C A N A D A
PROVINCE OF QUEBEC
DISTRICT OF SAINT-FRANÇOIS

Nº : 450-06-000001-259

(Class Action)
SUPERIOR COURT

K. L., residing and domiciled [redacted];

Plaintiff

vs.

CENTRE DE SERVICES SCOLAIRE DES APPALACHES / APPALACHIAN SCHOOL SERVICE CENTER, 650, rue Lapierre, City of Thetford Mines, District of Frontenac, Province of Quebec, G6G 7P1;

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 SAINT-FRANCOIS, THE PLAINTIFF STATES THE FOLLOWING:

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 whose personal or financial information was held by Defendant and was compromised in the Data Breach which occurred on or about August 25, 2025, or who received an email or letter from Defendant informing them of such Data Breach;
>
> or any other Group(s) or Sub-Group(s) to be determined by the Court;

(hereinafter Class Members are collectively referred to as "**Class Member(s)**", "**Group Member(s)**", the "**Group**", the "**Class**", "**Customer(s)**" or "**Client(s)**").

The Defendant

2. For over 100 years, Defendant the Appalachian School Services Center (including its various previous names) has provided educational services to thousands of students each year. Defendant's annual budget is close to $100 million and it serves customers from the Regional County Municipalities of: des Appalaches, L'Érable, Haut Saint-François, Arthabaska and Granit. Its clientele presently consists of 7,000 young people and adults who attend 19 primary schools, 3 secondary schools, a vocational training center, and an adult education center, as well as their service points, the whole as more fully appears from extracts of the Defendants' website, communicated herewith as **Exhibit P-1**.

The Situation

3. On or about **August 25, 2025**, unauthorized third parties gained access to Defendant's systems and obtained, accessed, and exfiltrated the personal and financial information and data of the Class Members (hereinafter the "**Data Breach**").

4. Defendant abusively waited over a month before attempting to contact the affected Class Members (if at all to date).

5. In this regard, on September 24, 2025, Plaintiff's mother received a voice message from Defendant's representative asking her to have Plaintiff send Defendant an email, a copy of said voice message is communicated herewith as **Exhibit P-2**.

6. That same day and as requested in the Exhibit P-2 voice message, Plaintiff immediately sent an email to Defendant providing her contact information, a copy of the Plaintiff's September 24, 2025 email is communicated herewith, ***under seal***, as **Exhibit P-3**.

7. Defendant then proceeded to send a notification email/letter to the Plaintiff that same day of September 24, 2025, a copy of which is communicated herewith, as though recited at length, as **Exhibit P-4** (hereinafter the "**Notice**"), namely an excessive 31 days after the Data Breach occurred and was apparently discovered by Defendant.

8. Defendant is hereby summoned to retain and to file into the Court record herein the copies of all other notification emails or letters sent by Defendant to the Class Members.

9. As appears from the Notice, Defendant has confirmed and admitted the following:

    a) That the Data Breach occurred on August 25, 2025 wherein data including personal information of the Plaintiff and Class Members was stolen;

b) That Defendant was made aware of the Data Breach on that same day (August 25, 2025);

c) That in the days following August 25, 2025, some of the stolen data and personal information had already been published on the Dark Web;

d) That on September 10, 2025, additional stolen data and personal information was once again published on the Dark Web;

e) That the Plaintiff's personal information was also stolen in the context of said Data Breach, including without limitation her name, date of birth, gender, and a copy of her previous passport which therefore includes her picture (physical likeness) and the relevant passport number and information.

f) That Plaintiff's personal information and an actual copy of Plaintiff's passport had already been posted publicly on the Dark Web;

g) That Defendant suggests that Plaintiff contact Passport Canada in order to inform it of the theft of the copy of her passport;

h) That Defendant was only undertaking to reimburse a portion and not the totality of any passport replacement costs, the whole representing admissions by the Defendant: (i) that this theft is serious enough to inform Passport Canada and possibly request to change passports and (ii) that Defendant is responsible to reimburse the out-of-pocket expenses incurred by the Plaintiff and Class Members stemming from the Data Breach;

i) That Defendant would in the future (*très prochainement*) "propose" credit monitoring services (such as from Equifax) to the Plaintiff, representing a further admission by Defendant that such credit monitoring is required considering the severity of the Data Breach and the threat to the Plaintiff's and the Class Members' credit file;

j) That if the Plaintiff or Class Members notice "irregular activity" involving their bank accounts or identity, that Revenue Quebec and Revenue Canada should be notified, representing a further admission by Defendant that such so-called "irregular activity" is possibly stemming from this severe Data Breach and that said "irregular activity" can include bank fraud and/or identity theft;

k) That Defendant apologizes for the inconvenience that Plaintiff will suffer as a

result of the Data Breach, representing an admission by Defendant that the Plaintiff and Class Members will suffer moral damages such as inconvenience;

l) That Defendant's investigation is still ongoing, Defendant being hereby summoned to retain all investigation reports and findings, including the IT data used and consulted in the context of the investigation (including without limitation copies of the stolen data sets and the notification lists used by the Defendant).

10. The Plaintiff and the Class Members can therefore reasonably rely on these admissions, namely that the Data Breach represents a reasonably, real and current threat and risk of fraud and/or identity theft.

11. Accordingly, Defendant is confirming and admitting that the Plaintiff and Class Members are now at risk of social engineering and phishing techniques used by fraudsters in order to commit identity theft and/or fraud.

12. The stolen information is highly sensitive and essential to the security of the Plaintiff and Class Members. In particular, the name, date of birth, passport information and copies of passports, and physical likeness (i.e. passport picture) are critical data points frequently used in identity verification and, if exposed, significantly increases the risk of identity theft and/or fraud.

13. Defendant, who required the personal and financial information of its customers in the context of its enterprise and activities, had the obligation to protect that information and to ensure by all proper and required means that this information is safeguarded from compromise, theft or loss.

14. Defendant also had the obligation to not retain the Plaintiff's and the Class Members' personal information and data for longer than absolutely required, whereas Defendant retained said information for way too long, namely over 12 years in the case of the Plaintiff, representing further faults committed by the Defendant.

15. When a Data Breach affecting many thousand person occurs, Defendant had the obligation to immediately and accurately notify the Class Members in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience. This lawsuit stems from Defendant's multiple and repeated failures to follow these obligations, causing damages to the Class Members.

16. The Data Breach was reported by multiple media outlets, as appears from the various news articles, communicated herewith as **Exhibit P-5**, *en liasse*.

17. The September 3, 2025 courrierfrontena.qc.ca article entitled "*Le Centre de services scolaire des Appalaches ciblé par un rançongiciel*" (included in P-5), confirms *inter alia* the following:

> Le Centre de services scolaire des Appalaches (CSSA) est confronté à une attaque par rançongiciel après une cyberintrusion survenue la semaine dernière. Le groupe INC Ransom prétend via un portail du Web caché [dark web] avoir obtenu 180 Go de données de l'organisation.
>
> Une alerte a été publiée sur X [anciennement Twitter], le mercredi 3 septembre vers midi, par le compte ThreatMon Ransomware Monitoring, une plateforme de renseignements sur les menaces en ligne. Elle désigne la Commission scolaire des Appalaches en tant que victime de ce groupe de pirates informatiques. Rappelons que c'est la deuxième fois en moins de dix ans que l'organisation est l'objet d'une cyberattaque.
>
> …
>
> Le CSSA a par ailleurs assuré que toute exfiltration de données sensibles, le cas échéant, serait immédiatement communiquée avec les personnes concernées et des mesures de protection personnalisées seraient mises en place, en conformité avec les obligations de l'organisation.
>
> Enfin, une évaluation globale de l'incident devra être réalisée afin de comprendre ce qui n'a pas fonctionné malgré les mesures de sécurité ayant été renforcées depuis l'attaque de 2016.
>
> **Des données sensibles pourraient avoir été exposées**
>
> Selon le consultant en cybersécurité Steve Waterhouse, comme ce fut le cas en 2016, les pirates sont parvenus à s'installer dans le système informatique de l'organisation. M. Waterhouse est aussi chargé de cours au microprogramme en maîtrise de l'Université de Sherbrooke en sécurité de l'information, ancien officier de sécurité informatique au ministère de la Défense nationale et ancien sous-ministre adjoint à la sécurité de l'information gouvernementale et à la cybersécurité du Québec.
>
> D'après les informations divulguées par INC Ransom, environ 70 % de ce qu'ils auraient soutiré contiendraient des données personnelles d'importance concernant les élèves et les employés, des documents financiers, des documents légaux ainsi que des signatures. Des échantillons de ces données auraient été mis en circulation sur le Web caché et ceux-ci comporteraient notamment des photos de passeports, de permis de conduire et de spécimens de chèque. Une autre partie, environ 20 %, serait composée de documents scolaires et administratifs.

> M. Waterhouse a expliqué que la mise en circulation sur le Web caché d'un échantillon des données vise à démontrer la véracité de ce que les rançonneurs ont réussi à soutirer et qu'ils sont sérieux. Il a de plus affirmé qu'il est essentiel d'informer les personnes susceptibles d'être touchées puisqu'elles pourraient être victimes d'une cyberattaque à leur tour.
>
> …
>
> La conséquence pourrait alors être une fuite des informations sur le Web pouvant mener à des vols d'identité. M. Waterhouse a mentionné que lorsque cela arrive à des compagnies privées, comme on l'a vu avec Desjardins, les victimes se voient offrir une surveillance de dossier de crédit pour un certain temps. « Est-ce que ce sera le cas avec le gouvernement ? Je ne le sais pas, mais ce serait peut-être de bon augure parce que lorsque des fraudes surviennent, le fardeau de la preuve revient aux victimes, autrement dit, aux citoyens dont les informations personnelles ont été compromises. »
>
> Il a ajouté que si la fuite se confirmait, les personnes touchées devraient entreprendre des démarches afin de protéger leurs données financières.

18. Accordingly, from the P-4 Notice sent to the Plaintiff and from the above-cited P-5 news article, Plaintiff understands that the Data Breach involved the theft and exfiltration from the Defendant's servers of a staggering 180 gigabytes of data, including the Plaintiff's and the Class Members' personal and financial information, including without limitation the following data (*sauf à parfaire*):

a) Name;
b) Date of Birth;
c) Gender;
d) Copy or photos of passports (which therefore includes pictures and physical likeness) and the relevant passport number and information;
e) Copy or photos of driver's licenses (which therefore includes pictures and physical likeness) and the relevant driver's license number and information;
f) Copies of cheques (*spécimens de chèque*);
g) Financial documents;
h) Legal documents;
i) Other important personal data concerning students and employees,
j) School related documents;
k) Administrative related documents.

19. In addition, the P-5 article also confirms that the Defendant had already suffered a first

ransomware attack less than ten years ago and it therefore did not properly secure its IT systems thereafter, facilitating and permitting this new ransomware Data Breach to occur, further justifying a claim for punitive damages herein.

20. As mentioned above, Defendant was negligent in choosing to wait over and excessive 31 days 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.

21. The Notices were also faulty in that they did not properly and clearly confirm what information was actually stolen in the context of the Data Breach.

22. Moreover, Defendant failed to confirm that it would indemnify and hold the Class Members harmless of any losses or damages suffered as a result of the Data Breach.

23. Defendant has not yet actually offered any insurance or credit monitoring services to the Class Members, which is the bare minimum it should have already offered and provided under the circumstances. As mentioned above, the Notice promises to offer credit monitoring (sometime in the future) but there is no justification as to why over a month following the Data Breach, Defendant has not already set up and paid for said credit monitoring services, representing additional faults by the Defendant.

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

25. Defendant was negligent and committed faults in this regard since it failed to activate the TransUnion and Equifax services for their Class Members, and many Class Members are not even aware of the Data Breach (in case of not receiving the Notice for whatever reason including change of address or phone number, or bounce-back of emails).

26. By choosing not to automatically activate both credit agencies' credit monitoring services and by not posting the proper fraud alerts for all Class Members, Defendants 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 presently not offering this and has not paid to automatically activate these services.

27. As mentioned above, after becoming aware of the Data Breach, Defendant waited an excessive 31 days before starting to contact some but not all of the Class Members in order to inform them of Data Breach.

28. Accordingly, Defendant failed to promptly and quickly disclose the Data Breach to the Class Members/victims of the Data Breach, representing further faults committed.

29. Defendant is hereby summoned to confirmed whether it communicated with the unauthorized third parties who perpetuated the Data Breach, to confirm whether it paid the ransom being claimed by said third parties, and to produce copies of the said communications and/or details of payments made into the Court record.

30. 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.

31. As a result of the Defendant's inadequate data security, unauthorized third parties / cyber-criminals now possess the private information of Plaintiff and the Class Members and have already published samples of the stolen information (including a copy of the Plaintiff's passport) on the dark web, increasing the severity of this particular Data Breach and increasing the damages suffered by the Class Members (including without limitation moral damages).

32. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. By letting the excessive amounts of days pass before starting to notify affected Class Members (as detailed above), with many Class Members not even informed yet at all, Defendant failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Class Members.

33. Class Members have been and/or will be exposed to fraud and/or identity theft and these Class Members have been harmed as a result.

34. 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 or changing documents, loss time and expenses related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards, bank accounts, driver's licenses, or passports; (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, 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 the Class Members

potential targets for fraud and/or identity theft.

36. 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) To closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, for many months or years;

c) To be even more attentive than normally necessary concerning the communication of their personal information since they are at threat of social engineering and phishing, due to the higher possibility of fraudulent activity caused by Defendant's loss of the information (as confirmed in the Notice);

d) To inform their financial institutions of the loss of the information by the Defendant and to deal with said financial institutions 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) To inform the tax departments and/or Passport Canada and/or the SAAQ of the loss of the information and copies of passport and/or driver's license by the Defendant, and to deal with said institutions in order to reduce risk of fraud as much as possible.

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

g) A negative effect on their credit score.

37. 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 or alerts, title or other insurance, to change their personal information such as requesting new driver's licence numbers, new Social Insurance Numbers or new passport, for credit protection consulting services, etc. Defendant is solely responsible for these costs or fees paid by the Class Members and for the inconvenience caused to Class Members in this regard.

38. Plaintiff invokes *inter alia* the following sections of provincial and federal legislation and Plaintiff respectfully submits that the mere fact that the personal information was entrusted to the Defendant and subsequently lost by Defendant as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which make Defendant liable to pay compensatory, moral and punitive damages:

a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, S.Q. 1991, c. 64*;*

b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, CQRL, c. C-12;

c) Sections 1, 2, 3.1 and following, 10, 13, 17, 28, 29, and 93.1 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c. P-39.1;

d) Sections 52.2 to 70.1 and 167 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*, chapter A-2.1;

e) 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, 4.4, 4.7 of its Schedule 1;

f) Sections 1, 2, 8-12, 16, 17, 40-42, 215-228, 253, 261-272 of the Consumer Protection Act, Chapter P-40.1;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF

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

40. Plaintiff attended the Polyvalente de Thetford Mines high school from 2009 to 2014 (which is managed by the Defendant).

41. In 2012, Plaintiff participated in a school trip to Europe and was obliged to provide a copy of her passport to the Defendant via her high school. Assuming this is indeed the passport that was stolen and later posted on the dark web, Defendant therefore also failed in its obligation to not retain the Plaintiff's personal information and data (including the copy of her passport) for longer than absolutely required, whereas Defendant retained said information (and copy of passport) for way too long, namely over 12 years, representing further faults and gross negligence committed by the Defendant.

42. Plaintiff is now a practicing tax lawyer and a member in good standing of the *Barreau du Québec* since 2021.

43. As mentioned above, on September 24, 2025, Plaintiff's mother received a voice message from Defendant's representative asking her to have Plaintiff send Defendant an email, a copy of said voice message is already communicated Exhibit P-2.

44. That same day and as requested in the Exhibit P-2 voice message, Plaintiff immediately sent an email to Defendant providing her contact information, a copy of the Plaintiff's September 24, 2025 email is already communicated, ***under seal***, as Exhibit P-3.

45. Defendant then proceeded to send the P-4 Notice to the Plaintiff that same day of September 24, 2025, namely an excessive 31 days after the Data Breach occurred and was apparently discovered by Defendant.

46. This Notice informed Plaintiff for the very first time that Defendant had permitted unauthorized third-party individuals to gain access to her personal information, including a photo of her passport picture (and personal likeness / photo), and that here personal information and copy of passport had already been posted on the dark web (namely the part of the Internet used by fraudsters and criminals in order to facilitate crimes, fraud, identity theft, etc.).

47. Plaintiff immediately called Passport Canada on September 24, 2025 to inform it of the Data Breach. The Passport Canada agent confirmed that Plaintiff was indeed facing an elevated risk of identity theft as a result of the Data Breach in question. Plaintiff spent approximately 10 to 15 minutes on that call (loss of time being claimed as damages against Defendant herein).

48. Plaintiff then called her primary financial institution, namely the Desjardins, on September 24, 2025 to inform it of the Data Breach. The Desjardins agent also confirmed that Plaintiff was indeed facing an elevated risk of identity theft as a result of the Data Breach in question and that Plaintiff should contact Equifax Canada and TransUnion in order to place a freeze or fraud alert on her credit files. The agent proceeded to place a fraud alert note regarding Plaintiff's bank file at the Desjardins. Plaintiff spent approximately 20 to 30 minutes on that call (loss of time being claimed as damages against Defendant herein).

49. Plaintiff also exchanged emails with the Financière Banque Nationale to inform it of the Data Breach, a copy of said September 24, 2025 exchange of email with the Financière Banque Nationale is communicated herewith as **Exhibit P-6**.

50. As appears from P-6, the Financière Banque Nationale also recommended that Plaintiff place fraud alerts on her credit files with the credit bureaus and recommended that Plaintiff call its customer service department in order to discuss who to properly secure her bank accounts and investments.

51. That same day of September 25, 2025, Plaintiff indeed called the Financière Banque Nationale and was referred several times without being able to reach a representative capable of making the proper fraud alert notes on her filed. Plaintiff spent a total of approximately 45 minutes on those calls (loss of time being claimed as damages against Defendant herein).

52. On September 25, 2025, Plaintiff also called the Defendant's telephone number mentioned on the P-4 Notice. However, there was no way to reach an actual human agent and Plaintiff was forced to leave a voice message. An agent later called her back and left a voice message of her own, indicating that the agent would not be returning any calls until at least the following Monday, September 29, 2025.

53. Plaintiff then proceeded to access the Equifax Canada website and place a lock on her Equifax credit report, the September 25, 2025 confirmation email from Equifax Canada is communicated herewith as **Exhibit P-7**.

54. Plaintiff then called Equifax Canada in order to have a fraud alert placed on her credit file. Plaintiff spent approximately 20 to 30 minutes on that call (loss of time being claimed as damages against Defendant herein).

55. Plaintiff is very careful and cautious about protecting her personal information, credit file and data, especially as a tax lawyer.

56. Indeed, at the time of receiving the P-4 Notice, Plaintiff was already subscribed to the Equifax Canada credit monitoring services, although not the TransUnion credit monitoring services.

57. Very worried about protecting her credit file and assets after learning of the Data Breach, and in order to help further protect herself from fraud and identity theft (since Defendant was not actually offering any protection at all, as mentioned above), Plaintiff subscribed to the TransUnion Interactive credit monitoring services, at a price of $24.95 (plus taxes) per month, payable on an automatic recurring basis, which amounts she claims from Defendant as damages stemming directly from the Data Breach and the receipt of the Notice, the whole as more fully appears from her TransUnion email confirmation dated September 25, 2025, communicated herewith as **Exhibit P-8**.

58. As alleged above, Defendant should have offered such credit monitoring services to the Plaintiff and the Class Members (for multiple years of coverage) when sending the Notice, but it has refused or neglected to offer such protection in order to save money, therefore transferring the burden, cost, loss of time and inconvenience onto the Plaintiff and the Class Members, further faults committed by the Defendants.

59. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Defendant would properly safeguard their personal and financial information, which Defendant clearly did not.

60. As a result of learning that her personal information was lost by Defendant, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and fear due to the loss of personal information, and this, aside from unexpected out-of-pocket expenses.

61. In order to save money, Defendant have failed or refused to mandate and pay for TransUnion and Equifax Canada to immediately and automatically activate credit monitoring and fraud alerts for all affected Class Members such as Plaintiff.

62. 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.

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

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

65. Moreover, further faults were committed by Defendant, namely that it failed to even encrypt the personal information and data of its clients (Plaintiff and the Class Members).

Punitive Damages:

66. 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.

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

a. did not follow or properly implement an effective data security industry standard to protect the Class Members' highly sensitive personal and financial information, which information Defendant allowed to be accessed and/or downloaded/stollen by unauthorized third parties;

b. failed to promptly and clearly notify the Plaintiff and the Class Members of the Data Breach and failed to keep them informed;

c. failed to properly ensure that Plaintiff and Class Members are protected by credit monitoring services by both Equifax Canada and TransUnion and failing to post fraud alerts on the Class Members' credit files immediately after the Data Breach;

d. failed to timely detect and prevent the Data Breach;

e. failed to encrypt and protect the Class Members' personal and financial information and data;

f. retained the personal and financial information and data of the Plaintiff and the Class Members for an abusive amount of time, for instance the Plaintiff's passport picture for over 12 years;

g. failed to close off and/or remedy the vulnerabilities in its systems after a first similar ransomware data breach had occurred less than 10 years prior, evidencing a repeated pattern of negligence and carelessness when it comes to protecting and safeguarding the Class Members' data;

h. failed to offer indemnification for losses suffered by Class Members; and

i. Defendant has repeatedly committed such faults putting its clients' information at great risk and such past faults and conduct further warrant the award of punitive damages.

68. 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 at least $1,000 (*à parfaire*) to each Class Member

in punitive damages due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class Members.

69. Indeed, Plaintiff invokes and relies upon the following legislative provisions which provide for the minimum award of punitive damages in this particular situation, which applies herein (in favor of Plaintiff and each Class Member)*:*

a) Section 93.1 of the *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c. P-39.1:

> "Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the Civil Code causes an injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000."

b) Section 167 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*, chapter A-2.1;

> "Where the unlawful infringement of a right recognized by Chapter III causes injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000."

70. Defendant's above detailed actions qualify the fault as intentional which is a result of wild and foolhardy recklessness in disregard for the rights of the Class Members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class Members.

71. 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 of at least $1,000 (*à parfaire*) should be awarded to each Class Members.

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

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

73. Class Member had their personal information lost by Defendant as described hereinabove, and/or received a notice from Defendant.

74. Class Members have or will experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information and/or the receipt of the notice. Defendant has already admitted and confirmed that the Plaintiff and the Class Members will suffer inconvenience as a result of the Data Breach (as confirmed in the Notice).

75. Class Members have to closely monitor their accounts and emails looking for possible fraud and phishing, from now on and for all periods subsequent to the loss of information.

76. Class Members 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, IDs 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.

77. 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.

78. The Class Members' credit score may also be negatively affected as a result of the Data Breach.

79. 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.

80. 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 and negligence in the way it handled itself after being made aware of this Data Breach.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

81. 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 reasons detailed below.

82. Plaintiff is unaware of the specific number of persons included in the Class, but Plaintiff estimates that tens of thousands of Canadian Class Members have been impacted by the

Data Breach. Defendant is hereby summoned to confirm the total number of affect Class Members in Canada in general, and in Quebec particularly.

83. Class Members are numerous and are scattered across the entire province (and country).

84. 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 Defendant's conduct would increase delay and expense to all parties and to the Court system;

85. 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;

86. 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;

87. 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;

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

89. The claims of the Class Members raise identical, similar or related issues of law and facts (Article 575 (1) C.C.P.), namely:

(a) Did Defendant commit faults regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendant commit faults by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendant commit faults due to the deficiencies of the notices and information given to Class Members about the Data Breach?

(d) Is Defendant solidarily liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

92. 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 and moral damages caused as a result of Defendant's loss of Class Members' information, and **ORDER** collective recovery of these sums;
>
> **CONDEMN** Defendant to pay $1,000, *sauf à parfaire*, to each Class Members as punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;
>
> **THE WHOLE** with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

93. Plaintiff suggests that this class action be exercised as a national class action, before the

Superior Court, in either the District of Montreal or District of Saint-Francois, for the following reasons:

a) Plaintiff resides in the District of Saint-Francois;

b) A great number of Class Members reside in the judicial districts of Montreal and/or Sherbrooke;

c) The undersigned attorneys representing the Plaintiff and the proposed Class practice in the District of Montreal;

94. 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 well as out of pocket expense, 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.

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;

95. 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 whose personal or financial information was held by Defendant and was compromised in the Data Breach which occurred on or about August 25, 2025, or who received an email or letter from Defendant informing them of such Data Breach;
>
> 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) Did Defendant commit faults regarding the storage and the safe-keeping of the personal information of the Class Members?

(b) Did Defendant commit faults by delaying the notification to Class Members that a Data Breach had occurred?

(c) Did Defendant commit faults due to the deficiencies of the notices and information given to Class Members about the Data Breach?

(d) Is Defendant solidarily liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

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 and moral damages caused as a result of Defendant's loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendant to pay $1,000, *sauf à parfaire*, to each Class Members as punitive damages for the unlawful and intentional interference with their right to privacy and **ORDER** collective recovery of these sums;

THE WHOLE with interest and additional indemnity provided for in the *Civil Code of Quebec* and with full costs and expenses including experts' fees and publication fees to advise Class Members;

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 or notification of a notice to the Class Members in accordance with Article 579 C.C.P., pursuant to a further order of this Honorable Court;

ORDER that said notice be posted and available on the home page of Defendant's various websites, Facebook account(s), Instagram account(s) and X (formerly Twitter) account(s), and **ORDER** Defendant to send the notice by email with proof of receipt and by direct mail to all Class Members;

ORDER Defendant to pay for all said publication/notification costs;

THE WHOLE with costs including without limitation the Court filing fees herein, expert fees, stenography fees, bailiff and/or process server fees, and all costs related to preparation and publication of the notices to Class Members.

MONTREAL, September 26, 2025

(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. 101
Fax: 514.940.1605

SUMMONS

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

Filing of a judicial application

Take notice that the Plaintiff(s) has filed this application in the office of the Superior Court of Quebec in the judicial district of Saint-François.

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Sherbrooke, situated at 375, rue King Ouest, in the City of Sherbrooke (Quebec), District of Saint-François, within 15 days of service of the application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Plaintiff's lawyer or, if the Plaintiff is not represented, to the Plaintiff.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgment may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the Plaintiff in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Québec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Change of judicial district

You may ask the court to refer the originating application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the Plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

Transfer of application to Small Claims Division

If you qualify to act as a Plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the Plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

Calling to a case management conference

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the application, the Plaintiff intends to use the following exhibits:

Exhibit P-1: Extracts of the Defendants' website;

Exhibit P-2: September 24, 2025 voice message from Defendant;

Exhibit P-3: September 24, 2025 email from Plaintiff to Defendant;

Exhibit P-4: September 24, 2025 notification email/letter from Defendant to Plaintiff;

Exhibit P-5: Various news articles, *en liasse*;

Exhibit P-6: September 24, 2025 exchange of email with the Financière Banque Nationale.

Exhibit P-7: September 25, 2025 confirmation email from Equifax Canada to Plaintiff.

Exhibit P-8: TransUnion email confirmation dated September 25, 2025.

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, September 26, 2025

(s) *Lex Group Inc.*

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff

NOTICE OF PRESENTATION

(Article 223 of the Superior Court's Directives for the Montreal District)

TO:

CENTRE DE SERVICES SCOLAIRE DES APPALACHES /
APPALACHIAN SCHOOL SERVICE CENTER
650, rue Lapierre
Thetford Mines, Quebec
G6G 7P1

Defendant

TAKE NOTICE that the present Application for Authorization to Institute a Class Action will be presented before the Superior Court, at the Sherbrooke Courthouse located at 375, rue King Ouest, in the City of Sherbrooke (Quebec), District of Saint-François, at a date to be determined by the Court.

MONTREAL, September 26, 2025

(s) *Lex Group Inc.*

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff

№.: 450-06-000001-259

(Class Action)
SUPERIOR COURT
PROVINCE OF QUEBEC
DISTRICT OF SAINT-FRANÇOIS

K. L.

Plaintiff

vs.

CENTRE DE SERVICES SCOLAIRE DES APPALACHES / APPALACHIAN SCHOOL SERVICE CENTER

Defendant

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION

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 (ext./poste 101)
F: 514.940.1605
@: davidassor@lexgroup.ca