C A N A D A
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

N° : 500-06-001422-258

(Class Action)
SUPERIOR COURT

M.O.;

Plaintiff

vs.

ORGANISME CANADIEN DE RÉGLEMENTATION DES INVESTISSEMENTS / CANADIAN INVESTMENT REGULATORY ORGANIZATION, legal person domiciled at Bay Adelaide North, 40 Temperance, Suite 2600, City of Toronto, Province of Ontario, M5H 0B4;

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:

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 11, 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. Defendant the Canadian Investment Regulatory Organization (hereinafter "**CIRO**") is the national self-regulatory body that oversees all investment dealers, mutual fund dealers, and trading activity on Canada's debt and equity marketplaces. It carries on the regulatory functions of the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association of Canada (MFDA), and is mandated to protect investors, enforce high standards of conduct and proficiency for firms and representatives, and ensure compliance with regulatory requirements. Its enforcement and surveillance teams, based in multiple cities in Canada, monitor trading activity in real time and discipline firms or individuals where misconduct is identified, the whole as more fully appears from extracts of CIRO's website, communicated herewith as **Exhibit P-1**.

The Situation

3. On or about **August 11, 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. Defendant proceeded to send a notification email/letter to the Plaintiff on or about September 9, 2025, a copy of which is communicated herewith, as though recited at length, as **Exhibit P-2** (hereinafter the "**Notice**"), namely an excessive 30 days after the Data Breach occurred and was apparently discovered by Defendant (Plaintiff having only received said notice himself during the week of September 22, 2025).

6. 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.

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

   a) That the Data Breach occurred on August 11, 2025 wherein data including personal and financial information of the Plaintiff and Class Members was stolen;

   b) That Defendant was made aware of the Data Breach on that same day (August 11, 2025);

   c) That data relating to all mutual fund dealer and investment dealer firms and

individuals had been impacted;

d) That the Plaintiff's personal information was also stolen in the context of said Data Breach, including without limitation his name, residential address, date of birth, country of birth, email address, gender, eye and hair colour, height, weight, any possible civil or criminal infractions, and the Defendant's complete investigation into the Plaintiff, as well as any information submitted by the Plaintiff when registering with Defendant (or its predecessors), namely passport number, investment and beneficiaries information, financial information, information regarding other external activities, student numbers, and non-securities license numbers;

e) That Defendant has undertaken to provide two years of credit monitoring services (such as from Equifax and Transunion) 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 and identity;

f) That Defendant is monitoring the dark web for any suggestion that data has been published, further admitting the ongoing risk of publication and misuse of Plaintiff's confidential information going forward;

g) That the Plaintiff and Class Members must remain vigilant since they are now at higher risk of phishing and other social engineering methods in order to commit fraud and/or identity theft as a result of this severe Data Breach;

h) That Defendant regrets that this Data Breach occurred and that it has now put into place additional security measures in order to avoid a reoccurrence, representing an admission by Defendant that its original security measures were inadequate (a fault committed by Defendant);

i) That Defendant has conducted an investigation - 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).

8. 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.

9. The nature and extent of the compromised data remain highly sensitive and capable of identifying individuals and being misused for fraudulent purposes.

10. 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.

11. The stolen information is highly sensitive and essential to the security of the Plaintiff and Class Members. In particular, the name, date of birth, physical traits, passport information and financial information are critical data points frequently used in identity verification and, if exposed, significantly increases the risk of identity theft and/or fraud.

12. 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.

13. Defendant, whose mandate includes the protection of investors, the supervision of Canada's investment and mutual fund dealers, and the monitoring of market integrity, is under the obligation to maintain robust information technology systems in order to protect the sensitive personal and financial information of the Plaintiff and the Class Members that it collects and holds in the exercise of its regulatory functions.

14. Despite this obligation and the Defendant's own public representations emphasizing its role in safeguarding market confidence and enforcing high standards across the financial industry, Defendant failed to implement adequate cybersecurity and data protection measures, thereby committing a fault inconsistent with the trust placed in it by registrants, investors, and the public.

15. Defendant confirms that registration data dating back to the early 2000s remains stored in the National Registration Database, and that it "cannot delete historic registration information", despite being aware of the risks associated with the indefinite retention of highly sensitive personal data (a further fault).

16. 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 also stems from Defendant's failures to follow these obligations, causing damages to the Class Members.

17. Accordingly, from the P-2 Notice sent to the Plaintiff and the P-1 FAQ section of the

Defendant's website regarding the Data Breach, Plaintiff understands that the Data Breach involved the theft and exfiltration from the Defendant's servers, including the Plaintiff's and the Class Members' personal and financial information, including without limitation the following data (*sauf à parfaire*):

a) Legal and other personal names;
b) Residential address;
c) Email address;
d) Telephone number;
e) Date of Birth;
f) Country of Birth;
g) Gender;
h) Eye and hair colour;
i) Height;
j) Weight;
k) Bank account numbers;
l) Investment and beneficiary information;
m) Financial information;
n) Civil and criminal disclosure;
o) Investigation notes or findings;
p) External activity information;
q) Passport information;
r) Student numbers;
s) Non-securities license numbers.

18. As mentioned above, Defendant was negligent in choosing to wait over an excessive 30 days before actually starting to notify 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 (Plaintiff having only received the P-2 notice approximately 42 days after the Data breach has occurred, as mentioned above).

19. 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.

20. 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.

21. Defendant was negligent and committed faults in this regard since 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).

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

23. In order to save money, Defendant chose to only offer a two (2)-year period of credit monitoring and identity theft protection, rather than implementing stronger, ongoing safeguards. This measure is manifestly insufficient given the gravity of the breach, the sensitivity of the information exposed (including biometric and financial data), and the vast number of current and former registrants affected across Canada.

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

25. 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.

26. 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 may have already published all or portions of the stolen information 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).

27. 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.

28. 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.

29. 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;

30. 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.

31. 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 other governmental institutions of the loss of the personal, financial and passport information 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.

32. 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 (including after the inadequate 2 year period offered by the Defendant) 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 bank account 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.

33. 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

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

35. Plaintiff was previously a broker at [redacted] Securities Inc. / Valeurs mobilières [redacted] Inc. which is regulated by the Investment Industry Regulatory Organization of Canada ("**IIROC**"), now regulated by the Defendant.

36. Plaintiff was registered to trade and act as a dealing representative and salesperson in Quebec. He further provided Defendant with various information, namely without limitation his personal information, his workplace, his registered location, the list of completed industry courses, and answers to regulatory disclosure questions, the whole as more fully appears from the IIROC Advisor Report on the Plaintiff, communicated herewith as **Exhibit P-3, under seal.**

37. Plaintiff ceased working as a broker in 2012.

38. During the week of September 22, 2025, Plaintiff received the P-2 Notice from Defendant (which is dated September 9, 2025), namely an excessive approximate 42 days after the Data Breach occurred and was apparently discovered by Defendant.

39. This Notice informed Plaintiff for the very first time that Defendant had permitted unauthorized third-party individuals to gain access to his personal information, including his bank account numbers, passport number, non-securities license numbers, other financial and personal information, etc.

40. Plaintiff then proceeded to access the Equifax Canada website and subscribe to its credit monitoring services, the whole as more fully appears from the October 3rd, 2025 confirmation email from Equifax Canada is communicated herewith as **Exhibit P-4**.

41. Plaintiff also proceeded to subscribe to the TransUnion Interactive credit monitoring services, the whole as more fully appears from the October 3rd, 2025 TransUnion email confirmation, communicated herewith as **Exhibit P-5.**

42. Plaintiff is very careful and cautious about protecting his personal information, credit file and data, especially as a former broker. He is very worried about protecting his credit file and assets after learning of the Data Breach.

43. As alleged above, Defendant should have offered credit monitoring services and insurance coverage to the Plaintiff and the Class Members for more than 2 years of coverage, but it has refused or neglected to offer more than 2 years of protection in order to save money, therefore transferring the burden, cost, loss of time and inconvenience onto the Plaintiff and the Class Member (further faults committed by the Defendants). Indeed, Plaintiff will be forced to renew the said credit monitoring services at his own costs after the first two years expire (further claims against Defendant).

44. The 2-year credit monitoring services offered are wholly insufficient considering the magnitude of the breach, the sensitivity of the information compromised, and the vast

number of current and former individuals registered with CIRO whose personal and financial data has been exposed.

45. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Defendant would properly safeguard their personal and financial information, especially given the nature of the CIRO's mission, which Defendant clearly did not.

46. 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 fear due to the loss of personal information, and this, aside from unexpected out-of-pocket expenses.

47. Defendant, whose mandate includes protecting investors, supervising investment and mutual fund dealers across Canada, and ensuring the integrity of financial markets, had the obligation to ensure, by the most technologically sophisticated means possible and available, that said personal and financial 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.

48. In addition, Defendant committed a fault by retaining the very private, personal and financial information of the Plaintiff and the Class Members for several years more that Defendant actually required to retain said information, Indeed, in the case of the Plaintiff, the Defendant abusively retain his personal and financial information for over 13 years following Plaintiff ceasing to be a broker, which in an of itself is excessive and abusive, engaging the Defendant's liability herein.

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

g. retained the private, personal and financial information of the Plaintiff and Class Members for an abusive and excessive number of years instead of deleting said information.

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 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.

52. 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."

53. 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.

54. 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

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

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

57. 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).

58. 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.

59. 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.

60. 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.

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

62. 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.

63. 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

64. 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.

65. 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.

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

67. 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;

68. 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;

69. 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;

70. 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;

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

72. 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 liable to pay compensatory damages, moral damages or punitive damages to the Class Members, as a result? And if so, in what amounts?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

75. 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;

76. Plaintiff suggests that this class action be exercised as a national class action, 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 District of Montreal;

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

77. 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 lost by Defendant as described hereinabove;

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 his 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;

78. 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 11, 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 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, October 6, 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 Montreal.

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal, situated at 1, Notre-Dame Est, Montréal, Québec within 15 days of service of the application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Plaintiff's lawyer or, if the Plaintiffs is not represented, to the Plaintiffs.

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, *en liasse*;

Exhibit P-2: The September 9, 2025 notification letter from Defendant;

Exhibit P-3: The IIROC Advisor Report regarding Plaintiff, **under seal**;

Exhibit P-4: The October 3rd, 2025 Equifax Canada email confirmation;

Exhibit P-5: The October 3rd, 2025 TransUnion email confirmation.

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, October 6, 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:

ORGANISME CANADIEN DE RÉGLEMENTATION DES INVESTISSEMENTS / CANADIAN INVESTMENT REGULATORY ORGANIZATION
Bay Adelaide North
40 Temperance, Suite 2600
Toronto, Ontario
M5H 0B4

Defendant

TAKE NOTICE that APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION will be presented before the Superior Court at 1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6, on the date set by the coordinator of the Class Action chamber.

MONTREAL, October 6, 2025

(s) *Lex Group Inc.*

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

№.: 500-06-001422-258

(Class Action)
SUPERIOR COURT
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

M. O.

Plaintiff

vs.

ORGANISME CANADIEN DE RÉGLEMENTATION DES INVESTISSEMENTS / CANADIAN INVESTMENT REGULATORY ORGANIZATION

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