CANADA
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

SUPERIOR COURT
(Class Action)

Nº : 500-06-001015-193

Y[redacted] B[redacted], residing and domiciled at [redacted];

Plaintiff

-vs-

STOCKX, LLC, a legal person constituted according to the law, having its head office at 1046 Woodward Ave., in the City of Detroit, State of Michigan, United-States of America, 48226;

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 Quebec and the rest of Canada, including their estates, executors or personal representatives, whose personal and/or financial information was provided to Defendant and compromised, lost and/or stolen from Defendant as a result of the Data Breach that occurred on or before July 26, 2019, 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. Defendant ("**StockX**") is a Detroit (U.S.A.) based company primarily known for its e-commerce platform StockX.com. The company was founded in 2015 with an emphasis on the sneaker resale market.

3. StockX calls itself the world's first "stock market of things". The platform works by buyers undercutting each other in a fashion, similar to the stock market. Defendant gives consumers a platform to buy and sell like-new merchandise in four categories: sneakers, watches, handbags and street wear.

4. StockX is considered one of the leading gauges of market value in the sneaker resale world.

5. The company earns revenue through a flat transaction fee and by taking a percentage of each sale. The website acts as a middleman between buyers and sellers, making these resale market transactions purportedly safe and secure.

6. StockX claims that it authenticates all products before they are sent to customers, so they never have to worry about scammers and fake items.

7. Before allowing a consumer to make a bid or purchase, StockX requires users to create an online profile with the company whereby users (and Class Members) are prompted to input personal information such as a user's name, email address, password, payment information and other related profile information.

8. StockX requires consumers to link to a payment method (PayPal or a credit/debit card) when placing bids.

9. StockX was recently valued at over $1 billion USD after a $110 million USD fundraise.

10. Plaintiff, like millions of other consumers in Canada, the United States, Australia, the United Kingdom and other countries who used Defendant's website, created a profile through which he provided his private Information in connection with his use of Defendant's online platform.

11. Despite learning on or about July 26, 2019 that its records and client information had been hacked, Defendant, incredibly, failed to inform its users and instead tried to hide the fact by sending out an email to its clients on August 1, 2019 telling its users to reset their passwords citing "system updates", the whole as more fully appears from the email sent to Plaintiff and the Class Members by Defendant, communicated herewith as **Exhibit R-1**.

12. The R-1 email does not mention the data breach or hack of Defendant's client information.

13. However, we note that since StockX users regularly receive multiple emails, sometimes multiple per day when tracking their bid or ask prices on desired goods, StockX users do not typically read all of their incoming StockX emails. They instead track their relevant activity through the Defendant's mobile application ("APP"). Accordingly, Plaintiff and many Class Members did not even read the misleading Exhibit R-1 password reset email;

14. Defendant chose not to draw attention to the data breach in question by not pushing the above notification and notifications mentioned below over their mobile APP and instead sent them by email.

15. After the Exhibit R-1 password reset email was sent, several media outlets reported that more than 6.8 million records were stolen from Defendant's website in May of 2019 by a computer "hacker", the whole as more fully appears from various online news articles, communicated herewith, *en liasse*, as **Exhibit R-2**.

16. It was only after this media coverage that Defendant first notified some of its clients of the data breach, by mere email once again, the whole as more fully appears from a copy of the August 3, 2019 email sent by Defendant to the Class Members, communicated herewith as though recited at length herein, as **Exhibit R-3**.

17. Plaintiff notes that as mentioned above, he did not read and did not retain the copy of the R-3 email in question sent to him specifically (if sent at all by Defendant), Plaintiff having likely deleted it together with other StockX emails received around the same time in the normal course of his use of Defendant's website and APP. Defendant is therefore summoned to file into the Court record the copy of the R-3 email sent to the Plaintiff as well as copies of all emails sent to the Plaintiff from August 1 to the date of this application inclusively.

18. In any case, the R-3 email does not offer much information about the incident nor offer any protection to Class Members.

19. However, a prominent technology publication, TechCrunch.com, was contacted by an unnamed data breached seller claiming more than 6.8 million records were stolen from Defendant in May 2019 by a hacker, the whole as more fully appears from the August 3, 2019 TechCrunch article at https://techcrunch.com/2019/08/03/stockx-hacked-millions-records, communicated herewith as though recited at length herein, as **Exhibit R-4**.

20. The seller in question declined to say how they obtained the data but informed

TechCrunch that the seller had already placed the data for sale for $300 and in fact sold it to presumed thieves, on the "dark web" (as per Exhibit R-4).

21. As appears from Exhibit R-4, the seller provided TechCrunch a sample of 1,000 records and TechCrunch contacted customers and provided them information only they would know from their stolen records, such as their real name and username combination and shoe size. Every person who responded to TechCrunch apparently confirmed their data as accurate.

22. 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.

23. The "dark web" is a part of the internet that is not indexed by search engines and has been described as a place where a "hotbed" of criminal activity occurs because of its difficulty to trace user activity.

24. Indeed, "dark web" users routinely buy and sell credit card numbers, all manners of drugs, guns, and other private information, including the private information now at issue in this class action.

25. The StockX stolen data in question purportedly contained names, email addresses, shipping address, purchase history, user passwords, users' shoe size, trading currency, and other profile information such as users' device type (for instance Android or iPhone) and the software version used by said device (hereinafter the "**Data Breach**").

26. Defendant, who requires the personal and financial information of its Customers in the context of a purchase or sale of goods over its online platform, 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.

27. When a data breach affecting 6.8 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.

28. This lawsuit stems from Defendant's failure to follow these obligations.

29. Indeed, as mentioned above, Defendant first covered up the Data Breach by merely pushing a password reset notification email to its clients on August 1, 2019 (Exhibit R-1), only citing a "system update".

30. After being exposed by the media (Exhibit R-2), Defendant sent the vague email notification to Class Members on August 3, 2019 (Exhibit R-3).

31. On August 8, 2019, Defendant sent a further email to Plaintiff and other Class Members, a copy of which is communicated herewith as though recited at length herein, as **Exhibit R-5**.

32. Once again, the R-5 email was not read by Plaintiff and likely other StockX users who receive multiple emails from the Defendant in the normal course of the use of the StockX mobile platform. Defendant chose not to push the notification in question through its mobile APP.

33. In the R-5 email, Defendant admits more facts about the Data Breach, namely that it had been first informed of it on July 26, 2019, namely alerted to "suspicious activity potentially involving customer data". It also confirms that the "an unknown third party had been able to fain unauthorized access to certain customer data from our cloud environment on or around May 14, 2019".

34. In the R-5 email, Defendant also apologized for the "ambiguity that resulted from [its] initial communication".

35. Plaintiff communicates herewith as though recited at length herein, *en liasse*, as **Exhibit R-6**, the various extracts from Defendant's website, including those related to the Data Breach in question.

36. The R-5 email to affected clients (including Plaintiff) and the R-6 extracts from Defendant's website confirm that Defendant was offering affected clients "12 months of free fraud detection and identity theft protection for added peace of mind", namely the MyIDCare™ product provided by IDExperts® which includes "CyberScan monitoring, fully managed id theft recovery services, a $1,000,000 insurance reimbursement policy, and 12 months of free credit monitoring".

37. This is a clear admission by Defendant that at very least, these types of insurance coverage and other protections are required under the circumstances in order to protect the affected clients.

38. However, all of these IDExperts® products and so-called protections are not available to anyone that does not have a US address and US Social Security Number (SSN).

39. Therefore, all of these IDExperts® protections and offers made by Defendant do not cover

and cannot be used by Plaintiff or any other Class Members in Canada and that there is no other products or protections offered to Canadians.

40. Plaintiff communicates herewith as though recited at length herein, *en liasse*, as **Exhibit R-7**, the various extracts from the IDExperts® website regarding the StockX Data Breach.

41. Finally, Plaintiff communicates herewith as though recited at length herein, as **Exhibit R-8**, the Class Action Complaint filed before the United States District Court - Southern District of Florida – Miami-Dade Division, in the case of Casey v. StockX, LLC, case 1:19-cv-23285-UU, the whole in order to more fully fulfill his burden to demonstrate an arguable case herein.

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

43. 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.

44. Defendant's 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.

45. 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.

46. 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;

47. Plaintiff and many Class Members have also paid or will pay certain fees or costs in order to further protect themselves, such as in order to activate a credit monitoring service or in order to purchase fraud insurance, 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.

48. 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

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

50. Plaintiff had previously created a profile through which he provided his private information in connection with his use of Defendant's online platform.

51. As mentioned above, Plaintiff received the password reset email from Defendant on August 1, 2019 (Exhibit R-1).

52. Plaintiff received the Exhibit R-5 email from Defendant. This confirms that his personal information is part of the Data Breach in question and that his information was stolen from Defendant's systems.

53. As mentioned above, Defendant did not send the notifications through its APP, knowing that many users, such as Plaintiff, receive many emails from StockX and do not read them all, or at the very least do not read them right away, since they are mostly related to specific auctions of goods over Defendant's online platform (many of which do not ultimately end with an actual transaction).

54. Before receiving the said emails, many Class Members had not otherwise been made aware of the Data Breach.

55. In the case of Plaintiff, he was only made aware of the Data Breach through subsequent online media reports published after the filing of the Florida Class Action proceedings (Exhibit R-8). Defendant therefore failed to notify the Plaintiff of the Data Breach.

56. 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. This represents additional faults by Defendant.

57. 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 the use of Defendant's website, which Defendant clearly did not.

58. As a result of learning that his personal information was lost by Defendant, Plaintiff

experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information.

59. Furthermore, Plaintiff has recently seen unauthorized transaction(s) on his credit card, following the StockX breach.

60. Plaintiff is therefore at greater risk of identity theft and fraud and has not been offered any protection from Defendant.

61. As detailed above, all of the so-called protections and offers by Defendant do not apply to Plaintiff or other Canadians and Defendant has failed or neglected to provide the Canadian Class Members with any protections whatsoever here in Canada.

62. Indeed, nowhere in the Defendants notices or website extracts (Exhibits R-3, R-5 and R-6) does Defendant mention that Canadians are not being offered protection at all;

63. In fact, Defendant provides 2 numbers for contacting IDExperts®, namely one number "if you are calling from the United States" and one number "if you are calling from outside of the United States", the whole in order to mislead the non-US clients as to what is being provided as coverage.

64. As mentioned above, the IDExpert® insurance coverage and protection products are not available to Canadians, unless they have a US social security number and US address.

65. In order to save money, Defendant has failed or refused to mandate and pay for TransUnion and Equifax Canada to automatically activate credit monitoring and fraud alerts for the Canadian clients affected such as Plaintiff.

66. Defendant has failed or refused to offer any protection or insurance whatsoever to the Plaintiff and the Class Members, who are left to fend for themselves.

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

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

69. Plaintiff and the Class Members would not have signed up for or used Defendant's website, providing the required personal and financial information, if they had known that Defendant would be negligent and careless with the Customers' personal information;

Punitive Damages:

70. 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;

71. 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. downplayed the gravity of the Data Breach and mislead the Class Members in its first communications and password reset push sent to the Class Members;

d. failed to notify the Plaintiff and many Class Members, including through its APP;

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 offer at least equivalent insurance coverage and other protections as those offered to US clients;

g. failed to inform the Class Members of the fact that the thief/thieves have already posted the stolen information for sale on the dark web and that certain individuals (thieves and/or fraudsters) have already purchased this stolen personal information, the whole as reported in the R-2 article.

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;

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

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

76. Every Class Member had his, her or its personal and financial information lost by Defendant as described hereinabove, including without limitation names, email addresses, shipping address, purchase history, user passwords, users' shoe size, trading currency, and other profile information such as users' device type (for instance Android or iPhone) and the software version used by said device.

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

78. 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.

79. 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.

80. 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.

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

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 great risk of fraud or identity theft.

83. 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

84. 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.

85. Plaintiff is unaware of the specific number of persons included in the Class but, as mentioned above, it appears that the names, email addresses, shipping address, purchase history, user passwords, users' shoe size, trading currency, and other profile information such as users' device type (for instance Android or iPhone) and the software version used by said device of 6.8 million of Defendant's customers had been lost, stolen or otherwise compromised as a result of the Data Breach.

86. Class Members are numerous and are scattered across the entire province and country since Defendant leases and finances vehicles across the country, including Quebec.

87. 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.

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

89. 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.

90. 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.

91. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely Defendant's negligence, and fault.

92. 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 July 26, 2019?

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?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

95. 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.

96. 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) A great number of Class Members used Defendant's website and completed consumer transaction from and in the judicial District of Montreal;

d) Defendant through its website carries on business in the District of Montreal;

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

97. 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) His personal information was provided to Defendant and lost by Defendant as described hereinabove, Plaintiff having received the Exhibit R-1 and R-3 notification emails from Defendant which were only sent to clients affected by the Data Breach (whose personal information was lost or stolen in the context of the Data Breach);

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

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

d) He 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) He 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) His interests are not antagonistic to those of other Class Members;

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

j) He, 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.

98. 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 Quebec and the rest of Canada, including their estates, executors or personal representatives, whose personal and/or financial information was provided to Defendant and compromised, lost and/or stolen from Defendant as a result of the Data Breach that occurred on or before July 26, 2019, 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 July 26, 2019?

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, August 12, 2019

(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