

CANADA  
PROVINCE OF QUEBEC  
DISTRICT OF MONTREAL

SUPERIOR COURT  
(Class Action)

N<sup>o</sup> : 500-06-000907-184

LEVY, residing and domiciled at  
[REDACTED];

*Plaintiff*

-VS-

**NISSAN CANADA INC.**, a legal person constituted according to the law, having its head office at 5290 Orbitor Street, in the City of Mississauga, Province of Ontario, L4W 4Z5, and having its elected domicile at 1 Place-Ville-Marie, Suite 3700, in the City and District of Montreal, Province of Quebec, H3B 3P4;

*Defendant*

---

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

---

**TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT OF QUEBEC,  
SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PLAINTIFF STATES THE  
FOLLOWING:**

**INTRODUCTION**

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

All persons in Canada (subsidiarily in Quebec), whose personal and/or financial information was compromised, lost and/or stolen from Defendant as a result of the data breach that occurred on or before December 11, 2017, or any other Group(s) or Sub-Group(s) to be determined by the Court;

(hereinafter, both Quebec resident and non-Quebec resident Class Members are collectively referred to as “**Class Member(s)**”, “**Group Member(s)**”, the “**Group**”, the “**Class**”, “**Consumers**” or “**Customers**”);

2. 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;
3. 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) report regarding Defendant, communicated herewith as **Exhibit R-1** (hereinafter “**Defendant**” or “**Nissan Canada**”);
4. 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;
5. As appears from the R-1 CIDREQ report, Nissan Canada also operates under the following names (or divisions): Infiniti Financial Services Canada and Nissan Canada Finance (hereinafter collectively “**NCF**”);
6. Customers can finance the purchase or lease of new or used vehicle through NCF;
7. On or before December 11, 2017, the NCF database was breached by unknown parties, resulting in the compromise, loss and/or theft of personal and/or financial information pertaining to approximately 1.13 million past and/or present Customers of the Defendant (hereafter the “**Data Breach**”);
8. This personal information included without limitation the name, address, vehicle make and model, vehicle identification number (VIN), 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;

9. 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;
10. When a data breach affecting approximately 1.13 million Consumers occurs, Defendant had the obligation to immediately and accurately notify its Customer in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience;
11. This lawsuit stems from Defendant's failure to follow these obligations;

### **The Data Breach**

12. 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. Plaintiff is presently not aware of the exact date(s) on which the Data Breach occurred nor on which date Defendant knew or should have known about the Data Breach;
13. 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 R-2** (hereafter the "**Notice**");
14. 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 Consumers 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;

15. 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;
16. The Notice clearly indicates 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 Consumers now face;
17. 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;
18. Furthermore, although Defendant has offered 12 months of TransUnion (credit agency) credit monitoring to Class Members (who have to jump through many hoops and provide private information in order to hopefully activate said service), this service does not prevent fraud;
19. The 12 months period is also inadequate since fraud can occur well after the first year following the Data Breach, especially in instances where such a large number of Customers are affected;
20. Defendant chose to only offer TransUnion's credit monitoring, instead of credit monitoring by both Canadian credit agencies TransUnion and Equifax Canada;
21. Defendant failed to mandate (and pay for) TransUnion and Equifax Canada to automatically activate the said credit monitoring;
22. Defendant was negligent and committed faults in this regard since it is 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 is even aware of the Data Breach which is not the case for many Class Members for various reasons;

23. 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;
24. 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 is now asking the Class Members (who are 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;
25. 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;
26. 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;
27. 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);



28. Accordingly, Nissan Canada failed to promptly and quickly disclose the Data Breach to the Class Members/victims of the Data Breach;
29. 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 in the past five (5) years, namely (1) in April 2012, when third parties breached the Nissan employee database, seizing personal information such as names, user IDs and passwords, and (2) 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;
30. Defendant clearly failed to implement the proper steps and required IT security measures in order to safeguard and protect the Class Members information;
31. 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;
32. As a result of Nissan Canada's inadequate data security, cyber-criminals now possess the private information of Plaintiff and the Class Members;
33. 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;
34. Nissan Canada customers have been and/or will be exposed to fraud and/or identity theft and these Customers have been harmed as a result. Harm to victims of the Data Breach

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

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

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

- a) Delays in the processing of any future requests or applications for credit in the future;
- b) The obligation to closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, which will be longer than 12 months;
- c) 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;
- d) 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;

- e) Obtaining their credit report in order to look for unauthorized transaction or fraud;
- f) A negative effect on their credit score;

37. 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;

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

- a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, LRQ, c C-1991;
- b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, RDQ, c C-12;
- c) Sections 1, 2, 10, 13 and 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1;



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

**FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF**

39. On January 30, 2018, Plaintiff finally received the notification letter from Defendant, the whole as appears from said notification letter, communicated herewith as though recited at length herein **Exhibit R-3**;
40. Before receiving the R-3 letter, Plaintiff (as is the case for many other Class Members) had not otherwise been made aware of the Data Breach;
41. 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;
42. Through its R-3 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;

43. 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;
44. Immediately following the being made aware of the loss of her personal information by Defendant, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information;
45. On February 2, 2018, she followed the instructions on the R-3 notification letter in order for Defendant to send her a code to activate the TransUnion protection;
46. Defendant failed to send her the code, leaving her vulnerable to fraud and identity theft;
47. On February 5, 2018, Plaintiff once again went through all of Defendant’s process to request the said activation code. As of the date of these presents, Defendant has still failed to send Plaintiff the said code, continuing to leave Plaintiff vulnerable to fraud and identity theft;
48. 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:**

49. For all of the reasons more fully detailed above, which are reiterated as though recited at length in the present section, Plaintiff respectfully submits that Defendant was grossly and/or intentionally negligent and is liable to pay punitive damages to the Class Members;
50. 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;
  - 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;
  - 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. not properly and promptly sending the credit monitoring activation code to Plaintiff as detailed above, and surely other Class Members;
51. 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 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;



52. 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;
53. 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;

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

54. Every Class Member had his, her or its personal and financial information lost by Defendant as described hereinabove, including name, address, vehicle make and model, vehicle identification number (VIN), loan amount, amount of monthly payments and credit scores;
55. Every Class Member has or will experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information;
56. Every Class Member had and has to closely monitor his or her accounts looking for possible fraud from now on and for all periods subsequent to the loss of information;
57. Every Class Member will be inconvenienced by any safety measures that may become necessary in order to prevent further fraud exposure, such as signing up for credit monitoring service, posting an alert on their accounts or credit files, changing their personal information or account numbers, transferring money from one account to another, closing and opening accounts, paying for and dealing with NSF or other bank charges or interest, etc.;

58. Furthermore, every Class Member may be required to pay costs or fees in order to sign up for such credit monitoring, to post an alert on their accounts or credit files, to change their personal information, to purchase insurance, or in order to otherwise protect themselves from further fraud exposure;
59. The Class Members' credit score has and/or will be negatively affected;
60. Moreover, as mentioned above, is likely that many Class Members have not been notified of the loss of their information, making them still at great risk of fraud or identity theft;
61. Every Class Member can still fall victim to fraud or identity theft, in the future, due to Defendant's negligence in the safekeeping of their personal information;

#### **CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION**

62. The composition of the Group makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (Article 575 (3) C.C.P.) for the following reasons;
63. Plaintiff is unaware of the specific number of persons included in the Class but, as mentioned above, it appears that the names, addresses, vehicle makes and models, vehicle identification numbers (VIN), loan amounts, amounts of monthly payments and the credit scores of 1.13 million of Defendant's Customers in Canada had been lost, stolen or otherwise compromised as a result of the Data Breach;
64. Class Members are numerous and are scattered across the entire province and country since Defendant leases and finances vehicles across the country, including Quebec;
65. In fact, even before the institution of the proceedings, Class Members contacted the undersigned attorneys on their corporate website in order to be kept informed of the

present class action, the whole as more fully appears from the said communications from Class Members in different provinces, together with their comments, communicated herewith as though recited at length herein, **confidentially and under seal** (in order to protect their personal information), as **Exhibit R-4**;

66. In addition, given the costs and risks inherent in an action before the Courts, many people will hesitate to institute an individual action against the Defendant. Even if the Class Members themselves could afford such individual litigation, the Court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by the conduct of the Defendant would increase delay and expense to all parties and to the Court system;
67. Moreover, a multitude of actions instituted risks leading to contradictory judgments on issues of fact and law that are similar or related to all Class Members;
68. These facts demonstrate that it would be impractical, if not impossible, to contact each and every Class Member to obtain mandates and to join them in one action;
69. In these circumstances, a class action is the only appropriate procedure for all of the Class Members to effectively pursue their respective rights and have access to justice;
70. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely Defendant's negligence, and fault;
71. The claims of the Class Members raise identical, similar or related issues of law and fact (Article 575 (1) C.C.P.), namely:
- a) Was Defendant negligent and/or did Defendant commit a fault in the storing and safekeeping of the financial and/or personal information of the Class Members whose information was ultimately compromised, lost and/or stolen on or before December 11, 2017?



- b) Did Defendant commit a fault in the way in which it notified the Class Members about the data breach?
- c) Is Defendant liable to pay compensatory and/or moral damages to the Class Members as a result of the loss of said information, including without limitation actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and if so in what amounts?
- d) Is Defendant liable to pay punitive and/or exemplary damages to the Class Members, and if so in what amount?

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

### **NATURE OF THE ACTION AND CONCLUSIONS SOUGHT**

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

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

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

**CONDEMN** Defendant to pay to the Class Members compensatory damages for all monetary losses 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 compensatory and/or moral damages, in the amount to be determined by the Court, as a result of Defendant's loss of Class Members' information, including without limitation for actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and **ORDER** collective recovery of these sums;

**CONDEMN** Defendant to pay an amount in punitive / exemplary damages to every Class Member, in the amount to be determine by the Court, 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 expert's fees and publication fees to advise Class Members;

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

- a) Plaintiff resides in the District of Montreal;
- b) A great number of Class Members reside in the judicial District of Montreal and/or provided their personal and financial information to Defendant in the District of Montreal;
- c) Defendant carries on business, including the leasing and financing of vehicles, in the District of Montreal;
- d) Defendant has elected domicile in the Montreal (Exhibit R-1);

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

76. Plaintiff, who is requesting to be appointed as Representative Plaintiff, is in a position to properly represent the Class Members (Article 575 (4) C.C.P.), since:

- a) Her personal information was lost by Defendant as described hereinabove;
- b) She has already and will continue to suffer anxiety, inconvenience, stress, loss of time, and fear as a result of said loss of information;
- c) She may in the future fall, victim to fraud and/or identity theft because of Defendant's loss of her personal information;
- d) She understands the nature of the action and has the capacity and interest to fairly and adequately protect and represent the interest of the Class Members;
- e) She is available to dedicate the time necessary for the present action before the Courts of Quebec and to collaborate with Class Counsel in this regard and Plaintiff is ready and available to manage and direct the present action in the interest of the Class Members that Plaintiff wishes to represent;
- f) Plaintiff is determined to lead the present file until a final resolution of the matter, the whole for the benefit of the Class Members;
- g) Her interests are not antagonistic to those of other Class Members;



- h) She has given the mandate to the undersigned attorneys to obtain all relevant information to the present action and intends to keep informed of all developments;
- i) She has given the mandate to the undersigned attorneys to post the present matter on their firm website in order to keep the Class Members informed of the progress of these proceedings and in order to more easily be contacted or consulted by said Class Members. In this regard, Class Counsel have already been contacted by many Class Members, R-4;
- j) She, with the assistance of the undersigned attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other Class Members and to keep them informed;

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

**FOR THESE REASONS, MAY IT PLEASE THE COURT:**

**GRANT** the present Application;

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

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

All persons in Canada (subsidiarily in Quebec), whose personal and/or financial information was compromised, lost and/or stolen from Defendant as a result of the data breach that occurred on or before December 11, 2017, or any other Group(s) or Sub-Group(s) to be determined by the Court;

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

- a) Was Defendant negligent and/or did Defendant commit a fault in the storing and safekeeping of the financial and/or personal information of the Class Members whose information was ultimately compromised, lost and/or stolen on or before December 11, 2017?
- b) Did Defendant commit a fault in the way in which it notified the Class Members about the data breach?
- c) Is Defendant liable to pay compensatory and/or moral damages to the Class Members as a result of the loss of said information, including without limitation actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and if so in what amounts?
- d) Is Defendant liable to pay punitive and/or exemplary damages to the Class Members, and if so in what amount?

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

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

**CONDEMN** Defendant to pay to the Class Members compensatory damages for all monetary losses 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 compensatory and/or moral damages, in the amount to be determined by the Court, as a result of Defendant's loss of Class Members' information, including without limitation for actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and **ORDER** collective recovery of these sums;

**CONDEMN** Defendant to pay an amount in punitive / exemplary damages to every Class Member, in the amount to be determine by the Court, 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 expert's fees and publication fees to advise Class Members;

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

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

**ORDER** the publication and notification of a notice to the Class Members in accordance with Article 579 C.C.P. pursuant to a further order of the Court and **ORDER** Defendant to pay for all said publication costs;



**THE WHOLE** with costs including the costs related to preparation and publication of the notices to Class Members.

**MONTREAL, February 12, 2018**

(s) Lex Group Inc.

---

**Lex Group Inc.**

Per: David Assor

Class Counsel / Attorneys for Plaintiff

4101 Sherbrooke St. West

Westmount, (Québec), H3Z 1A7

Telephone: 514.451.5500 ext. 321

Fax: 514.940.1605