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

Nº : 500-06-000083-267

CLASS ACTIONS DIVISION
SUPERIOR COURT

J[redacted] G[redacted] residing and domiciled at [redacted];

Plaintiff

vs.

LOBLAW COMPANIES LIMITED / LES COMPAGNIES LOBLAW LIMITÉE, legal person duly constituted according to the Law, having its head office at 800-22 St. Clair Avenue East, City of Toronto, Province of Ontario, M4T 2S5, and having its *fondé de pouvoir* at 900-1000 rue De La Gauchetière Ouest, in the City and District of Montreal, Province of Quebec, H3B 5H4;

-and-

LOBLAWS INC., legal person duly constituted according to the Law, having its head office at 800-22 St. Clair Avenue East, City of Toronto, Province of Ontario, M4T 2S5, and having its elected domicile at 10-400 Sainte-Croix Avenue, in the City and District of Montreal, Province of Quebec, H4N 3L4;

Defendants

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:

Class:	**Groupe:**
All persons in Canada whose personal and/or financial information was held by Defendants and was accessed, compromised or stolen in the Data Breach which occurred between on or about February 23, 2026 and on or about March 5, 2026, or who received an email or letter from Defendants informing them of such Data Breach;	Toutes les personnes au Canada dont les renseignements personnels et/ou financiers étaient détenus par les Défenderesses et ont été consultés, compromis ou volés lors de la Fuite de données survenue entre le ou vers le 23 février 2026 et le ou vers le 5 mars 2026, ou qui ont reçu un courriel ou une lettre des Défenderesses les informant de cette Fuite de données;
or any other Group(s) or Sub-Group(s) to be determined by the Court.	ou tout autre groupe ou sous-groupe à déterminer par le Tribunal.

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

The Defendants

2. Loblaw Companies Limited / Les Compagnies Loblaw Limitée (hereinafter "**Loblaw**") describes itself as "Canada's food and pharmacy leader", operating more than 2,400 stores across Canada, employing approximately 190,000 Canadians, and counting more than 18 million PC Optimum members and 3 million PC Financial Mastercard cardholders, the whole as more fully appears from a copy of the extracts of Loblaw's website ("Who we are"), communicated herewith as **Exhibit AP-1**.

3. Loblaw is a legal person constituted in 1956 under the Canada Business Corporations Act, registered in Quebec since 1995, having its head office in Toronto, Ontario, and having a *fondé de pouvoir* in Quebec, the whole as more fully appears from a copy of the *Registraire des entreprises du Québec* report concerning Loblaw Companies Limited / Les Compagnies Loblaw Limitée, communicated herewith as **Exhibit AP-2**.

4. Loblaws Inc. (hereinafter "**Loblaws Inc.**", and together with Loblaw, the "**Defendants**") is a legal person constituted under the Ontario Business Corporations Act, registered in Quebec since 1999, having its head office at the same address as Loblaw in Toronto, Ontario, and having an elected domicile in Quebec, the whole as more fully appears from a copy of the *Registraire des entreprises du Québec* report concerning Loblaws Inc., communicated herewith as **Exhibit AP-3**.

5. Loblaws Inc. is a subsidiary of Loblaw: Loblaw is the majority shareholder of Loblaws Inc. and its ultimate beneficiary, holding more than 75% of its voting rights, as appears from Exhibit AP-3. It is indeed likely the wholly owned subsidiarity of Loblaw.

6. Loblaws Inc. has its principal establishment in Montreal at 400 Sainte-Croix Avenue, more than 5,000 employees in Quebec, and numerous establishments throughout Quebec operating notably under the Maxi, Maxi & Cie and Provigo names, as appears from Exhibit AP-3.

7. Loblaws Inc. also carries on business in Quebec under numerous other declared names, including "Les Compagnies Loblaw limitée / Loblaw Co. Ltd.", "Compagnie Loblaw limitée / Loblaw Company Ltd.", "LCL", "Loblaw", "Loblaw Québec", "Groupe Loblaws", "Loblaws", "Maxi", "Provigo" and "PC mobile", as appears from Exhibit AP-3.

8. Per Bank is both the President and Chief Executive Officer of Loblaw and the President and Chief Executive Officer (Président, Directeur général) of Loblaws Inc., as appears from Exhibits AP-2 and AP-3.

9. Loblaw also operates in Quebec through its Provigo grocery banner (acquired in 1998) and its Pharmaprix pharmacy banner (in Quebec since 1972), as appears from Exhibit AP-1.

10. In the course of their enterprise, Defendants collect, use and store the personal information of millions of their customers, including through the PC Optimum loyalty program, the PC Express online grocery service and the other applications using the universal "PCid" login credentials, the PC Optimum and PCid trademarks being trademarks of Loblaws Inc. used under license.

11. Defendants are hereby summoned to confirm which of them collected, held and controlled the personal information of the Class Members affected by the Data Breach, and which of them operated the systems that were accessed (breached).

The Situation

12. On or about February 23, 2026, unauthorized third parties gained access to Defendants' information technology systems and accessed, obtained and/or exfiltrated the personal information of the Class Members (hereinafter the "**Data Breach**" or "**Data Incident**").

13. Defendants only became aware of this unauthorized access on or about March 5, 2026, namely ten (10) days after it began, and only started notifying the affected Class Members directly on October 19, 2026, namely 228 days later, as detailed below.

14. Both of these delays are excessive, confirm that Defendants' security, IT, cybersecurity, and other protocols were grossly lacking, and warrant a condemnation in damages against Defendants, including punitive damages.

15. As Loblaw has itself confirmed to the Office of the Privacy Commissioner of Canada (hereinafter the "**OPC**"), the threat actors gained access to its systems "by leveraging compromised credentials for a platform it used for quality assurance activities", the whole as more fully appears from a copy of the Compliance Letter signed by Loblaw on October 21, 2026 and published by the OPC, communicated herewith as **Exhibit AP-4** (at par. 10).

16. In other words, the personal information of approximately two (2) million Canadians was accessible through a quality assurance platform protected by credentials which Defendants failed to adequately secure, representing a fault committed by Defendants. Defendants are hereby summoned to confirm whether multi-factor authentication or any other access control was in place on said platform at the time of the Data Breach.

17. On March 10, 2026, Loblaw issued a press release entitled "Loblaw Notifies Customers of a Low-Level Data Breach", the whole as more fully appears from a copy of the press release issued by Loblaw on March 10, 2026, communicated herewith as **Exhibit AP-5**.

18. In said press release, Loblaw described the incident as "low-level", stated that the breach occurred on "a contained, non-critical part of its IT network", and stated that the criminal third party had accessed "some basic customer information such as **names, phone numbers, and email addresses**", as appears from Exhibit AP-5.

19. On that same day, Loblaw posted a public advisory on its website and sent an in-app message to users of its PC Optimum application, stating that "passwords, health information and credit card data were not compromised" and reassuring its customers that "Your account is secure", the whole as more fully appears from a copy of the public advisory entitled "Important information about your account" published by Loblaw on its website on March 10, 2026 and updated on October 2, 2026, communicated herewith as **Exhibit AP-6**.

20. These March 10, 2026 communications abusively minimized the gravity and the scope of the Data Breach, as subsequently revealed by Loblaw itself several months later. This was done intentionally in order to downplay the Data Breach and further pacify Class Members and the public.

21. Indeed, it was only on October 2, 2026, namely 206 days later, and only "following a request from the OPC", that Loblaw posted an updated public advisory disclosing that the information impacted also included **addresses, dates of birth, loyalty account numbers, certain purchase order details, partial payment card information and billing and shipping addresses**, as appears from Exhibit AP-4 (par. 11) and Exhibit AP-6.

22. Contrary to Loblaw's March 10, 2026 representations that only "basic customer information such as names, phone numbers, and email addresses" had been accessed and that "credit card data were not compromised", the Data Breach in fact exposed, *inter alia*, the Class Members' dates of birth, home addresses, email addresses, loyalty card numbers, purchase order details and partial payment card information, as admitted by Loblaw itself to the OPC and in its updated public advisory, as appears from Exhibit AP-4 (par. 10) and Exhibit AP-6, and as also reported in the media, the whole as more fully appears from a copy of various news articles reporting on the Data Breach, communicated herewith, *en liasse*, as **Exhibit AP-7**.

23. As summarized by the OPC itself, the Data Breach occurred in February 2026 when "a hacking group gained access to its systems and customer account information", the whole as more fully appears from a copy of the news release published by the OPC on October 26, 2026, communicated herewith as **Exhibit AP-8**.

24. Loblaw has confirmed to the OPC that the Data Breach affected approximately two (2) million Canadians, whose impacted information included one or more of their **name, email address, postal address, phone number, date of birth, loyalty account number, purchase order details, incomplete payment card information, and billing and shipping address**, as appears from Exhibit AP-4, para. 10.

25. Loblaw has also confirmed to the OPC that other personal information was impacted for approximately 300 affected individuals, who were to receive tailored notification letters, as appears from Exhibit AP-4 (par. 10, footnote 3). Defendants are hereby summoned to disclose the nature of this other personal information.

26. Loblaw further determined, and confirmed to the OPC, that the legal threshold of a "**real risk of significant harm**" within the meaning of the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") was met with respect to the impacted data, as appears from Exhibit AP-4 (par. 10). This represents an admission that the Data Breach exposes the Class Members to a real risk of significant harm.

27. Direct notifications to the affected individuals only started being sent on October 19, 2026, as appears from Exhibit AP-4 (par. 12), namely 238 days (almost eight (8) months) after the Data Breach began and 228 days (more than seven (7) months) after Defendants became aware of it, which constitutes an excessive and abusive delay.

28. It is excessive and abusive, let alone being an additional fault and negligence committed by Defendant, that approximately two (2) million Canadians remained unaware, for 228 days after Defendants became aware of the Data Breach, that their personal information was in the hands of criminals, especially for sophisticated enterprises of Defendants' size and means which had the proper contact information to quickly reach the Class Members.

29. The OPC has launched a Commissioner-initiated investigation into the Data Breach to examine the adequacy of (i) the security safeguards in place at the time of the Data Breach and (ii) the notifications to affected individuals, which investigation remains open until Loblaw has fulfilled the commitments set out in the Compliance Letter, as appears from Exhibit AP-4 (par. 2 and 4) and from Exhibit AP-8.

30. By said Compliance Letter, Loblaw notably committed to provide the OPC with an independent external security assessment of its safeguards, and with a description of the process and methodology used to determine who was impacted and to notify them, as appears from Exhibit AP-4 (par. 17 to 21). Defendants are hereby summoned to retain and to file into the Court record herein all such reports, assessments, descriptions and updates provided to the OPC, as well as all their own investigation reports and findings regarding the Data Breach.

31. The notifications were sent through Loblaw's partner Cyberscout, a division of

TransUnion, as appears from Exhibit AP-6.

32. In the "Frequently Asked Questions" section of its public advisory, Loblaw further admits and represents the following, as appears from Exhibit AP-6:

    (i) that "Our investigation confirmed that certain data containing personal information was illegally obtained";

    (ii) that it holds its customers' personal information "in connection with its relationship with customers through providing various services to them, in-store, online, or through an app";

    (iii) that persons who believe they have experienced fraud should report it to their local police service and to the Canadian Anti-Fraud Centre;

    (iv) that customers should be alert to the risk of phishing and fraudulent emails, regularly review their account statements, change their passwords and "Enable multi-factor authentication"; and

    (v) that persons who received a notification letter are encouraged to take advantage of the credit monitoring and identity theft protection "offered through TransUnion".

33. These represent further admissions that the personal information of the Class Members was stolen and that there is a real and substantial risk of fraud and phishing (or other fraud or identity theft methods) as a result of the Data Breach.

34. In that same advisory, Loblaw represents that "Privacy and information security are top priorities, and strict measures are in place to protect the information in our care", as appears from Exhibit AP-6. These representations are contradicted by the Data Breach itself, which was carried out by leveraging compromised credentials for a quality assurance platform, while Loblaw recommends multi-factor authentication to its own customers.

35. Loblaw also answers "Yes" to the question "Has the incident been resolved?", as appears from Exhibit AP-6, although the approximately two (2) million affected Class Members had not yet even begun to be notified when said answer was published, and although the Class Members' stolen information remains in the hands of criminals.

36. Loblaw's various public statements regarding the Data Breach are inconsistent with

one another and with the facts later admitted to the OPC, as detailed hereinabove and below.

37. As to the nature of the breach, on March 10, 2026, Loblaw described "suspicious activity on a contained, non-critical part of its IT network" and "unusual activity on a limited part of our system" (Exhibits AP-5 and AP-6), whereas it later admitted to the OPC that the threat actors used compromised credentials for a quality assurance platform to access the personal information of approximately two million Canadians, meeting the "real risk of significant harm" threshold (Exhibit AP-4, par. 10).

38. As to the information stolen, on March 10, 2026, Loblaw represented that only "some basic customer information such as names, phone numbers, and email addresses" was accessed and that "credit card data were not compromised" (Exhibits AP-5 and AP-6), whereas it later admitted that the information stolen also included dates of birth, home, billing and shipping addresses, loyalty account numbers, purchase order details and incomplete payment card information, and, for approximately 300 individuals, other personal information (Exhibit AP-4 (par. 10 and footnote 3) and Exhibit AP-6).

39. As to the dates, the March 10, 2026 press release did not disclose the date on which the unauthorized access began nor the date on which Loblaw became aware of it (Exhibit AP-5), whereas Loblaw later disclosed that it became aware of the unauthorized activity "on or around March 5, 2026" (Exhibit AP-6), that it "confirmed unauthorized access" on March 5, 2026 (Exhibit AP-4, par. 10), and that the earliest access was likely on February 23, 2026 (Exhibit AP-4, par. 10), the OPC itself describing the breach as having occurred in February 2026 (Exhibit AP-8).

40. As to prior disclosure, the notice sent to the Plaintiff on October 29, 2026 (described below) states "Comme nous l'avons divulgué précédemment" (as we previously disclosed) before referring to March 5, 2026, although the Plaintiff (and likely many if not all other Class Members) never received any prior disclosure from Defendants before the end of October 2026.

41. As to PC Financial, on March 10, 2026, Loblaw stated that "PC Financial was not impacted by this breach" (Exhibits AP-5 and AP-6), whereas the customers were logged out of all applications using PCid credentials, which, as reported in the media, include the PC Optimum loyalty program, the PC Express online grocery service and the PC Financial portal (Exhibit AP-7). Defendants are hereby summoned to confirm whether any PC Financial customer information or credentials were accessed.

42. Loblaw has also admitted to the OPC that, after the Data Breach, it implemented additional security enhancements, namely enhanced identity security controls and procedures, strengthened monitoring and threat-detection capabilities, extended geo-based access restrictions, and enhanced training and awareness regarding secure development practices, as appears from Exhibit AP-4, par. 14. These measures, which were only implemented after the Data Breach, confirm that Defendants' prior safeguards were inadequate.

43. Moreover, as announced by the OPC, Loblaw "has committed to take actions aimed at strengthening its security measures following a cyberattack that impacted approximately two million Canadians" and "agreed to take additional measures to meet its obligations under Canada's federal private-sector privacy law and prevent future breaches", including engaging an external security firm to assess the effectiveness of its enhanced measures, as appears from Exhibit AP-8 and Exhibit AP-4 (par. 16 to 18). Loblaw thereby confirms that its security measures were lacking and did not meet its legal obligations at the time of the Data Breach.

44. Loblaw has also admitted that it must still provide the OPC with a description of the process used "in its efforts to notify impacted individuals as soon as feasible" and of its methodology for determining which affected individuals were subject to a real risk of significant harm, as appears from Exhibit AP-4 (par. 20 and 21). Defendants are hereby summoned to produce said descriptions and methodology into the Court record.

45. Loblaw has further admitted that its notices would include, only "where appropriate", an offer of complimentary credit monitoring and identity protection services, as appears from Exhibit AP-4 (par. 15). Defendants are hereby summoned to confirm which Class Members were not offered such services.

46. On October 29, 2026, a notice entitled "Avis concernant un incident de sécurité des données" was sent by email to the Plaintiff in the name of "Les Compagnies Loblaw Limitée" (a name used in Quebec by both Defendants, as detailed above), signed by Mr. Per Bank as "Président et chef de la direction", the whole as more fully appears from a copy of the notice dated October 29, 2026 sent to Plaintiff (name, email and activation code redacted), communicated herewith as **Exhibit AP-9** (hereinafter the "**Notice**").

47. Defendants are hereby summoned to retain and to file into the Court record herein copies of all other versions of the notification emails and letters sent to the Class Members, since, as Loblaw admits, the information impacted "varied by customer"

and the notices were tailored accordingly.

48. As appears from the Notice, Defendants have confirmed and admitted the following:

    (i) that they detected unauthorized activity in certain of their technology systems on or about March 5, 2026;

    (ii) that the first unauthorized access likely took place on February 23, 2026;

    (iii) that certain personal information was consulted by an unauthorized third party;

    (iv) that, as a precaution, they logged their customers out of their applications using PCid credentials;

    (v) that they reported the incident to the relevant privacy authorities and to law enforcement;

    (vi) that the Class Members must be cautious of unexpected emails, calls or text messages asking for personal information or inviting them to click on a link or download an attachment, and must monitor their accounts; and

    (vii) that they are offering 24 months of credit monitoring and identity restoration services through TransUnion's myTrueIdentity service.

49. By offering credit monitoring and identity restoration services and by warning the Class Members to be cautious of phishing and to monitor their accounts, Defendants admit that the Data Breach creates a real and current threat and risk of fraud, phishing and/or identity theft for the Class Members.

50. In the Notice, Defendants further state (in French): "Nous sommes désolés de l'inquiétude que cela pourrait susciter", as appears from Exhibit AP-9, thereby admitting that the Data Breach causes worry and concern to the Class Members.

51. The Notice is also deficient in that it does not clearly confirm what information was actually stolen. In the case of the Plaintiff, the Notice lists her name, email address, address, telephone number and "détails du bon de commande" (purchase order details), without explaining what such purchase order details include, namely whether they include her billing or shipping address, her payment card information, or the list of products she purchased.

52. Moreover, Defendants have failed to confirm that they would indemnify and hold the Class Members harmless of any losses or damages suffered as a result of the Data Breach.

53. Defendants, who required and collected the personal information of their customers in the context of their enterprise, 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.

54. Despite this obligation, Defendants failed to implement adequate cybersecurity and data protection measures, as confirmed notably by the means of access used by the threat actors and by the additional security enhancements only implemented after the Data Breach, as appears from Exhibit AP-4 (par. 14).

55. When a Data Breach affecting approximately two (2) million persons occurs, Defendants had the obligation to promptly and accurately notify the Class Members in order to help them prevent fraud, identity theft, financial losses, loss of time, stress and inconvenience.

56. Section 3.5 of the Act Respecting the Protection of Personal Information in the Private Sector requires an enterprise to promptly notify any person whose personal information is concerned by a confidentiality incident presenting a risk of serious injury, and section 10.1 of the Personal Information Protection and Electronic Documents Act (**PIPEDA**) requires notification as soon as feasible. Defendants failed to comply with these obligations.

57. Moreover, section 6 of the Regulation respecting confidentiality incidents provides that, where a public notice is given in order to act rapidly to reduce the risk of a serious injury, the enterprise "must still send a notice to the person concerned with proper diligence". A public advisory on a website in March 2026, followed by individual notices only as of October 19, 2026, does not meet this standard.

58. Similarly, subsection 10.1(5) of the Personal Information Protection and Electronic Documents Act (**PIPEDA**) requires that the notification be "conspicuous" and "given directly to the individual", and subsection 10.1(4) requires that it contain sufficient information to allow the individual to understand the significance of the breach to them, which the Notice failed to do as regards the undefined "détails du bon de commande".

59. Defendants are also hereby summoned to produce the entry concerning the Data Breach in their register of confidentiality incidents kept pursuant to section 3.8 of the

Act Respecting the Protection of Personal Information in the Private Sector, as well as the notice sent to the Commission d'accès à l'information pursuant to section 3 of the Regulation respecting confidentiality incidents, which must notably state the number of persons concerned who reside in Quebec.

60. Defendants are hereby summoned to confirm the date on which they notified the Commission d'accès à l'information du Québec of the Data Breach, and to produce a copy of said notice.

61. Defendants are hereby summoned to confirm whether they communicated with the unauthorized third parties who perpetrated the Data Breach, to confirm whether they paid any ransom or other sums, and to produce copies of the said communications and/or details of payments made into the Court record.

62. Immediate notice of a data breach is essential for the affected persons to obtain the best protection against fraud and identity theft. By letting 228 days pass after becoming aware of the Data Breach before starting to notify the affected Class Members, while publicly minimizing the scope of the Data Breach in the meantime, Defendants deprived the Class Members of the opportunity to protect themselves and exacerbated the damages sustained by them. These represents additional faults and negligence committed.

63. 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 Data Breach increases the likelihood of Class Members falling victim to phishing, fraud and identity theft.

64. The combination of a person's name, address, phone number, email address, date of birth, loyalty account number, purchase history and partial payment card information is precisely the type of information used by fraudsters to impersonate a trusted organization and conduct convincing phishing and social engineering attacks.

65. Class Members have been and/or will be exposed to phishing, fraud and/or identity theft, and have been harmed as a result.

66. Harm to victims of the Data Breach includes without limitation fraudulent charges on their accounts, disbursements incurred such as for purchasing extra insurance or credit monitoring, placing a fraud alert on their credit file, and loss of time and expenses related to finding fraudulent charges, cancelling and reissuing payment cards, monitoring their credit, and the general nuisance and annoyance of dealing with

all these issues resulting from the Data Breach.

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

68. In order to save money, Defendants chose to only offer a two (2) year period of credit monitoring and identity restoration services. This measure is manifestly insufficient given the gravity of the Data Breach, the permanent nature of certain of the information exposed (such as dates of birth), and the vast number of persons affected across Canada, and it transfers onto the Class Members the burden, cost and inconvenience of protecting themselves after the expiry of said period.

69. Moreover, Defendants only offered credit monitoring through TransUnion, and failed to also offer credit monitoring through Equifax Canada, the other major credit reporting agency in Canada. Since lenders and creditors may consult either credit bureau, monitoring a single credit file leaves the Class Members exposed to fraudulent credit applications reported only to Equifax Canada, unless they subscribe to such services at their own cost.

Prior Security Incidents

70. Moreover, the Data Breach is not the first security incident affecting Defendants' customers and their customer accounts.

71. In February 2017, accounts of members of Defendants' PC Plus loyalty program were accessed without authorization and points were stolen. Loblaw itself then stated: "In recent weeks, we have observed some unusual activity on select PC Plus accounts. Our investigation indicates that the PC Plus system has been the target of fraud, resulting in some members having their points stolen." Loblaw had to reset its members' usernames and passwords, the whole as more fully appears from copies of news articles reporting on the 2017 and 2018 security incidents affecting Defendants' customer accounts, communicated herewith, *en liasse*, as **Exhibit AP-10**.

72. In July 2017, Loblaw notified users of its websites, including loblaws.ca, joefresh.com and beautyboutique.ca, as follows: "On behalf of Loblaw Companies Limited, we are writing to inform you of recent unauthorized online activity, which may have impacted a small number of user accounts on our websites". This was the second security

incident affecting Defendants' customers that year, as appears from Exhibit AP-10.

73. In March and April 2018, shortly after Defendants merged their PC Plus and Shoppers Optimum programs into the PC Optimum program, the accounts of numerous PC Optimum members across Canada were accessed without authorization and millions of points were stolen. The stolen points were redeemed, among other places, at Defendants' Pharmaprix stores in Laval and Montreal and at a Maxi & Cie store in Montreal, in the Province of Quebec, as appears from Exhibit AP-10.

74. Points continued to be stolen from certain members even after they had changed their passwords as Loblaw recommended. Loblaw admitted the cause: "As part of our password reset process, devices—like a mobile phone—attached using the original account password may have continued to have access to points", as appears from Exhibit AP-10.

75. At the time, Loblaw publicly represented that "We have strong security measures in place across our digital platforms" and that "The PC Optimum program is more secure than either of our legacy programs", as appears from Exhibit AP-10.

76. Defendants were therefore aware, since at least 2017, of the vulnerability of their customer accounts and login credentials. Nevertheless, in February 2026, threat actors once again gained access to Defendants' systems, this time by leveraging compromised credentials for a quality assurance platform, and accessed the personal information of approximately two million Canadians (Exhibit AP-4, par. 10).

77. Defendants are hereby summoned to disclose and produce all incident reports, notices and findings regarding any security or confidentiality incident affecting their customers' personal information or accounts since January 1, 2017.

The March 2026 OPC Findings Against Loblaw

78. Furthermore, on March 5, 2026, only five (5) days before announcing the Data Breach, the OPC published its PIPEDA Findings #2026-001 following an investigation into the personal information retention practices of Loblaw for the PC Optimum program, the whole as more fully appears from a copy of the OPC's PIPEDA Findings #2026-001 dated March 5, 2026, communicated herewith as **Exhibit AP-11**.

79. The OPC notes therein that the PC Optimum program, which has more than 17 million members across Canada, is operated by President's Choice Services Inc., a subsidiary of Loblaws Inc., as appears from Exhibit AP-11.

80. The OPC concluded that “since it took Loblaw an unreasonable amount of time to address these deletion requests and the company failed to respond to some privacy-related inquiries, we conclude that Loblaw contravened principle 4.10 of PIPEDA”, as appears from Exhibit AP-11.

81. The OPC further found that, upon the closure of a PC Optimum account, Loblaw deletes certain personal identifiers “while retaining most other information, including purchase transaction data”, and that “Loblaw did not demonstrate during our investigation that it was or is taking sufficient steps to ensure that information is properly anonymized”, as appears from Exhibit AP-11.

82. Defendants’ retention of their customers’ purchase transaction data beyond what is necessary represents a further fault, which increased the quantity of personal information exposed in the Data Breach, including the purchase order details of the Plaintiff and the Class Members. Defendants are hereby summoned to confirm whether the personal information of former PC Optimum members, including those who had closed their accounts, was affected by the Data Breach.

83. 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 Defendants and subsequently lost by Defendants as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which make Defendants liable to pay compensatory, moral and punitive damages:

(a) Sections 3, 35, 36, 37, 1457, 1458, 1526 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, CQLR, c. C-12;

(c) Sections 1, 2, 3.1 and following (including sections 3.5 and 3.8), 10, 13, 17 and 93.1 of the Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c. P-39.1;

(d) Sections 3, 5 and 6 of the Regulation respecting confidentiality incidents, CQLR, c. A-2.1, r. 3.1;

(e) Sections 2, 3, 5, 10.1, 10.3 and 11 of the Personal Information Protection and Electronic Documents Act, SC 2000, c. 5, as well as sections

4.1, 4.3, 4.4 and 4.7 of its Schedule 1;

(f) Sections 3, 4 and 5 of the Breach of Security Safeguards Regulations, SOR/2018-64;

(g) Sections 1, 2, 8 to 12, 16, 17, 40 to 42, 215 to 228, 253 and 261 to 272 of the Consumer Protection Act, CQLR, c. P-40.1;

FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF

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

85. Plaintiff is a customer of Defendants and has placed multiple orders with Defendants either online for deliver or for curbside pick up (aside from in store purchases). She has not retained any proof of orders or purchases.

86. It is in this context that Defendants collected and held her personal information, including purchase order details.

87. On October 29, 2026, Plaintiff received the Notice by email, namely 248 days after the Data Breach began and 238 days after Defendants became aware of it, as appears from Exhibit AP-9.

88. Plaintiff never received any prior email or other communication from Defendants regarding the Data Breach, and did not know of the Data Breach, before receiving the Notice on October 29, 2026.

89. The Notice therefore informed Plaintiff for the very first time that Defendants had permitted an unauthorized third party to access her personal information, 248 days after the Data Breach began.

90. The Notice did not explain what the "détails du bon de commande" concerning her actually included, leaving Plaintiff unable to know whether her payment card information or her purchase history were also in the hands of criminals.

91. Upon receiving the Notice, Plaintiff became nervous, anxious, stressed and worried about the loss of her personal information, about what precisely had been stolen, and about the risk of becoming a victim of phishing, fraud and/or identity theft.

92. On October 30, 2026, Plaintiff proceeded to sign up for the TransUnion myTrueIdentity credit monitoring and identity restoration services offered in the Notice, using the activation code provided therein, the whole as more fully appears from a copy of the confirmation email from TransUnion confirming Plaintiff's enrollment in the myTrueIdentity service, communicated herewith as **Exhibit AP-12**.

93. However, as mentioned above, Defendants did not offer Plaintiff any credit monitoring with Equifax Canada, the other major credit reporting agency in Canada. This means that Defendants wanted Plaintiff's Equifax Canada credit file to remain unmonitored unless she subscribes to such services at her own cost (i.e. Defendants wanting to save their own money by refusing to pay for this Equifax Canada protection as well for Plaintiff and other Class Members, representing a further fault committed).

94. Accordingly, on October 30, 2026, Plaintiff had no other choice but to call Equifax Canada herself to inform them about the Data Breach herein. Plaintiff was verbally recommended by the agent to subscribe to the Equifax Complete Premier protection plan in order to protect herself, which Plaintiff indeed did at a cost of $24.95 plus taxes ($28.69) per month, with auto-renews each month (at whatever the current rate will be) and charges on her credit card, which amounts she paid and will continue to pay and which she claims from Defendants solidarily herein, the whole as more fully appears from the October 30, 2026 Equifax Canada confirmation email, communicated herewith as **Exhibit AP-13**.

95. Plaintiff spent and lost time reading the Notice, enrolling in said services, and monitoring her accounts and communications, and will have to continue doing so going forward.

96. Plaintiff must now be even more vigilant than usual regarding any email, call or text message she receives, given the risk of phishing and social engineering created by the Data Breach, as admitted by Defendants in the Notice.

97. As alleged above, Defendants should have offered credit monitoring services and insurance coverage to the Plaintiff and the Class Members for more than two (2) years, but they refused or neglected to do so in order to save money, therefore transferring the burden, cost, loss of time and inconvenience onto the Plaintiff and the Class Members. Plaintiff will be forced to renew said services at her own cost as well to protect herself.

98. Plaintiff, in good faith, was reasonably justified in assuming that Defendants, part of

Canada's largest retail group, would properly safeguard her personal information, which Defendants clearly did not.

99. As a result of learning that her personal information was lost by Defendants, Plaintiff experienced and continues to experience anxiety, stress, worry, nervousness, inconvenience, loss of time and fear.

100. Defendants had the obligation to ensure, by the most technologically sophisticated means possible and available, that said personal information was protected and could not be accessed. Defendants failed in this regard, and their negligence and carelessness facilitated the Data Breach, making Defendants liable to pay compensatory, moral and punitive damages.

Punitive Damages

101. 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 Defendants were grossly and/or intentionally negligent and are liable to pay punitive damages to the Class Members.

102. In fact, without limiting the generality of the foregoing, Defendants were grossly negligent and/or intentionally negligent when they:

(a) failed to follow or properly implement an effective data security industry standard to protect the Class Members' personal information, which they allowed to be accessed through compromised credentials for a quality assurance platform;

(b) failed to timely detect the Data Breach;

(c) publicly minimized the Data Breach as "low-level" and limited to "basic customer information", and reassured their customers that their accounts were "secure", when the Data Breach in fact affected approximately two (2) million Canadians and included dates of birth, addresses, loyalty account numbers, purchase order details and partial payment card information;

(d) only updated their public advisory 206 days later, and only following a request from the OPC;

(e) waited 228 days after becoming aware of the Data Breach before starting to notify the affected Class Members;

(f) failed to clearly inform the Class Members of what information concerning them was actually stolen;

(g) failed to adequately encrypt and protect the Class Members' personal information;

(h) offered only two (2) years of credit monitoring, through TransUnion only and not through Equifax Canada;

(i) failed to offer indemnification for losses suffered by Class Members;

(j) committed all of the above notwithstanding the prior security incidents of 2017 and 2018 affecting their customers' accounts, which put them on notice of the vulnerability of their customer accounts and login credentials (Exhibit AP-10); and

(k) retained their customers' purchase transaction data beyond what was necessary, as found by the OPC only days before the Data Breach was announced (Exhibit AP-11).

103. Considering the above and considering the fact that Defendants have violated various laws which have been enacted in order to protect the Class Members' personal information, Defendants are liable to pay at least $1,000 (*à parfaire*) to each Class Member in punitive damages, aside from any other compensatory and moral damages suffered by the Class Members.

104. Indeed, Plaintiff invokes and relies upon section 93.1 of the Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c. P-39.1, which provides for the minimum award of punitive damages in this particular situation (in favour of Plaintiff and each Class Member): "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."

105. Plaintiff also invokes section 49 of the Charter of Human Rights and Freedoms, which provides for punitive damages in case of unlawful and intentional interference with the right to respect for private life protected by section 5 of the Charter, as well as Article 1621 of the Civil Code of Quebec.

106. Defendants' above detailed actions qualify the fault as intentional, being the 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 their actions would cause to the Class Members.

107. Defendants' negligence has shown a malicious, oppressive and high-handed conduct that represents a marked departure from ordinary standards of decency. Punitive damages of at least $1,000 (*à parfaire*) should therefore be awarded to each Class Member.

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

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

109. Class Members had their personal information lost by Defendants as described hereinabove, and/or received a notice from Defendants.

110. Class Members have or will experience stress, anxiety, worry, inconvenience, loss of time and/or fear due to the loss of their personal information and/or the receipt of the notice, as admitted by Defendants in the Notice.

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

112. 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 services, posting an alert on their accounts or credit files, changing their personal information or account numbers, cancelling and replacing payment cards, closing and opening accounts, etc.

113. Furthermore, Class Members may be required to pay costs or fees in order to sign up for or renew credit monitoring (including with Equifax Canada), to post an alert on their accounts or credit files, to purchase insurance, or in order to otherwise protect themselves from further fraud exposure.

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

115. Moreover, it is likely that many Class Members have not yet been notified, or will never be notified, of the loss of their information (for example due to a change of address or email address, or emails filtered as spam), making them still at great risk of fraud or identity theft.

116. Every Class Member can still fall victim to fraud or identity theft in the future, due to Defendants' negligence in the safekeeping of their personal information and in the way they handled themselves after being made aware of the Data Breach.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

117. 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.

118. Loblaw has confirmed that the Data Breach affected approximately two (2) million Canadians, as appears from Exhibit AP-4 (par. 10). Defendants are hereby summoned to confirm the total number of affected Class Members in Canada in general, and in Quebec particularly.

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

120. 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 Defendants. 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 Defendants' conduct would increase delay and expense to all parties and to the Court system;

121. 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;

122. 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;

123. 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;

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

125. 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 Defendants commit faults regarding the storage and the safe-keeping of the personal information of the Class Members?

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

(c) Did Defendants commit faults by minimizing the scope and gravity of the Data Breach in their public communications?

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

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

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

128. 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 Defendants;

CONDEMN Defendants solidarily to pay to the Class Members compensatory damages for all monetary losses and moral damages caused

as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendants solidarily to pay not less than $1,000, *sauf à parfaire*, to each Class Member 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;

129. 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) Defendants conduct business online and in physical stores in Quebec and the same way across Canada;

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

130. Plaintiff respectfully submits that this Honourable Court has jurisdiction over a national class action herein since:

(a) Loblaws Inc. has its principal establishment and its elected domicile in Montreal, more than 5,000 employees in Quebec and numerous establishments throughout Quebec, and Loblaw, its majority shareholder and ultimate beneficiary, has its fondé de pouvoir in Montreal and carries on its activities in Quebec, notably through Loblaws Inc. and its Provigo, Maxi and Pharmaprix banners, as appears from Exhibits AP-1, AP-2 and AP-3;

(b) Plaintiff resides and is domiciled in the Province of Quebec, and Defendants collected and held her personal information in the context of her relationship with Defendants as their customer in Quebec;

(c) Defendants sent the Notice to Plaintiff in Quebec, and Plaintiff suffered her damages in Quebec;

(d) Defendants collect, use and store the personal information of their customers, including PC Optimum members, in the same manner across Canada, and the Data Breach affected Class Members across Canada in the same manner, as appears from Exhibits AP-4 and AP-6;

(e) The law applicable to the Class Members residing outside Quebec is substantially similar to Quebec law for the purposes of the present action: the Personal Information Protection and Electronic Documents Act (**PIPEDA**) applies across Canada to the personal information collected by Defendants in the course of their commercial activities and imposes the same safeguarding and breach notification obligations, Alberta and British Columbia have private-sector privacy legislation recognized as substantially similar, the common law of the other provinces likewise sanctions the failure to safeguard personal information in contract and in negligence, and the applicable limitation periods are comparable; any differences can be managed through the identification of sub-groups at the merits stage;

(f) Accordingly, Article 3148 C.C.Q. is fulfilled, namely paragraph 2 thereof (Defendants have establishments and carry on activities in Quebec, and the dispute relates to their activities in Quebec) and paragraph 3 thereof (damage was suffered in Quebec), and nothing prevents a national group herein;

131. 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 Defendants as described hereinabove;

(b) She has already and will continue to suffer anxiety, inconvenience, stress, loss of time, and fear as a result of the facts described hereinabove;

(c) She may in the future suffer further harm as a result of Defendants' conduct described hereinabove;

(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;

132. 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:

Class: All persons in Canada whose personal and/or financial information was held by Defendants and was accessed, compromised or stolen in the Data Breach which occurred between on or about February 23, 2026 and on or about March 5, 2026, or who received an email or letter from Defendants informing them of such Data Breach; or any other Group(s) or Sub-Group(s) to be determined by the Court.	**Groupe:** Toutes les personnes au Canada dont les renseignements personnels et/ou financiers étaient détenus par les Défenderesses et ont été consultés, compromis ou volés lors de la Fuite de données survenue entre le ou vers le 23 février 2026 et le ou vers le 5 mars 2026, ou qui ont reçu un courriel ou une lettre des Défenderesses les informant de cette Fuite de données; ou tout autre groupe ou sous-groupe à déterminer par le Tribunal.

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

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

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

(c) Did Defendants commit faults by minimizing the scope and gravity of the Data Breach in their public communications?

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

(e) Are Defendants 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 Defendants;

CONDEMN Defendants solidarily to pay to the Class Members compensatory damages for all monetary losses and moral damages caused as a result of Defendants' loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendants solidarily to pay not less than $1,000, *sauf à parfaire*, to each Class Member 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 Honourable Court;

ORDER that said notice be posted and available on the home page of Defendants' various websites, Facebook account(s), Instagram account(s) and X (formerly

Twitter) account(s), and **ORDER** Defendants to send the notice by email with proof of receipt and by direct mail to all Class Members;

ORDER Defendants 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 30, 2026

(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.

Exhibits supporting the application

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

Exhibit AP-1: Extracts of Loblaw's website ("Who we are");

Exhibit AP-2: Extract from the Registraire des entreprises concerning Loblaw Companies Limited / Les Compagnies Loblaw Limitée;

Exhibit AP-3: Extract from the Registraire des entreprises concerning Loblaws Inc.;

Exhibit AP-4: Compliance Letter signed by Loblaw on October 21, 2026 and published by the OPC;

Exhibit AP-5: Press release issued by Loblaw on March 10, 2026;

Exhibit AP-6: Public advisory entitled "Important information about your account" published by Loblaw on its website on March 10, 2026 and updated on October 2, 2026;

Exhibit AP-7: News articles reporting on the Data Breach, *en liasse*;

Exhibit AP-8: News release published by the OPC on October 26, 2026;

Exhibit AP-9: Notice dated October 29, 2026 sent to Plaintiff (activation code redacted);

Exhibit AP-10: News articles reporting on the 2017 and 2018 security incidents, *en liasse*;

Exhibit AP-11: Office of the Privacy Commissioner of Canada, PIPEDA Findings #2026-001, “Investigation into the personal information retention practices of Loblaw for the PC Optimum Loyalty Program” (March 5, 2026);

Exhibit AP-12: Confirmation email from TransUnion confirming Plaintiff's enrollment in the myTrueIdentity service (October 30, 2026);

Exhibit AP-13: October 30, 2026 Equifax Canada Confirmation email to Plaintiff;

These exhibits are available on request.

Defendants' 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.

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 30, 2026

(s) Lex Group Inc.

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

NOTICE OF PRESENTATION

(Article 108 of the Directives of the Superior Court, Division of Montreal)

TO:

LOBLAW COMPANIES LIMITED / LES COMPAGNIES LOBLAW LIMITÉE
800-22 St. Clair Avenue East
Toronto, Ontario M4T 2S5

fondé de pouvoir in Quebec:
Borden Ladner Gervais LLP
900-1000 De La Gauchetière Street West
Montreal, Quebec H3B 5H4

-and-

LOBLAWS INC.
800-22 St. Clair Avenue East
Toronto, Ontario M4T 2S5

elected domicile in Quebec:
10-400 Sainte-Croix Avenue
Montreal, Quebec H4N 3L4

Defendants

TAKE NOTICE that APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION will be presented before the Superior Court at the Montreal Courthouse, located at 1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6, on a date to be determined by the coordinating Judge of the Class Action Division.

MONTREAL, October 30, 2026

(s) Lex Group Inc.

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

500-06-000083-267

CLASS ACTIONS DIVISION
SUPERIOR COURT
PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

J[redacted]G[redacted]

Plaintiff

vs.

LOBLAW COMPANIES LIMITED / LES COMPAGNIES LOBLAW LIMITÉE

-and-

LOBLAWS INC.

Defendants

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