendant 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 Defendant asked the Class Members (those aware of the Data Breach) to activate this service which involves many steps and requires the customer to provide detailed personal and/or financial information, which clearly reduces the chances of many Class Members actually registering for said service;

35. Nissan Canada's sought to impart a false sense of security to the Class Members by deceptively downplaying the Data Breach. Nissan Canada also sought to placate customers by offering the free credit monitoring instead of advising customers of the high risk of fraud and identity theft associated with the stolen data. Nissan Canada also failed to promptly and effectively inform the Class Members of the data theft, which left them vulnerable to attack;

36. After becoming aware of the Data Breach, Nissan Canada waited more than six (6) weeks, namely until the end of January 2018, before contacting some but not all of the Class Members in order to inform them of Data Breach. This delay was clearly excessive[1];

37. In this regard, Defendant sent notification letters by regular mail, instead of registered mail, email or direct calls, which clearly left many Class Members unaware of the risks to which they were now exposed (since letters sent by regular mail can fail to reach the recipient for many different reasons and there is no confirmation of receipt as opposed to notices sent by registered mail or email);

38. Accordingly, Nissan Canada failed to promptly and quickly disclose the Data Breach to the Class Members/victims of the Data Breach;

39. Furthermore, this was far from Nissan's first data breach. As a matter of fact, Nissan has experienced at least two data breaches and hacking of this nature, namely one in April 2012, when third parties breached the Nissan employee database, seizing personal information such as names, user IDs and passwords, and another in 2016, when Nissan disclosed that the mobile app linked to the Nissan Leaf was prone to hacking in such a way that the driver's comings and goings could be spied on by third parties;

[1] At paragraph 82 of its September 19, 2019 authorization judgment, this Honorable Court already concluded and stated the following "*Mais, a priori, il est soutenable qu'un délai de 50 jours était excessif avant que Mme Lévy reçoive la lettre R-3 et soit mise en garde*."

40. Defendant clearly failed to implement the proper steps and required IT security measures in order to safeguard and protect the Class Members information;

41. Furthermore, although all of the information was concerning vehicles leased or sold in Canada, Defendant illegally chose to house the Class Members' sensitive private and financial in its data center located in Denver, Colorado, USA. These Denver U.S.A. servers were owned and operated by Nissan North America, Inc.

42. Furthermore, since the Data Breach, Defendant has been unable to ascertain whether the thief accessed and stole the data from Denver servers or from Defendant's other servers located in Canada.

43. 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;

44. As a result of Nissan Canada's inadequate data security, cyber-criminals now possess the private information of Plaintiff and the Class Members;

45. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting more than six (6) weeks pass before notifying Class Members (with many not even informed yet), Nissan Canada failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class Members;

46. 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 longer than 12 months;

g) the obligation to be even more attentive than normally necessary concerning the communication of their personal information (threat of social engineering), 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 their credit report in order to look for unauthorized transaction or fraud;

j) a negative effect on their credit score;

k) loss 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;

47. 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, which has made Plaintiff and the Class Members potential targets for fraud and/or identity theft;

48. 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;

49. Plaintiff and the Class Members are justified in claiming and have also been authorized to claim punitive damages against Defendant, as confirmed and detailed by the Court of Appeal in its April 28, 2021, Authorization Judgment;

THE REPRESENTATIVE PLAINTIFF

50. On January 30, 2018, Plaintiff finally received a Data Breach notification letter from Defendant, the whole as appears from said notification letter, communicated herewith as though recited at length herein **Exhibit P-6**;

51. Before receiving the P-6 letter, Plaintiff (as is the case for many other Class Members) had not otherwise been made aware of the Data Breach;

52. 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 six (6) weeks[2];

[2] At paragraph 82 of its September 19, 2019 authorization judgment, this Honorable Court already concluded and stated the following "*Mais, a priori, il est soutenable qu'un délai de 50 jours était excessif avant que Mme Lévy reçoive la lettre R-3 et soit mise en garde*."

53. Through its P-6 notification letter, Defendant has clearly admitted the following, *inter alia*:

a) That it lost the Class Members' contact information including name and mailing address;

b) That it lost the Class Members' vehicle information, including vehicle make and model, as well as the vehicle information number;

c) That it lost the Class Members' financial information, including credit scores, loan amounts and the amount of monthly payments;

d) That Nissan Canada admits that the Data Breach will cause Class Members "frustration and anxiety", therefore admitting that it is reasonably possible that unauthorized persons could have received, accessed or misused the personal information of the Class Members;

e) That the Class Members should "review their bank account and payment card statements carefully and call their bank if they see any suspicious transactions," thereby admitting that it is reasonably possible that third parties may have accessed their financial information;

54. 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;

55. 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;

56. On February 2, 2018, she followed the instructions on the P-6 notification letter in order for Defendant to send her a code to activate the TransUnion protection;

57. Defendant failed to send her the activation code, leaving her at risk and vulnerable to fraud and identity theft;

58. On February 5, 2018, having not heard back from Defendant, Plaintiff once again went through all of Defendant's process to request the said TransUnion activation code, the whole as appears from a copy of Plaintiff's submission on Defendant's website to request the TransUnion activation code, communicated herewith, **confidentially and under seal**, as **Exhibit P-7**. By February 12, 2018, the date of the original Application for Authorization herein, Defendant had still failed to send Plaintiff the said activation code, continuing to leave Plaintiff at risk and vulnerable to fraud and identity theft;

59. Late on Friday, February 16, 2018, namely 14 days after Plaintiff's first request for the activation code and 11 days following Plaintiff's second request for said activation code, Plaintiff finally received the activation code from Defendant, the whole as more fully appears from a copy of Defendant's email to Plaintiff, communicated herewith, as **Exhibit P-8**;

60. Accordingly, Defendant made Plaintiff and other Class Members wait for many additional days, weeks or months before sending them the TransUnion activation code, all the while Plaintiff and said Class Members remained at great risk of fraud and identity theft. This represents further excessive delays and further intentional faults and negligence by Defendant, for which Defendant is liable to pay damages, including punitive damages;

61. On Monday, February 19, 2018, Plaintiff used the activation code received in order to activate the TransUnion credit monitoring, the whole as more fully appears from a copy of the confirmation email from TransUnion, communicated herewith as, as **Exhibit P-9**;

62. Defendant having failed or neglected to provide the Class Members with further updates or information regarding the Data Breach, and Plaintiff still being worried about the risk of fraud and identity theft, Plaintiff called TransUnion on March 2, 2018, for additional information about Defendant's TransUnion offer. Plaintiff asked the TransUnion representative why the service would only be in effect for one year whereas fraud or identity theft can occur well after the first year following such a

significant breach. The TransUnion representative simply replied that it was out of TransUnion's control since Defendant had only set up and offered the program for one year, after which Plaintiff would have to pay for additional coverage;

63. On March 11, 2018, Plaintiff, who was still concerned and who wanted to protect her identity and credit, signed up for TransUnion's six (6) year fraud warnings and TransUnion's one-year Social Insurance Number (SIN) alerts, both of which Defendant failed to offer to the Class Members, the whole as appears from a copy of the March 11, 2018 screenshot from the TransUnion website, communicated herewith as **Exhibit P-10**;

64. On March 20, 2018, Plaintiff, who continued to be concerned and who wanted to further protect her identity and credit, called Equifax Canada and signed up for its fraud and Social Insurance Number (SIN) alerts (both of which Defendant also failed to offer to the Class Members). Plaintiff paid $6.90 to Equifax Canada in order to activate these alerts, which amount Plaintiff hereby claims from Defendant as damages, the whole as appears from a screenshot of Plaintiff's credit card account history, communicated herewith **confidentially and under seal** as **Exhibit P-11**;

65. Defendant has to date intentionally failed and neglected to provide the Class Members with further updates or information regarding the Data Breach. Indeed, the Plaintiff never received any follow-up communications whatsoever from Defendant about the Data Breach, about the results of Defendant's "investigation", about the stolen information, etc. This represents further excessive delays and further intentional faults and negligence by Defendant, for which Defendant is liable to pay damages, including punitive damages;

66. Plaintiff and the Class Members would not have applied for and/or signed a finance or lease agreement with NCF if they had known that Defendant would be negligent and careless with the customers' personal information;

Punitive Damages:

67. For all of the reasons more fully detailed above, including those contained in the Court of Appeal's April 28, 2021 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;

68. 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' personal information, after being the victim of at least two prior data breach incidents;

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

c. decided to only notify the Class Members more than six (6) weeks after it became aware of the Data Breach (and excessive delay);

d. failed to notify many Class Members;

e. 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;

f. failed to properly and promptly send the credit monitoring activation code to Plaintiff as detailed above, and other Class Members;

g. failed to provide the Class Members with further updates or information regarding the Data Breach;

h. failed to inform the Class Members of the fact that the extortionist had provided Defendant with a sample document of the stolen information, which contained valid Social Insurance Numbers;

i. failed to properly preserve the evidence in this file, including failing to secure a full copy of the notification list used to send the P-6 letters to the Plaintiff and other Class Members.

69. As mentioned above, this was far from Nissan's first data breach. As a matter of fact, Nissan has experienced at least two data breaches and hacking of this nature, namely one in April 2012, when third parties breached the Nissan employee database, seizing personal information such as names, user IDs and passwords, and another in 2016, when Nissan disclosed that the mobile app linked to the Nissan Leaf was prone to hacking in such a way that the driver's comings and goings could be spied on by third parties;

70. Defendant's other instances of data being stolen or breached further warrants and supports a condemnation for punitive damages herein;

71. Defendant's excessive delays, faults and failures in the investigation and notification process after the Data Breach also further warrants and supports a condemnation for punitive damages herein;

72. 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 and moral damages suffered by the Class Members;

73. Defendant's above detailed actions qualify its 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, seeing as how this had happened before;

74. 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

75. Class Members had their personal and financial information lost by Defendant as described hereinabove, including name, address, vehicle make and model, vehicle identification number (VIN), Social Insurance Numbers, loan amount, amount of monthly payments and credit scores;

76. 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;

77. 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;

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

79. 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.;

80. 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;

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

82. 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;

83. 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;

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

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

FOR THESE REASONS, MAY IT PLEASE THE COURT:

ACCUEILLIR l'action collective de la demanderesse au nom de tous les membres du groupe, contre la défenderesse;	**GRANT** the Class Action of Plaintiff on behalf of all the Class Members against Defendant;
CONDAMNER la défenderesse à payer aux membres du groupe des dommages-intérêts pour toutes pertes économiques et tout préjudice moral résultant de la perte par la défenderesse des renseignements des membres du groupe, et **ORDONNER** leur recouvrement collectif;	**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;
CONDAMNER la défenderesse à payer aux membres du groupe des dommages punitifs pour l'atteinte illicite et intentionnelle à leur droit à la vie privée et **ORDONNER** leur recouvrement collectif;	**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;
LE TOUT avec intérêt plus l'indemnité additionnelle édictée au *Code civil du Québec*, plus tous les frais de justice incluant les	**THE WHOLE** with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees

honoraires des experts et des frais d'avis aux membres du groupe;

LE TOUT avec frais de Justice.

and publication fees to advise Class Members;

THE WHOLE with legal costs.

MONTREAL, July 27, 2021

(s) Lex Group Inc.

Lex Group Inc.
Per: David Assor
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 Representative Plaintiff 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 Representative Plaintiff's lawyer or, if the Representative Plaintiff is not represented, to the Representative 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 Representative 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 Representative 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 Representative Plaintiff intends to use the following exhibits:

Exhibit P-1:	Copy of the *Registraire des entreprises* CIDREQ reports regarding Defendant, *en liasse*;
Exhibit P-2:	Extortion demand email dated December 11, 2017;
Exhibit P-3:	Sample Document provided by the extortionist on December 11, 2017, **confidentially and under seal**;
Exhibit P-4:	Nissan Canada Finance Notice to Customers;
Exhibit P-5:	Copy of Nissan Canada Finance's website and copy of the Nissan.ca website, both dated February 12, 2018, *en liasse;*
Exhibit P-6:	Notification letter sent to Plaintiff;
Exhibit P-7:	Screenshot of Plaintiff's submission on Defendant's log-in form, on February 5, 2018, **confidentially and under seal**;

Exhibit P-8:	Defendant's email to Plaintiff, dated February 16, 2018;
Exhibit P-9:	TransUnion's email to Plaintiff, dated February 19, 2018;
Exhibit P-10:	TransUnion confirmation screenshot, March 11, 2018;
Exhibit P-11:	Plaintiff's credit card account history screenshot, **confidentially and under seal**;

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, July 27, 2021

(s) Lex Group Inc.

Lex Group Inc.
Per: David Assor
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

Nº.: 500-06-000907-184

(Class Action Division)
SUPERIOR COURT

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

K[redacted] L[redacted]

Representative Plaintiff

-vs-

NISSAN CANADA INC.

Defendant

ORIGINATING CLASS ACTION APPLICATION

ORIGINAL

Me David Assor

LEX GROUP
AVOCATS · ATTORNEYS
WWW.LEXGROUP.CA

BL 5606

Lex Group Inc.
4101 Sherbrooke St. West
Westmount, (Québec)
H3Z 1A7
T: 514.451.5500
F: 514.940.1605
@: davidassor@lexgroup.ca