CANADA
PROVINCE OF QUÉBEC
DISTRICT OF MONTRÉAL
N°500-06-000002-267

CLASS ACTION
SUPERIOR COURT

SOLOMON ABUDARHAM

Applicant

v.

EQUIFAX CANADA CO., a legal person duly incorporated under the *Companies Act*, R.S.N.S. 1989, c. 81 (Nova Scotia), having its place of business at 5700 Yonge Street, Toronto, Ontario, M2M 4K2, Canada.

EQUIFAX INC., a legal person duly incorporated under the laws of the State of Georgia, having its head office at 1550 Peachtree Street NW, Atlanta, Georgia, 30309, United States, and whose registered agent is Corporation Service Company, located at 2 Sun Court, Suite 400, Peachtree Corners, Georgia, 30092, United States.

Defendants

APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION AND FOR APPOINTMENT AS CLASS REPRESENTATIVE
(Articles 574 et seq. C.C.P.)

TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT SITTING IN AND FOR THE DISTRICT OF MONTRÉAL, THE APPLICANT STATES AS FOLLOWS:

I. THE CLASS ACTION

1. The Applicant seeks authorization to institute a class action on behalf of:

   All natural persons residing in Canada whose Equifax credit file shows one or more access entries or inquiries generated through an Equifax third-party partner platform since at least May 20, 2024, and who did not consent to the registration or opening of the relevant partner account that gave rise to such unauthorized access, or any other class the Court may deem appropriate to define.

2. Borrowell, KOHO, Credit Karma, and Mogo offer in Canada various technology-based financial services, including credit monitoring, credit-building or credit-improvement

tools, financial product comparisons, consumer lending, or the management of digital payment accounts. They are partner third-party platforms of Equifax, as appears from **Exhibit P-1.**

3. All these platforms rely on comparable matching, validation, and transmission mechanisms, which are operated and controlled exclusively by Equifax.

4. These entities are not credit assessment agencies within the meaning of the laws in force in Canada and do not have any independent authority to create, maintain, or disclose credit files. The creation and retention of credit files fall exclusively within the jurisdiction of duly recognized credit assessment agencies, including Equifax, which compile information provided by authorized data furnishers, as appears from **Exhibit P-2.**

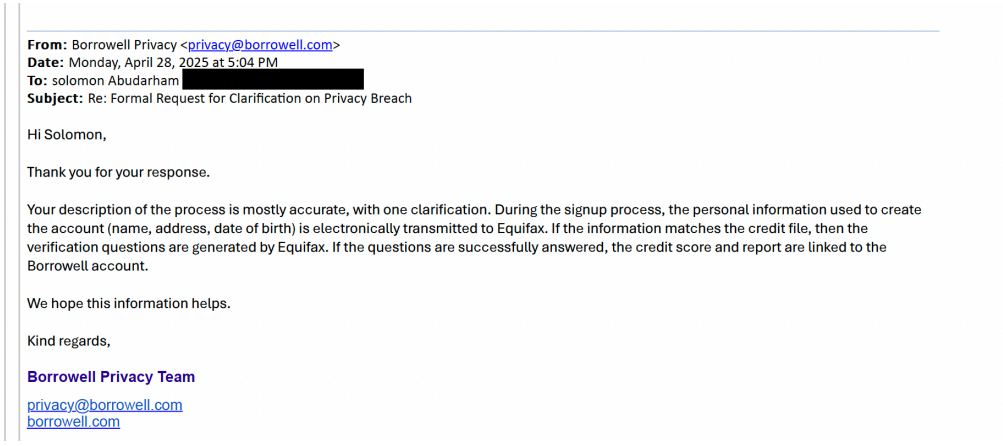
5. The present application arises from the Applicant's discovery that his credit file, which Equifax holds, administers, and controls, was the subject of multiple and repeated accesses without his authorization, through a platform, namely Borrowell Inc., over an extended period, while he was completely unaware of the existence of such access and had not consented to the disclosure of his personal information to any third party.

6. The Applicant has never opened an account with Borrowell, nor authorized the opening of such an account or the accessing of his credit file by that platform. However, it has been established that an unauthorized third party was able to fraudulently create an account in his name and, by this means, access his entire credit file and his personal information.

7. Borrowell offers a financial services platform that provides its users access to their credit score, relying on Equifax systems to supply this information. Opening an account on this platform requires the disclosure of basic personal information, which triggers the automated sending of a request to Equifax to obtain the corresponding credit file.

8. The validation, matching, and authentication mechanism implemented following this request is designed and administered in accordance with parameters determined by Equifax, which sets the matching rules, oversees the generation of authentication questions, and decides whether to disclose the credit file. Borrowell is limited to the technical initiation of the request and has no independent decision-making authority regarding the validity of the match or the scope of the information transmitted.

9. This transmission and authentication mechanism is described in the correspondence between the Applicant and Borrowell, an excerpt of which is reproduced below. The full correspondence is available in **Exhibit P-3**.



From: Borrowell Privacy <privacy@borrowell.com>
Date: Monday, April 28, 2025 at 5:04 PM
To: solomon Abudarham [redacted]
Subject: Re: Formal Request for Clarification on Privacy Breach

Hi Solomon,

Thank you for your response.

Your description of the process is mostly accurate, with one clarification. During the signup process, the personal information used to create the account (name, address, date of birth) is electronically transmitted to Equifax. If the information matches the credit file, then the verification questions are generated by Equifax. If the questions are successfully answered, the credit score and report are linked to the Borrowell account.

We hope this information helps.

Kind regards,

Borrowell Privacy Team

privacy@borrowell.com
borrowell.com

10. In the present case, following the opening of a fraudulent account on the Borrowell platform, the Applicant's entire credit file was disclosed to an unauthorized third party as a result of an authentication process based on partial, inaccurate, or outdated personal information, without enhanced identity verification, without validation of the true file holder's consent, and without any effective mechanism to detect inconsistencies between the information submitted and the data contained in the file.

11. Although, in the Applicant's particular case, the unauthorized access was identified only through Borrowell, Equifax applies in Canada this same access model through a computer interface with a significant number of third-party partner platforms, including notably Borrowell Inc., KOHO Financial Inc., Credit Karma Canada, Mogo Inc., Chexy, and other similar services.

12. In support of this Application, the Applicant alleges that the Defendants Equifax Canada Co. and Equifax Inc. are solidarily liable toward all Class Members as a result of wrongful breaches arising from their exclusive role as holders, custodians, and operators of the systems enabling access to, authentication, matching, and disclosure of credit files to their partners, in particular in that they:

    i) Allowed credit files to be accessible, consulted, and disclosed following requests initiated by third-party platforms to malicious individuals, without ensuring the implementation of a robust monitoring system;

    ii) Authorized the disclosure of highly sensitive personal and financial information through automated matching and validation processes relying on partial, inaccurate, or outdated information, without sufficient mechanisms to prevent identification errors or identity theft;

    iii) Failed to implement and maintain adequate technical, organizational, and administrative security measures proportionate to the sensitivity of the information contained in credit files;

iv) Tolerated repeated and prolonged access to credit files, without the knowledge of the affected file holders, and without effective monitoring, alerting, anomaly detection, or timely corrective intervention mechanisms;

v) Failed to meet their general duty of prudence, diligence, and protection of the personal information of the individuals concerned;

vi) Infringed the fundamental right of the Class Members to respect for their privacy and to the protection of their personal information.

13. Equifax acts as the exclusive custodian of credit files in its capacity as a credit assessment agent governed by the *Credit Assessment Agents Act*, CQLR, c. A-8.2 ("**CAAA"**), and regulated by the Autorité des marchés financiers in Québec, while also being subject, across Canada, to the obligations set out in the *Personal Information Protection and Electronic Documents Act*.

14. The applicable legislation includes the *Charter of Human Rights and Freedoms*, CQLR, c. C-12 ("**Charter**"), the *Civil Code of Québec*, CQLR, c. CCQ-1991 ("**C.c.Q**."), the *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1 ("**ARPIPS**"), as well as the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("**PIPEDA**"), the latter applying federally and to interprovincial commercial activities.

15. In addition, depending on the province of residence of the Class Members, provincial privacy legislation applies, including the *Privacy Act*, R.S.B.C. 1996, c. 373, applicable in British Columbia ("**BC Privacy Act**"); the *Privacy Act*, C.C.S.M., c. P125, applicable in Manitoba ("**Manitoba Privacy Act**"); the *Privacy Act*, R.S.S. 1978, c. P-24, applicable in Saskatchewan ("**Saskatchewan Privacy Act**"); the *Privacy Act*, R.S.N.L. 1990, c. P-22, applicable in Newfoundland and Labrador ("**NL Privacy Act**"); as well as the *Personal Information Protection Act*, S.A. 2003, c. P-6.5, applicable in Alberta ("**Alberta PIPA**").

II. DEFINITIONS AND OPERATIONS

16. For the purposes of this Application, the following terms are defined as follows.

17. An "**Application Programming Interface**" (API) refers to any computer mechanism controlled by Equifax that enables authorized third-party platforms to transmit automated requests for the purpose of consulting or disclosing credit files, with Equifax remaining responsible for processing, validating, and responding to such requests in accordance with its security and authentication parameters. The operation of the APIs is described in **Exhibit P-4**.

18. The "**matching mechanism**" refers to any process used by Equifax to establish a correspondence between the personal information submitted in a request and an existing credit file, whereas the "**matching operation**" or "**matching**" corresponds to

the step whereby Equifax assesses, according to its internal criteria, the degree of concordance between the data transmitted and the data contained in its databases, this assessment determining whether access is authorized or refused.

19. The "**partner third-party platform**" refers to any entity authorized by Equifax to use such APIs to submit automated requests, without control over credit databases or over decisions relating to the disclosure of files.

20. Equifax offers a suite of APIs intended for businesses that wish to provide their clients with direct access to their own credit information through a "**consumer-facing**" platform. Specifically, the partner's platform integrates these APIs and, as needed, sends requests to Equifax to obtain information such as scores, credit reports, summaries, and, depending on the product, monitoring with alerts.

21. Before actual access to the products, there is a consumer enrollment stage ("**Consumer Enrollment**") and an access management stage, during which the partner administers the client's rights to the Consumer Engagement Suite services. Once the consumer is enrolled and access is authorized, the partner's platform sends an API request to Equifax to retrieve the requested credit information and display it to the client within the partner's interface, as appears from **Exhibit P-5**.

22. For the returned data to correspond to the correct person, Equifax describes an "**Identity Matching**" mechanism based on a proprietary algorithm, used to identify and link the client's information in real time, even in the presence of variations (for example, changes of name or address). This service assigns persistent identifiers, including a "**consumer key**," as appears from **Exhibit P-6 (bundle)** (and, as needed, household and address keys), to maintain a consistent consumer view and avoid duplicates.

23. Where the monitoring product is used, the service is not limited to providing a report or score on demand. It also allows the file to be monitored and generates alerts when a "key" change is detected, to notify the consumer through the partner's platform, as appears from **Exhibit P-7.**

24. Finally, in the specific case of Borrowell, it is indicated that the score provided originates from Equifax and corresponds to the Equifax Risk Score 2.0 (ERS 2.0), purchased by Borrowell from Equifax, as appears from **Exhibit P-8**.

III. THE DEFENDANTS

25. Equifax Canada Co. and Equifax Inc., hereinafter collectively referred to as "Equifax," are credit assessment agencies that collect, retain, and disclose financial information concerning Canadian consumers across the country.

26. The Defendant Equifax Canada Co. is a legal person duly incorporated under the *Companies Act*, R.S.N.S. 1989, c. 81 (Nova Scotia), whose principal place of business

is located at 5700 Yonge Street, Toronto (Ontario), M2M 4K2, Canada, as appears from **Exhibit P-9**.

27. Equifax Canada Co. also operates a place of business in Montréal, as appears from the statement of information of a legal person registered with the enterprise register.

28. The Defendant Equifax Inc. is a legal person incorporated under the laws of the State of Georgia, whose head office is located at 1550 Peachtree Street NW, Atlanta, Georgia, 30309, United States, as appears from **Exhibit P-10**.

29. During their activities, the Defendants collect credit files from financial institutions, acting as a data hub. They then disclose certain information from those files to third-party platforms, such as Borrowell Inc., in particular through Equifax's Consumer Engagement Suite, which is a suite of APIs intended for businesses that provide their clients with direct access to their "personal credit reports and scores."

30. The partnership announced on June 28, 2022 between Equifax Canada and Borrowell Inc. forms part of Equifax's cloud transformation and is intended to enable, through Equifax's APIs, real-time access to credit file information in order to provide Borrowell members with credit scores and credit reports, as appears from **Exhibit P-11**.

IV. THE SITUATION

31. A breach of the confidentiality of the Applicant's personal information occurred between May 20, 2024 and September 16, 2024, during which, on more than nineteen occasions, personal and financial information belonging to him was accessed, communicated, and disclosed without authorization through a Borrowell account, a third-party partner platform of Equifax, as appears in detail from **Exhibit P-12** and from the excerpt reproduced below.

EQUIFAX Dossier De Crédit Date De La Demande 2025/01/14

Interrogations

Un registre des accès à votre dossier de crédit est créé à l'aide d'interrogations publiées dans votre dossier de crédit. Une interrogation inclura le nom de l'entité qui a accédé à votre dossier de crédit et un numéro de téléphone que vous pourrez composer si vous avez des questions à propos de cet accès. Deux types d'interrogations peuvent apparaître dans votre dossier de crédit; les interrogations inscrites et les non-inscrites. Les interrogations non-inscrites sont visibles que par vous et elles n'ont aucun impact sur vos pointages de crédit. Les interrogations inscrites sont visibles pour tout destinataire autorisé à consulter votre dossier de crédit et elles peuvent entraîner des répercussions sur vos pointages de crédit.

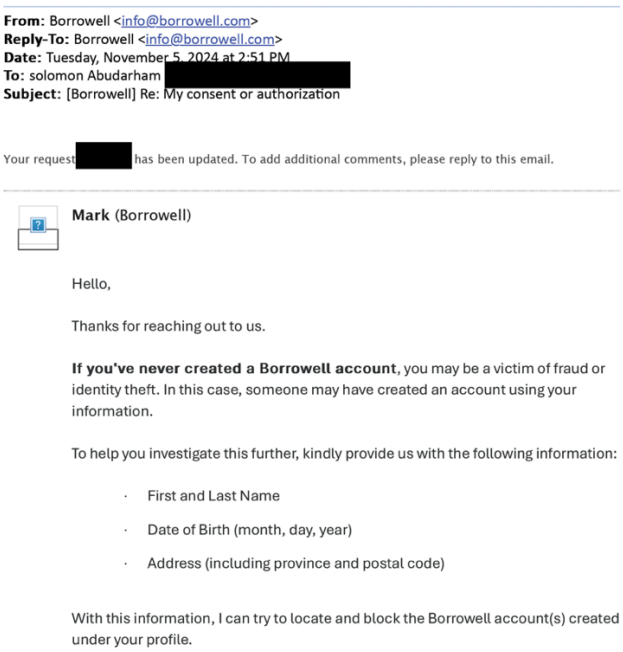
DATE	NUMÉRO DE MEMBRE	NOM DU MEMBRE	NUMÉRO DE TÉLÉPHONE	INCIDENCE SUR LES POINTAGES
2024/10/30	400AA00163	EQUIFAX PERSONAL SOL	800-871-3250	Non
2024/09/23	651ZC00014	EQUIFAX FILE CHECK	800-871-3250	Non
2024/09/16	481FZ50866	BORROWELL	888-285-0990	Non
2024/09/09	481FZ50866	BORROWELL	888-285-0990	Non
2024/09/02	481FZ50866	BORROWELL	888-285-0990	Non
2024/08/26	481FZ50866	BORROWELL	888-285-0990	Non
2024/08/19	481FZ50866	BORROWELL	888-285-0990	Non
2024/08/12	481FZ50866	BORROWELL	888-285-0990	Non
2024/08/05	481FZ50866	BORROWELL	888-285-0990	Non
2024/07/29	481FZ50866	BORROWELL	888-285-0990	Non
2024/07/22	481FZ50866	BORROWELL	888-285-0990	Non
2024/07/15	481FZ50866	BORROWELL	888-285-0990	Non
2024/07/08	481FZ50866	BORROWELL	888-285-0990	Non
2024/07/01	481FZ50866	BORROWELL	888-285-0990	Non
2024/06/24	481FZ50866	BORROWELL	888-285-0990	Non
2024/06/17	481FZ50866	BORROWELL	888-285-0990	Non
2024/06/10	481FZ50866	BORROWELL	888-285-0990	Non
2024/06/03	481FZ50866	BORROWELL	888-285-0990	Non
2024/05/27	481FZ50866	BORROWELL	888-285-0990	Non
2024/05/20	484FZ00279	BORROWELL		Non
2024/05/20	481FZ50330	BORROWELL INC.	888-285-0990	Non

32. Out of curiosity, the Applicant consulted the "inquiries" section of his Equifax account, to which he had logged in. To his surprise, he discovered that a member of Borrowell Inc. had accessed his account.

33. The Applicant has never opened an account with Borrowell, has never used the services offered by that platform, has never consented to that platform's access to his credit file, and has never authorized the disclosure of his personal information to Borrowell or to any third party acting on its behalf.

34. On November 5, 2024, the Applicant contacted Borrowell in order to obtain explanations regarding the repeated extractions of his credit report, which he had discovered despite never having created an account or provided express authorization.

35. Borrowell then informed him that a third party may have opened an account using his personal information and asked him to provide certain information through a secure portal, for the purpose of identifying and blocking any fraudulent account, as appears from Exhibit P-3 (bundle).



From: Borrowell <info@borrowell.com>
Reply-To: Borrowell <info@borrowell.com>
Date: Tuesday, November 5, 2024 at 2:51 PM
To: solomon Abudarham [redacted]
Subject: [Borrowell] Re: My consent or authorization

Your request [redacted] has been updated. To add additional comments, please reply to this email.

Mark (Borrowell)

Hello,

Thanks for reaching out to us.

If you've never created a Borrowell account, you may be a victim of fraud or identity theft. In this case, someone may have created an account using your information.

To help you investigate this further, kindly provide us with the following information:

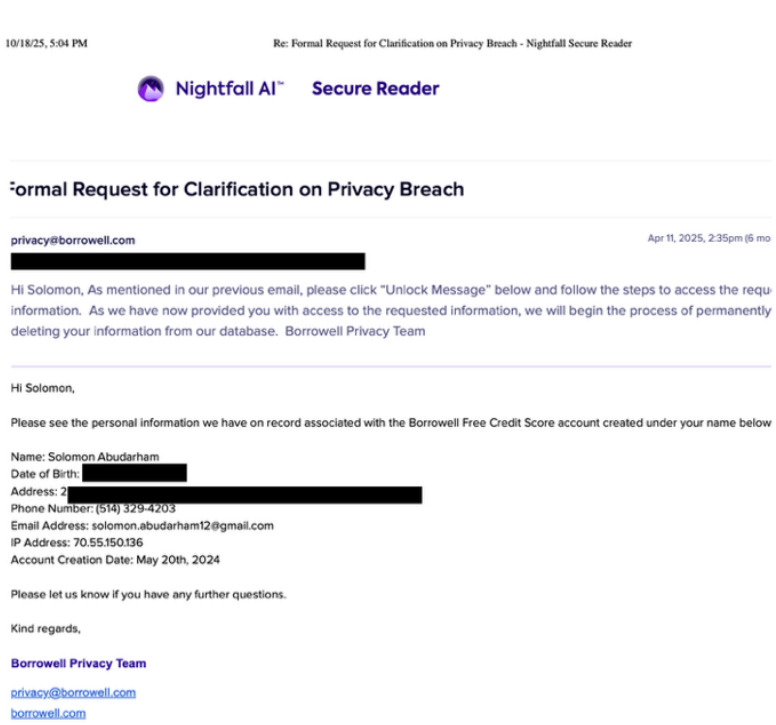
- First and Last Name
- Date of Birth (month, day, year)
- Address (including province and postal code)

With this information, I can try to locate and block the Borrowell account(s) created under your profile.

36. On April 11, 2025, Borrowell provided the Applicant, through the Nightfall secure portal, with all of the personal information associated with the Borrowell account that had been fraudulently created in his name.

37. This account, created on May 20, 2024, included in particular the name “Solomon Abudarham,” a date of birth listed as [redacted] an address located at [redacted] corresponding to a former address dating back more than 25 years, a telephone number that did not belong to the Applicant, and an email address different from his own.

38. The information provided by Borrowell shows that access to the credit file was authorized based on inaccurate and outdated data. These matches are available in their entirety in Exhibit P-3 (bundle). The correspondence includes the following excerpt, which illustrates the information provided by Borrowell and the data used to enable access:



10/18/25, 5:04 PM Re: Formal Request for Clarification on Privacy Breach - Nightfall Secure Reader

Nightfall AI™ Secure Reader

Formal Request for Clarification on Privacy Breach

privacy@borrowell.com Apr 11, 2025, 2:35pm (6 mo

[redacted]

Hi Solomon, As mentioned in our previous email, please click "Unlock Message" below and follow the steps to access the requ information. As we have now provided you with access to the requested information, we will begin the process of permanently deleting your information from our database. Borrowell Privacy Team

Hi Solomon,

Please see the personal information we have on record associated with the Borrowell Free Credit Score account created under your name below

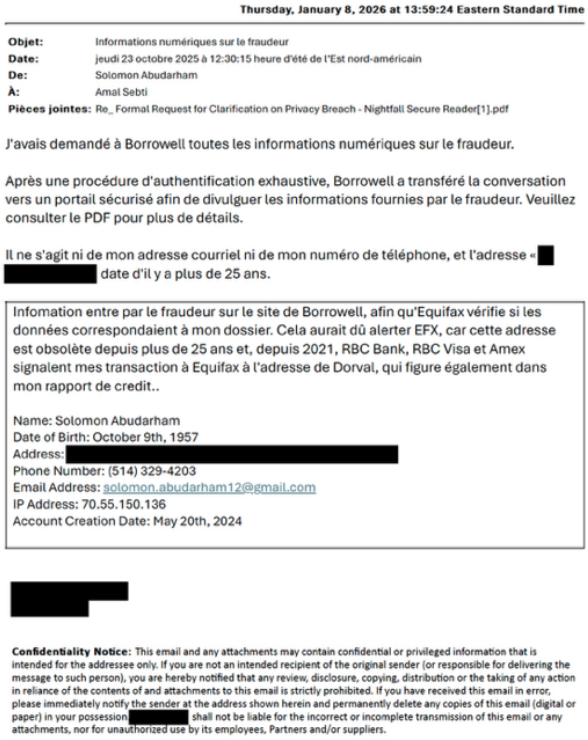
Name: Solomon Abudarham
Date of Birth: [redacted]
Address: 2[redacted]
Phone Number: (514) 329-4203
Email Address: solomon.abudarham12@gmail.com
IP Address: 70.55.150.136
Account Creation Date: May 20th, 2024

Please let us know if you have any further questions.

Kind regards,

Borrowell Privacy Team

privacy@borrowell.com
borrowell.com



Thursday, January 8, 2026 at 13:59:24 Eastern Standard Time

Objet: Informations numériques sur le fraudeur
Date: jeudi 23 octobre 2025 à 12:30:15 heure d'été de l'Est nord-américain
De: Solomon Abudarham
À: Amal Sebti
Pièces jointes: Re_ Formal Request for Clarification on Privacy Breach - Nightfall Secure Reader[1].pdf

J'avais demandé à Borrowell toutes les informations numériques sur le fraudeur.

Après une procédure d'authentification exhaustive, Borrowell a transféré la conversation vers un portail sécurisé afin de divulguer les informations fournies par le fraudeur. Veuillez consulter le PDF pour plus de détails.

Il ne s'agit ni de mon adresse courriel ni de mon numéro de téléphone, et l'adresse « [redacted] date d'il y a plus de 25 ans.

Infomation entre par le fraudeur sur le site de Borrowell, afin qu'Equifax vérifie si les données correspondaient à mon dossier. Cela aurait dû alerter EFX, car cette adresse est obsolète depuis plus de 25 ans et, depuis 2021, RBC Bank, RBC Visa et Amex signalent mes transaction à Equifax à l'adresse de Dorval, qui figure également dans mon rapport de credit..

Name: Solomon Abudarham
Date of Birth: October 9th, 1957
Address: [redacted]
Phone Number: (514) 329-4203
Email Address: solomon.abudarham12@gmail.com
IP Address: 70.55.150.136
Account Creation Date: May 20th, 2024

[redacted]

Confidentiality Notice: This email and any attachments may contain confidential or privileged information that is intended for the addressee only. If you are not an intended recipient of the original sender (or responsible for delivering the message to such person), you are hereby notified that any review, disclosure, copying, distribution or the taking of any action in reliance of the contents of and attachments to this email is strictly prohibited. If you have received this email in error, please immediately notify the sender at the address shown herein and permanently delete any copies of this email (digital or paper) in your possession [redacted] shall not be liable for the incorrect or incomplete transmission of this email or any attachments, nor for unauthorized use by its employees, Partners and/or suppliers.

39. Borrowell confirmed in its correspondence that the information used corresponded to the data provided by the malicious individual at the time of registration and that it had been used to allow access to the Applicant's credit file held by Equifax.

40. As previously indicated, Equifax's automated matching mechanisms accepted a match based on partial, inaccurate, or outdated information, such as his name, his date of birth, a former address dating back 25 years, as well as a telephone number and an email address that did not correspond to the account holder, all without conducting enhanced identity verification or adequately detecting inconsistencies.

41. Although these "inquiries," carried out for informational purposes, did not affect the Applicant's credit score, as they were "soft inquiries" (unlike "hard inquiries," which result in a credit check following an official financing application), the alleged harm does not lie in the consequences or impact of such an inquiry, but rather in the fact that an unauthorized third party succeeded in accessing the Applicant's highly sensitive personal and financial information, without his consent and without his knowledge.

42. Indeed, these "soft inquiries," carried out over a period of approximately four months at an almost weekly frequency, each time enabled access to the Applicant's credit report and to personal and financial information associated with his Equifax file.

43. In the course of their activities, partner third-party platforms may be granted access, through Equifax, to information contained in a consumer's credit file, which may include highly sensitive personal and financial information, such as credit scores,

credit accounts and payment history, lending and mortgage information, certain identifying information, and where applicable, public-record information (including civil and/or criminal court information).

44. Also included in this file are notes or findings from investigations, the email address, the telephone number, and the last four digits of the Social Insurance Number. This information is recorded in the documentation of the Autorité des marchés financiers (AMF), as appears from **Exhibit P-13,** and in the Applicant's credit file, Exhibit P-12.

45. The Autorité des marchés financiers states: "Individuals and businesses need your consent to view your credit report. The consent is valid for a limited time, lasting only as long as it takes for the requested service to be performed," as appears from Exhibit P-13.

46. Borrowell also states, in an article published on its website, that a credit check can only be carried out after obtaining the consent of the person concerned. Borrowell specifies that it is possible to verify whether such a consultation has been carried out by examining the "inquiries" section of the credit file, as appears from **Exhibit P-14**.

47. Equifax acts as the exclusive custodian of the credit file and retains effective control over the authentication mechanisms, the assignment of API keys, and the disclosure of credit files, as appears from **Exhibit P-15.**

V. PUBLIC COMPLAINTS

48. Numerous direct-to-consumer financial services operating in Canada, including notably Borrowell Inc., KOHO Financial Inc., Credit Karma Canada, Mogo Inc., and Chexy, rely on the application interfaces provided by Equifax. This centralized architecture, under Equifax's control, is deployed broadly across the Canadian market.

49. Borrowell promotes on its website the speed and simplicity of its registration process, expressly stating that users can "sign up in 3 minutes." The company also claims that once registered, a user can download their Equifax credit report free of charge and view their credit score at any time, without any negative impact on it. This information is available on Borrowell's website, and the article is appended as **Exhibit P-16**.

50. Partner third-party platforms do not have direct access to credit databases, nor do they control the algorithms, thresholds, or matching criteria used to link a request to a specific credit file. These platforms are limited to initiating technical requests and do not have decision-making authority over matching thresholds or validation criteria.

51. They are neither authorized financial institutions nor credit assessment agents within the meaning of the applicable legislation, and they carry out their activities exclusively through partnerships with credit assessment agencies, with the legal responsibility for access to credit files and identity validation remaining with the latter.

52. Given Equifax's role as a credit assessment agent and its control over the "**matching**" mechanisms that determine an individual's identification and the disclosure of a file, the responsibility for protecting personal information and preventing unauthorized access remains under its custody and cannot be avoided merely through the involvement of a partner, as appears from Exhibit P-6.

53. Despite repeated complaints reported on public forums and to organizations such as the Better Business Bureau regarding unauthorized access to credit files through Equifax partner third-party platforms, including notably Borrowell, KOHO, Mogo, Fairstone, and Credit Karma, the Defendants have made no substantial changes to their authentication mechanisms. These complaints are appended to the Application as **Exhibit P-17**.

54. These complaints report, among other things, the creation of fraudulent accounts, repeated consultations of credit files without consent, and matching issues or identity duplicates.

55. Certain complaints illustrate the recurring nature of these situations, including one dated December 22, 2023, in which a consumer reported more than 24 repeated consultations of their file by Borrowell since July 2023, without any account being created or authorization granted, in an alleged context of identity theft.

56. On December 7, 2023, another consumer reported repeated monthly inquiries conducted by Borrowell in the absence of any contractual relationship, raising serious concerns regarding the fraudulent use of their identity.

57. On January 2, 2024, a complaint reported the fraudulent opening of a Borrowell account that enabled access to a credit file, the submission of loan and credit card applications, and the obtaining of a card for fraudulent purposes.

58. On May 2, 2025, a consumer observed an unauthorized inquiry made by Borrowell without any existing business relationship.

59. On April 2, 2025, another individual reported an inquiry by Mogo dating back to September 2022, also without solicitation or consent.

60. Reports published on the r/PersonalFinanceCanada forum mention credit file inquiries by Credit Karma without any account being created, while a testimony covering the 2019–2020 period describes access occurring before or during an identity theft that led to the fraudulent opening of credit cards and lines of credit.

VI. KNOWLEDGE AND FORESEEABILITY (KNEW OR OUGHT TO HAVE KNOWN)

61. Public complaints, reports and customer communications described above show that unauthorized partner-platform access, identity mismatches and fraudulent

enrollments were being repeatedly reported in Canada in connection with consumer-facing partner platforms (including Borrowell and KOHO).

62. In this context, and given Equifax's exclusive role in designing, setting and operating the matching, authentication and disclosure parameters through its interfaces and APIs, Equifax knew or ought reasonably to have known that deficiencies affecting these mechanisms were enabling unauthorized access and identity impersonation.

63. Despite this, Equifax maintained and deployed the same access model at scale, without implementing safeguards proportionate to the sensitivity of credit-file information, including enhanced identity verification, effective anomaly detection, meaningful alerts to file holders, or timely corrective measures.

64. Maintaining automated matching mechanisms based on incomplete, inaccurate, or outdated information, without a systematic requirement for government-issued proof of identity or widespread use of multi-factor authentication, foreseeably increases the risk of identity theft and unauthorized disclosure to which consumers are exposed.

VII. APPLICABLE LAW

65. The laws applicable to the present class action include provincial regimes in certain common law provinces that recognize a statutory privacy tort, Québec civil law and statutory privacy protections, and federal provisions governing the collection, use, disclosure and protection of personal information.

66. In British Columbia, section 1 of the *Privacy Act* provides that "It is a tort, actionable without proof of damage" for a person, "wilfully and without a claim of right, to violate the privacy of another."

67. In Manitoba, section 2(1) of The *Privacy Act* provides that a person who "substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort" against that person.

68. In Saskatchewan, section 2 of The *Privacy Act* provides that "It is a tort, actionable without proof of damage" for a person "wilfully and without claim of right, to violate the privacy of another person."

69. In Newfoundland and Labrador, section 3(1) of the *Privacy Act* provides that "It is a tort, actionable without proof of damage" for a person, "wilfully and without a claim of right, to violate the privacy of an individual."

70. In Québec, article 35 of the C.c.Q. provides that "Every person has a right to the respect of his reputation and privacy" and that privacy "may not be invaded without the consent of the person or without the invasion being authorized by law."

71. Article 37 of the C.c.Q. provides that a person who establishes a file “shall have a serious and legitimate reason” and “may gather only information which is relevant,” and may not, without consent or authorization, “communicate such information to third persons” or “use it” inconsistently.

72. Article 1457 of the C.c.Q. provides a duty to abide by rules of conduct “so as not to cause injury to another,” and that a person who fails is liable for “any injury,” with reparation for injury “whether it be bodily, moral or material in nature.”

73. Section 5 of the Charter of Human Rights and Freedoms provides that “Every person has a right to respect for his private life,” and section 49 provides compensation for “the moral or material prejudice resulting therefrom,” with punitive damages “in case of unlawful and intentional interference.”

74. In Québec, section 10 of the ARPIPS provides that an enterprise “must take the security measures necessary to ensure the protection of the personal information” that are “reasonable given the sensitivity of the information” and related factors.

75. Section 11 of the ARPIPS provides that an enterprise must ensure personal information is “up to date and accurate when used to make a decision,” and that the information used “is kept for at least one year following the decision.”

76. Section 13 of the ARPIPS provides that no person may “communicate to a third person the personal information” unless the person consents or the Act provides for it, and consent must be given “expressly” for “sensitive personal information.”

77. Section 14 of the ARPIPS provides that consent “must be clear, free and informed” and given “for specific purposes,” and “must be requested for each such purpose, in clear and simple language,” and that consent not given accordingly “is without effect.”

78. Section 17 of the ARPIPS provides that before communicating personal information outside Québec an enterprise “must conduct a privacy impact assessment,” and that communication may occur if it would receive “adequate protection,” with a “written agreement” reflecting the assessment.

79. At the federal level, PIPEDA applies to an organization in respect of personal information it “collects, uses or discloses in the course of commercial activities” (s. 4(1)(a)); section 3 states its purpose and section 5(3) limits collection, use or disclosure to purposes “a reasonable person would consider are appropriate in the circumstances.”

80. Section 6.1 of PIPEDA provides that consent is only valid if it is reasonable to expect the individual would understand “the nature, purpose and consequences” of the collection, use or disclosure of the personal information to which they are consenting.

81. Sections 10.1 and 10.3 of PIPEDA impose breach duties where there is a "real risk of significant harm," including reporting, notification, and record-keeping; section 10.1(7) defines "significant harm" and includes "identity theft" and "negative effects on the credit record."

82. Under Schedule 1 of PIPEDA, organizations remain accountable for personal information under their control, including where it is transferred to a third party for processing. Clause 4.1.3 confirms that an organization "is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing" and that it "shall use contractual or other means to provide a comparable level of protection" while the third party processes that information.

83. Schedule 1 also requires meaningful consent and appropriate handling of personal information. Clause 4.3 states that "the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." Clauses 4.3.4 and 4.3.5 further emphasize that consent depends on "the sensitivity of the information" and that "the reasonable expectations of the individual are also relevant." In addition, clause 4.6 requires that personal information be "as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used." and clause 4.7 requires that it be protected by "security safeguards appropriate to the sensitivity of the information."

84. In the present case, the Applicant Solomon Abudarham alleges that Equifax held his credit file and that access entries or inquiries appeared "through a third-party partner platform" without his "consent" or "knowledge," and that he did not initiate the opening of the relevant partner account or the request. He further alleges that the third-party account was created using a decades-old address, along with a false email address and false phone number, yet it still resulted in access to his Equifax credit file.

85. Solomon's situation is central because it directly engages Equifax's duties to ensure that credit-file information is accurate and up to date, and that any access, use, or disclosure occurs only for appropriate purposes and with valid consent. On the Applicant's allegations, the access occurred on the basis of a partial or weak match relying on outdated address information, raising a direct issue as to Equifax's data-quality obligations and the adequacy of its identity-verification and access controls for sensitive credit-file information.

86. It is also central because, following the 2017 breach, the Privacy Commissioner of Canada concluded in PIPEDA Report of Findings 2019-001 (April 9, 2019) that Equifax Inc. and Equifax Canada contravened PIPEDA in key respects (including safeguards, accountability and meaningful consent) and issued recommendations to address those failures, confirming concrete compliance expectations that govern Equifax's handling, protection, and controlled disclosure of sensitive credit-file information.

87. In Québec, Equifax Canada is also governed by the *Credit Assessment Agents Act;* section 8 provides that protection measures include “a security freeze, a security alert and an explanatory statement.”

88. Section 17 of the *Credit Assessment Agents Act* provides that exercising a right requires a request to the credit assessment agent that proves identity or authority, and that “a request to exercise a right may be made verbally” unless an explanatory statement is necessary.

VIII. ADEQUATE REPRESENTATION

89. The Applicant is a resident of Canada domiciled in Montréal. His credit file is held by Equifax. He was employed by Equifax Canada Co., where he held a position of responsibility related to the strategy and execution of commercial enterprise data, including the maintenance and enrichment of data intended for businesses, as appears from **Exhibit P-18.**

90. The Applicant no longer works for Equifax and has no current employment, contractual, or financial relationship with either Defendant.

91. In the course of his duties, he contributed directly to the development and expansion of Equifax's user base with respect to business files.

92. Following an analysis of the access logs relating to his credit file, the Applicant noted that as of May 2024, unauthorized consultations had been carried out through the Borrowell platform at an almost weekly frequency, even though he held no account with that platform.

93. The Applicant was convinced that the origin of the situation lay with Borrowell.

94. Following a more thorough analysis conducted with his lawyer in October 2025, it became apparent that the determining cause was the deficient authentication mechanisms implemented by Equifax, which allowed a third party to access his credit file based on partial, inaccurate, or outdated information, without his consent.

95. As the Applicant never created an account with Borrowell nor consented to access to his credit file, a third party fraudulently opened an account in his name and thereby obtained full access to his file held by Equifax.

96. The Applicant has consistently demonstrated vigilance regarding the protection of his personal and financial information, vigilance that forms part of a professional reputation built over more than forty years.

97. The Applicant maintains an exemplary credit score, above 850, which he strives to protect diligently.

98. Since discovering the breach, he has experienced ongoing concern regarding the security of his credit file, his financial assets, and his identity.

99. The Applicant, like the Class Members, was reasonably entitled to expect that Equifax would ensure adequate protection of their personal information, given its central role, its regulated status, and its public commitments regarding security and fraud prevention.

100. The loss of control over his personal information caused the Applicant anxiety, stress, significant inconvenience, loss of time, as well as unexpected expenses related to managing and preventing risks.

101. By failing to use technological means appropriate and proportionate to the sensitivity of the data held, Equifax facilitated the breach and incurred civil liability for the harm suffered.

IX. CURRENT REPORTS AND FINDINGS

102. The Office of the Privacy Commissioner of Canada emphasizes that the information contained in a credit file is intrinsically sensitive and that the repeated, prolonged, and uncontrolled nature of access constitutes an aggravating factor revealing a failure to comply with the applicable protection obligations, regardless of the technical or organizational structure invoked.

103. Their report states, as appears from **Exhibit P-19**.:

> "These combinations of information are sensitive. If placed in the wrong hands they pose a real risk of harm through identity theft. In addition, the information is reputationally sensitive, as it includes, in many cases, detailed information about individuals' credit worthiness. In this context, under PIPEDA, the security safeguards in place by Equifax Inc. to protect this personal information should be commensurately high."

104. The Autorité des marchés financiers recognizes that the credit file is a central instrument of identification and financial assessment and that consultation of such a file is strictly subject to obtaining valid consent limited to its purpose, any unauthorized access exposing the person concerned to serious risks of identity theft and financial fraud and engaging the liability of the entities that enabled or validated such consultation.

105. Data published by the United States Federal Trade Commission for the years 2023 and 2024 place unauthorized consultations or disclosures of credit files, under the category "Credit Bureaus and Information Furnishers," as the leading type of complaints recorded, representing approximately 21% of annual reports in the Consumer Sentinel Network, as appears from **Exhibit P-20**.

106. The FTC specifies that such complaints may be made in the absence of immediate financial losses, since the exposure or unauthorized disclosure of sensitive financial information constitutes, in itself, real harm.

107. In Canada, the absence of distinct statistics specifically addressing unauthorized access to credit files, which are integrated into broader categories, limits the visibility of these incidents. Equifax Canada nonetheless reports an increase in financial fraud relying on the exploitation of personal information.

108. According to the “Market Pulse” report published on October 1, 2025, the rate of credit card fraud reached 0.75% in the second quarter of 2025, compared to 0.44% in 2024, while mortgage fraud and credit application fraud largely rely on the use of stolen or inaccurate data, as appears from **Exhibit P-21.**

109. The Canadian Anti-Fraud Centre reported losses of $530 million in 2023 and $645 million in 2024 attributable to identity theft fraud, which represents more than 75% of reports. The same institute notes that only a limited proportion of incidents are effectively reported, as appears from **Exhibit P-22.**

110. Furthermore, identity fraud in Canada, as reported by the Canadian Anti-Fraud Centre, indicates more than 108,000 fraud reports, of which 9,487 involve cases of identity theft, as appears from **Exhibit P-23**.

111. Identity theft, often triggered by unauthorized access to a credit file, enables the unlawful use of financial information and the fraudulent reconstruction of an identity. It is a recognized point of entry for large-scale fraud, including the opening of credit cards, and in the mortgage and real estate context. The mechanisms specific to real estate fraud are detailed in the articles filed in support of this Application, as appears from **Exhibit P-24 (bundle).**

112. In this context, Equifax Canada publicly presents itself as a key actor in the fight against fraud and identity theft, stating that it collaborates with more than forty organizations within the Canadian Anti-Fraud Coalition, acknowledging the constant increase in fraud-related losses and claiming a central role in the prevention, detection, and management of identity- and credit-related risks in Canada, as appears from **Exhibits P-25 and P-26.**

113. The Defendants also claim to hold ISO/IEC 27001 certification, one of the most recognized international standards in information security management, as appears from **Exhibit P-27.**

114. These representations made by Equifax give Canadian users a false impression of security regarding the management of their personal information. Despite the certifications and collaborations highlighted, there remains a notable gap between the public assurances given by Equifax and the security measures implemented.

X. COMPENSATORY, MORAL, AND PUNITIVE DAMAGES

115. The alleged facts reveal a serious, repeated, and prolonged infringement of the fundamental right of the Applicant and the Class Members to respect for their privacy and to the protection of their personal information. By its very nature, this infringement constitutes real, autonomous, and compensable harm, distinct from any immediate or measurable financial loss.

116. Under Québec law, harm corresponds to an infringement of a legally protected interest. It is not necessary for such an infringement to result in concrete economic damage when the violation directly affects the individual's personal sphere, intimacy, or dignity.

117. The Court of Appeal, in *Royer v. Capital One Bank (Canada Branch)*, 2025 QCCA 217, reiterates the principles applicable to damages arising from a security breach:

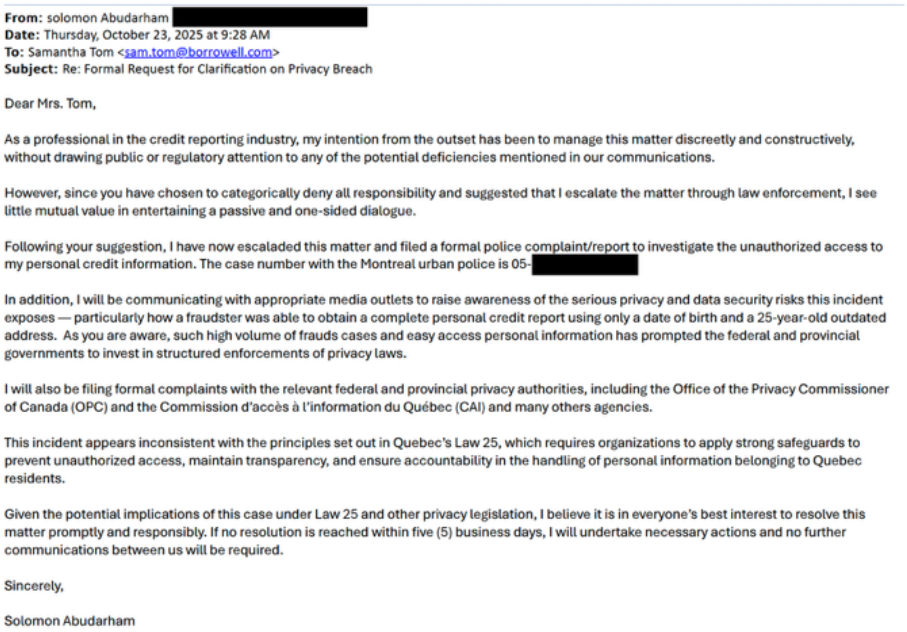
> [40] Il va sans dire que chaque situation est un cas d'espèce. C'est ainsi que le présent dossier s'éloigne de l'affaire *Sofio* où il s'agissait de la perte d'un ordinateur contenant des renseignements personnels. Cela se distingue du vol visant spécifiquement des données comme ici. De même, dans *Sofio*, aucune allégation ne référait à la dissémination potentielle des informations, voire à la connaissance de l'existence de celles-ci par une tierce personne qui aurait pu mettre la main sur l'ordinateur perdu. En l'espèce, les allégations réfèrent à un vol visant spécifiquement les données et au partage de la faille de sécurité (la recette) sur un site Internet de partage de codes et données informatiques. Une telle situation peut objectiver le risque quant à la sécurité des données exigeant ainsi des mesures, de même que susciter une crainte dépassant alors le seuil des inconvénients normaux.
>
> [13] Il en va différemment pour les coûts liés à la surveillance de crédit. Le juge retient que la surveillance accrue des opérations bancaires rendue nécessaire à la suite d'une fuite de données peut être la source d'un inconvénient indemnisable. Le groupe Capital One ayant offert une telle surveillance pour deux ans, c'est, pour le juge, la question de la suffisance de cette durée qui se pose. Il conclut, à l'instar d'autres affaires., que cette question relève du juge du fond et autorise donc l'action collective pour ce seul dommage qu'il décrit ainsi au paragraphe 248(d) de son jugement.

118. It is not necessary for the risk to materialize for harm to exist. Serious, lasting, and objectively concerning exposure to an increased risk of identity theft and financial fraud is sufficient to meet the threshold of real harm.

119. In the present case, the Applicant suffered a complete loss of control over his credit file for several months, marked by repeated, invisible, and unauthorized access carried out without his consent, without his knowledge, and without any adequate alert or protection mechanism.

120. This situation forced him to devote considerable time, sustained effort, and financial resources to constantly verifying his file, implementing credit monitoring measures, and proactively managing the risks arising from the exposure of his personal information. It also compelled him to investigate the origin of the situation. He devoted several months to understanding the problem.

121. The objective seriousness of the infringement is confirmed by the filing of an official complaint with the Service de police de la Ville de Montréal, as appears from Exhibit P-3, to investigate the unauthorized access to his personal and financial information.



From: solomon Abudarham [redacted]
Date: Thursday, October 23, 2025 at 9:28 AM
To: Samantha Tom <sam.tom@borrowell.com>
Subject: Re: Formal Request for Clarification on Privacy Breach

Dear Mrs. Tom,

As a professional in the credit reporting industry, my intention from the outset has been to manage this matter discreetly and constructively, without drawing public or regulatory attention to any of the potential deficiencies mentioned in our communications.

However, since you have chosen to categorically deny all responsibility and suggested that I escalate the matter through law enforcement, I see little mutual value in entertaining a passive and one-sided dialogue.

Following your suggestion, I have now escaladed this matter and filed a formal police complaint/report to investigate the unauthorized access to my personal credit information. The case number with the Montreal urban police is 05-[redacted]

In addition, I will be communicating with appropriate media outlets to raise awareness of the serious privacy and data security risks this incident exposes — particularly how a fraudster was able to obtain a complete personal credit report using only a date of birth and a 25-year-old outdated address. As you are aware, such high volume of frauds cases and easy access personal information has prompted the federal and provincial governments to invest in structured enforcements of privacy laws.

I will also be filing formal complaints with the relevant federal and provincial privacy authorities, including the Office of the Privacy Commissioner of Canada (OPC) and the Commission d'accès à l'information du Québec (CAI) and many others agencies.

This incident appears inconsistent with the principles set out in Quebec's Law 25, which requires organizations to apply strong safeguards to prevent unauthorized access, maintain transparency, and ensure accountability in the handling of personal information belonging to Quebec residents.

Given the potential implications of this case under Law 25 and other privacy legislation, I believe it is in everyone's best interest to resolve this matter promptly and responsibly. If no resolution is reached within five (5) business days, I will undertake necessary actions and no further communications between us will be required.

Sincerely,

Solomon Abudarham

122. Case law further recognizes that the steps imposed on victims of data breaches, including credit monitoring, placing fraud alerts, modifying or correcting personal information, consulting professionals, and the prolonged vigilance required to prevent future consequences—constitute real and compensable damages when they exceed the ordinary inconveniences that any person must tolerate in society.

123. In the Applicant's case, the situation is aggravated by the following:

(i) The unauthorized access occurred repeatedly, at an abnormal frequency and over an extended period. It targeted highly sensitive information and was made possible by deficient authentication mechanisms under Equifax's exclusive control.

(ii) The infringement is even more serious because it affects an essential tool of financial identification. Its compromise may lead to lasting, wide-ranging, and difficult-to-correct consequences.

124. The alleged deficiencies within this technological framework, presented as secure and high performing, expose Equifax to liability for the harm suffered by the Class Members, including the loss of control over sensitive information and an increased risk of fraud.

125. Personal and financial information constitutes significant economic value and is subject to illicit trade on cybercriminal markets, including on the dark web, where personal data is exchanged or disseminated. This reality substantially increases the risk that Class Members will be targeted by identity theft schemes.

126. As a result of the alleged deficiencies in the security measures implemented by Equifax, unauthorized third parties now possess personal information belonging to the Applicant and the Class Members and may have disseminated or made available all or part of this data on clandestine networks, thereby increasing the seriousness of the data breach and the scope of the harm suffered, including moral harm.

127. A high credit score constitutes an aggravating factor in the risk of identity theft. Indeed, such a score can be used to contract obligations in the name of a third party deemed creditworthy, simply by means of a false identity card, once the fraudster possesses a credit report attesting to that person's creditworthiness.

128. Class Members also suffer various harms such as fees incurred to purchase additional insurance, placing fraud alerts on their credit files, modifying personal documents, as well as time loss and costs related to detecting and managing fraudulent activity.

129. All have been exposed, without their consent, to a real risk of losing control over their personal information, to an infringement of their privacy, and to an increased risk of fraud and identity theft, requiring them to adopt sustained vigilance and to bear varying but real mitigation costs. These harms, considered both individually and collectively, exceed the threshold of ordinary inconveniences of life in society and constitute compensable compensatory and moral damages.

130. These damages flow directly from the faults alleged against the Defendants and engage their civil liability under sections 1457 and 35 et seq. of the C.c.Q., sections 5 and 49 of the *Charter of Human Rights and Freedoms*, as well as the applicable personal information protection statutes.

131. In addition to compensatory and moral damages, the alleged facts justify an award of punitive damages due to the unlawful and intentional nature, or at the very least the grossly negligent nature, of the infringements of the fundamental right of Class Members to respect for privacy.

132. Punitive damages are justified because the alleged facts first reveal an infringement of a right guaranteed by the Charter, namely the right to respect for privacy and the protection of personal information.

133. This infringement is unlawful, as it arises from wrongful conduct: Equifax, as the exclusive custodian and operator of the access, matching, and authentication mechanisms, allowed the consultation and disclosure of credit files without valid consent, following an automated process based on partial, inaccurate, or outdated information, without security measures proportionate to the extreme sensitivity of the information disclosed.

134. The infringement is also intentional within the meaning of section 49 of the Charter, as interpreted in *Québec (Public Curator) v. Syndicat national des employés de l'hôpital St-Ferdinand*, [1996] 3 S.C.R. 211, not because Equifax had a specific intent to harm, but because the unauthorized disclosure of a credit file is an immediate and natural consequence, or at the very least an extremely probable consequence, of an access model based on APIs, permissive matching, and the absence of enhanced identity verification, which Equifax maintained and deployed despite repeated reports and complaints of such incidents.

> [112] (…) Unlawful interference with one of the rights recognized by the Charter is a delict. In order to be intentional, it must be committed in circumstances which indicate a determined intent to cause the damage resulting from the violation. That intent may take a number of forms. It could appear from a finding that the fault committed is gross to the point that the mind cannot imagine that the person who committed it could have failed to realize from the outset that it would produce the harmful consequences that resulted from it. Fault is also intentional if it is the result of wild and foolhardy recklessness in disregard for the rights of others, with full knowledge of the immediate and natural or at least extremely probable consequences that his or her action will cause to the victim.

135. By maintaining and deploying this model on a large scale through partners offering direct-to-consumer services, while Equifax is aware of the sensitivity of credit files and the foreseeable risk of identity theft, Equifax acted with full knowledge of the probable consequences of this architecture on the privacy rights of the individuals concerned.

136. The repeated, prolonged, and undetected nature of the unauthorized access reinforces this conclusion. Class Members cannot protect themselves otherwise than through constant vigilance, since inquiries may occur without their knowledge and without an effective alert mechanism.

137. The loss of control over highly sensitive financial information, anxiety, the steps required, and the resulting mitigation costs exceed mere ordinary inconveniences and constitute compensable harm, even in the absence of immediate financial loss.

138. In these circumstances, an award of punitive damages is warranted in order to sanction conduct that trivializes a serious, systemic, and foreseeable risk and to prevent repetition of such infringements under section 49 of the Charter and section 93.1 of the *Act respecting the protection of personal information in the private sector*, since the infringement of the right to privacy causes harm and results, at a minimum,

from intentional conduct in the sense that Equifax maintained its system with knowledge of the extremely probable consequences, or alternatively from gross fault given the security and prudence obligations imposed by the sensitivity of the information held.

139. Even though the facts alleged here are distinct, it remains relevant to recall that Equifax has previously faced a major breach of personal information protection following the 2017 data leak. This episode gave rise to investigations, public undertakings, and class proceedings, including in Ontario, some of which are still ongoing, as appears from Exhibit P-19.

140. In this context, Equifax cannot claim today to be discovering the extreme sensitivity of the information contained in a credit file, nor the highly foreseeable nature of the risk of identity theft where access is granted based on partial or outdated data. On the contrary, this history places Equifax in a position of heightened knowledge and imposes a reinforced standard of prudence.

XI. FACTS GIVING RISE TO AN INDIVIDUAL CAUSE OF ACTION FOR EACH CLASS MEMBER

141. The Applicant reiterates all the foregoing allegations as though fully set out and incorporated herein.

142. Class Members must actively and continuously monitor not only their bank accounts, emails, and transaction statements, but also all “soft” credit inquiries, that is to say credit inquiries that do not affect the score (such as those carried out by Borrowell or other third-party partners involved in the sharing or matching of personal data transmitted without consent).

143. Such vigilance measures include, where applicable, subscribing to paid credit monitoring services, activating fraud alerts with financial institutions or credit bureaus, frequently changing passwords and sensitive personal information, placing security alerts on their credit files, or closing and reopening bank or credit accounts to minimize residual risks.

144. These steps are essential to prevent or mitigate new harm resulting from the alleged violation of the Class Members’ privacy and data protection rights by the Defendants.

145. Class Members may also be required to incur additional and verifiable expenses to subscribe to credit monitoring services, establish permanent fraud alerts, change their personal information with various third parties, purchase supplemental insurance against identity theft, or implement other reasonable protective and mitigation measures.

146. The risks to which the Defendants expose Class Members are real. The unauthorized use of personal information may lead to identity theft, where malicious individuals create false identifiers and carry out fraudulent transactions in the victim's name. Such a situation may have significant repercussions on the concerned person's credit score as well as substantial financial losses. The victim may, among other things, end up with debts they never contracted, and accounts opened without their knowledge, thereby worsening their financial situation.

147. It should be noted that many Class Members are likely unaware that the exposure of their personal information results from the unlawful transmission carried out through a "matching" system between Equifax and its third-party partners. Indeed, a fraudster may use an Equifax third-party partner system to create an account using the victim's name, address (even an outdated one), and date of birth, information that is already easily accessible online. This allows any malicious individual to access all the victim's personal information without their knowledge.

148. As a result, Class Members may incorrectly attribute any fraud or suspicious activity to other sources, without realizing that it directly results from the Defendants' alleged negligence in protecting personal information and obtaining valid consent.

XII. CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

149. The composition of the group makes it difficult or impracticable to apply the rules relating to mandates to act in the name of others or to join proceedings (article 575(3) C.C.P.) for the reasons set out below.

150. The Applicant does not know the exact number of Class Members. The identity and number of affected individuals cannot be determined without access to the Defendants' records, including access logs and partner-platform inquiry data. The Defendants are therefore called upon to confirm the total number of affected Class Members in Canada.

151. Class Members are numerous and dispersed across the province and the country.

152. Given the costs and risks inherent in legal proceedings, many individuals will hesitate to bring an individual action against the Defendants.

153. Even if Class Members could assume such an individual action, the judicial system could not cope with it, as it would be overloaded. Moreover, the multiplicity of individual actions on the issues of fact and law raised by the Defendants' conduct would lead to increased delays and costs for all parties and for the judicial system.

154. In addition, a multitude of individual actions could result in contradictory judgments on similar or related issues of fact and law concerning all Class Members. These facts demonstrate that it would be impracticable, or even impossible, to contact each Class Member to obtain a mandate and join them in a single action.

155. In these circumstances, a class action constitutes the only appropriate means allowing all Class Members to assert their respective rights and gain access to justice.

156. The harm suffered by Class Members arises, in each case, from a common core of facts, namely the Defendants' negligence and wrongful conduct in the management of their application programming interfaces and the matching mechanism used with their third-party partner platforms.

157. The claims of Class Members raise identical, similar, or related issues of law and fact within the meaning of article 575(1) C.C.P., which may be framed more specifically as follows:

a) Did the Defendants have an obligation to regulate and secure access to credit files, including where access occurs through third-party partners?

b) Were the Defendants required to impose on their third-party partners, by contract or otherwise, sufficient identity verification prior to any consultation of a file (e.g., government-issued identification, enhanced authentication, equivalent measures)?

c) Were the matching, authentication, and identity validation mechanisms implemented by the Defendants adequate and reasonable, given the highly sensitive nature of credit information?

d) Did the Defendants commit a fault by allowing access to or disclosure of a file following a process based on partial, inaccurate, or outdated information?

e) Did the Defendants know, or should they have known, that unauthorized access or fraudulent accounts were occurring through third-party partners? If so, did they delay in correcting, strengthening, or suspending the mechanisms at issue?

f) Did the alleged breaches result in an infringement of the right to privacy, including the loss of control over personal information, and a real endangerment of Class Members (serious risk of identity theft and/or fraud)?

g) Did the Defendants have an obligation to promptly and adequately notify the persons concerned when an incident presents a real risk of significant harm? Was this obligation complied with?

h) Are Class Members entitled to compensatory damages for the consequences of the alleged breaches (mitigation costs and steps, loss of time, inconvenience, stress/anxiety, other pecuniary or non-pecuniary losses)? If so, in what amount?

i) Do the alleged facts justify an award of punitive damages, notably under section 49 of the Charter and section 93.1 of the Act respecting the protection of personal information in the private sector? If so, in what amount?

XIII. NATURE OF THE ACTION AND RELIEF SOUGHT

158. The action that the Applicant seeks to bring for the benefit of the Class Members is an action in damages.

159. The alleged facts appear to justify the relief sought by the Applicant (section 575(2) C.C.P.), namely the following conclusions that the Applicant intends to present by way of an originating application:

GRANT the Applicant's class action against the Defendants.

DECLARE that the Defendants breached their obligations relating to the protection of personal information and the security of credit files, including their obligations regarding the supervision and control of access through third-party partners.

ORDER the Defendants to pay the Class Members **compensatory damages** for all pecuniary and non-pecuniary losses caused by the alleged breaches, including in particular: (i) loss of control over their personal information; (ii) mitigation steps and expenses (monitoring, verifications, protective measures); (iii) loss of time, inconvenience, stress, and anxiety; and to **ORDER** collective recovery (or, subsidiarily, individual recovery).

ORDER the Defendants to pay the Class Members **punitive damages**, pursuant to section 49 of the Charter and section 93.1 of the Act respecting the protection of personal information in the private sector, and to **ORDER** collective recovery.

ORDER the Defendants to review and strengthen their identification, matching, and authentication mechanisms allowing access to credit files, including through their application programming interfaces, in order to prevent any access resulting from erroneous matching or insufficient identity verification.
ORDER the Defendants to require, from any third-party partner, prior to the opening of an account providing access to a credit file, enhanced identity verification, including the presentation and validation of a valid government-issued identification document, or any other equivalent method providing a comparable level of security.

ORDER the Defendants to implement reasonable protection and information measures, including alerts to the holder when inquiries are made through third-party platforms, and to offer Class Members, free of charge, a protection and assistance service (including monitoring and alerts) for a period of five (5) years, or for any other duration the Court deems appropriate.

ORDER the filing of a compliance report within a time period set by the Court, describing the technical, organizational, and contractual corrections implemented.

ALL WITH interest, the additional indemnity, and costs, including expert fees and publication costs.

160. The Applicant proposes that this class action be brought on a pan-Canadian basis before the Superior Court in the District of Montréal for the following reasons:

161. The Applicant resides in the District of Montréal.

162. Many Class Members reside in the Province of Québec.

163. The undersigned lawyers representing the Applicant and the proposed class practise in the District of Montréal.

164. The Applicant, who seeks to be appointed as Class Representative, can adequately represent the Class Members (article 575(4) C.C.P.) for the following reasons:

165. The Applicant is a Class Member.

166. The Applicant understands the nature of the action.

167. The Applicant's interests are not antagonistic or otherwise contrary to those of the other Class Members.

168. The Applicant can ensure adequate representation of the members of the proposed class. Moreover, he has the capacity and interest to represent all members of the proposed class, who were affected by the breach of confidentiality and protection of their personal information resulting from the acts alleged against the Defendants.

169. The Applicant is willing to manage this class action in the interests of the proposed Class Members and is determined to see this matter through to completion, for the benefit of all proposed Class Members. He is also willing to devote the necessary time to this matter, both before the Superior Court and, where applicable, before the Class Action Assistance Fund, and to cooperate with his lawyers.

170. In this regard, concurrently with the filing of the present application, the Applicant and his lawyers are launching a website that will enable members of the proposed class to obtain information about this matter and to subscribe to an electronic newsletter regarding upcoming developments.

171. The Applicant has mandated his lawyers to obtain all relevant information in this matter concerning Equifax's practices and will remain informed as the evidence and proceedings develop.

172. The Applicant is acting in good faith and is bringing this class action solely to ensure that the rights of the proposed class members are recognized and that the harm each of them suffered because of Equifax's conduct is remedied.

173. The present Application is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

174. **GRANT** the present application.

175. **AUTHORIZE** the institution of a class action in the form of an originating application for damages in the District of Montréal.

176. **APPOINT** the Applicant as Class Representative for all persons included in the class described as follows:

> All natural persons residing in Canada whose Equifax credit file shows one or more access entries or inquiries generated through an Equifax third-party partner platform since at least May 20, 2024, and who did not consent to the registration or opening of the relevant partner account that gave rise to such unauthorized access, or any other class the Court may deem appropriate to define.

177. **IDENTIFY** the main issues of law and fact to be dealt with collectively as follows:

a) Did the Defendants have an obligation to regulate and secure access to credit files, including where access occurs through third-party partners?

b) Were the Defendants required to impose on their third-party partners, by contract or otherwise, sufficient identity verification prior to any consultation of a file (e.g., government-issued identification, enhanced authentication, equivalent measures)?

c) Were the matching, authentication, and identity validation mechanisms implemented by the Defendants adequate and reasonable, given the highly sensitive nature of credit information?

d) Did the Defendants commit a fault by allowing access to or disclosure of a file following a process based on partial, inaccurate, or outdated information?

e) Did the Defendants know, or should they have known, that unauthorized access or fraudulent accounts were occurring through third-party partners? If so, did they delay in correcting, strengthening, or suspending the mechanisms at issue?

f) Did the alleged breaches result in an infringement of the right to privacy, including the loss of control over personal information, and a real endangerment of Class Members (serious risk of identity theft and/or fraud)?

g) Did the Defendants have an obligation to promptly and adequately notify the persons concerned when an incident presents a real risk of significant harm? Was this obligation complied with?

h) Are Class Members entitled to compensatory damages for the consequences of the alleged breaches (mitigation costs and steps, loss of time, inconvenience, stress/anxiety, other pecuniary or non-pecuniary losses)? If so, in what amount?

i) Do the alleged facts justify an award of punitive damages, notably under section 49 of the Charter and section 93.1 of the Act respecting the protection of personal information in the private sector? If so, in what amount?

178. **IDENTIFY** the relief sought by the class action as follows:

GRANT the Applicant's class action against the Defendants.

DECLARE that the Defendants breached their obligations relating to the protection of personal information and the security of credit files, including their obligations regarding the supervision and control of access through third-party partners.

ORDER the Defendants to pay the Class Members compensatory damages for all pecuniary and non-pecuniary losses caused by the alleged breaches, including in particular: (i) loss of control over their personal information; (ii) mitigation steps and expenses (monitoring, verifications, protective measures); (iii) loss of time, inconvenience, stress, and anxiety; and to **ORDER** collective recovery (or, subsidiarily, individual recovery).

ORDER the Defendants to pay the Class Members **punitive damages**, pursuant to section 49 of the Charter and section 93.1 of the Act respecting the protection of personal information in the private sector, and to **ORDER** collective recovery.

ORDER the Defendants to review and strengthen their identification, matching, and authentication mechanisms allowing access to credit files, including through their application programming interfaces, to prevent any access resulting from erroneous matching or insufficient identity verification.

ORDER the Defendants to require, from any third-party partner, prior to the opening of an account providing access to a credit file, enhanced identity verification, including the presentation and validation of a valid government-issued identification document, or any other equivalent method providing a comparable level of security.

ORDER the Defendants to implement reasonable protection and information measures, including alerts to the holder when inquiries are made through third-party platforms, and to offer Class Members, free of charge, a protection and assistance service (including monitoring and alerts) for a period of five (5) years, or for any other duration the Court deems appropriate.

ORDER the filing of a compliance report within a time period set by the Court, describing the technical, organizational, and contractual corrections implemented.

ALL WITH interest, the additional indemnity, and costs, including expert fees and publication costs.

179. **DECLARE** that all Class Members who have not requested exclusion within the prescribed time limit are bound by any judgment rendered in the class action;

180. **SET** the opt-out period at thirty (30) days from the publication date of the notice to Class Members;

181. **ORDER** the publication or notification of a notice to Class Members in accordance with article 579 C.C.P., pursuant to a subsequent order of the Court;

182. **ORDER** that such notice be posted and made available on the homepage of the Defendants' websites and on their Facebook, Instagram, and X accounts, and to ORDER the Defendants to send the notice by email with acknowledgment of receipt and by direct mail to all Class Members;

183. **ORDER** the Defendants to pay all publication and notification costs;

184. **ALL WITH** costs, including, without limitation, court filing fees, expert fees, stenography fees, bailiff or process server fees, and all costs related to the preparation and publication of notices to Class Members.

MONTRÉAL, January 22, 2026

_____

TWIN LISBET INC.
Me Amal Sebti
Attorney for the Applicant
79 rue Bresoles, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

NOTICE OF SUMMONS
(Articles 145 et seq. C.C.P.)

Filing of a judicial application

Take notice that the Applicant has filed with the registry of the Superior Court of Québec, in the judicial district of Montréal, Canada, the present Application for authorization to institute a class action and to be appointed as the representative Applicant.

Response to this application

You must respond to this application in writing, personally or through a lawyer, at the Montréal courthouse located at **1 Notre-Dame Street East, Montréal (Québec) H2Y 1B6, district of Montréal, Canada**, within 15 days after service of this application or, if you have no domicile, residence, or establishment in Québec, within 30 days after service. This response must be served on the Applicant's lawyer.

Failure to respond

If you do not respond within the prescribed time limit, of 15 or 30 days, as the case may be, a default judgment may be rendered against you without further notice once that time limit has expired, and you may, depending on the circumstances, be required to pay legal costs.

Contents of the response

In your response, you must indicate your intention, namely:

- to agree to a settlement of the matter;
- to propose mediation to resolve the dispute;
- to contest this application and, in the cases required by the Code of Civil Procedure, to establish for that purpose, in cooperation with the Applicant, the case protocol that will govern the conduct of the proceeding. This protocol must be filed with the registry of the Court in the district mentioned above within 45 days after service of this notice. However, this time limit is 3 months in family matters or if you have no domicile, residence, or establishment in Québec;
- to propose holding a settlement conference.

This response must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Place where the judicial application is filed

This application is, except in certain cases, heard in the judicial district where your domicile is located or, failing that, your residence or the domicile you have chosen or agreed upon with the Applicant. If it has not been filed in the district where it may be heard and you wish for it to be transferred there, you may apply to the Court for such a transfer.

However, if this application relates to an employment contract, a consumer contract or an insurance contract, or to the exercise of a hypothecary right on the immovable serving as your principal residence, it will be heard in the district where the employee, consumer or insured person is domiciled or resides, whether as Applicant or Respondent, in the district where such immovable is located, or in the district where the loss occurred if it involves property insurance. If this application has not been filed in the district where it may be heard and you wish for it to be transferred there, you may, without any contrary agreement being set up against you, file an application to that effect with the special clerk of that district.

Transfer of the application to the Small Claims Division

If you have the capacity to act as an Applicant under the rules governing small claims recovery, you may contact the clerk of the Court so that this application may be processed in accordance with those rules. If you make such a request, the Applicant's legal costs may not exceed the amount of costs provided for small claims recovery.

Exhibits in support of the application

In support of their Application for authorization to institute a class action and to be appointed as representative Applicant, the Applicant relies on the following exhibits:

Exhibit	**Description**
P-1	"Partners" file (bundle): documents/materials relating to the partner
P-2	AMF document: requirements and regulatory framework applicable to credit assessment agents
P-3	Correspondence (bundle): exchanges and communications relevant to the file (redacted version)
P-4	Equifax Consumer Engagement Suite: overview of API operations
P-5	Equifax Consumer Engagement Suite: presentation of a consumer engagement solution and services
P-6	Equifax Identity Matching: identity matching and identity validation service
P-7	Equifax Credit Report Monitoring: credit file monitoring and alert service
P-8	Help Centre (Borrowell/Equifax): explanation of the credit bureau providing the credit score
P-9	Revenu Québec Statement of information: document indicating the status/information on file
P-10	Corporate registry (Georgia, USA): Equifax registration information
P-11	Press release (Borrowell/Equifax Canada): cloud transformation, final stage of the cloud project
P-12	Equifax report: Plaintiff's credit report
P-13	AMF "credit report" document: AMF exhibit relating to the credit report
P-14	Equifax article: credit check without permission, explanations and warning

P-15 Equifax Terms of Use: contractual terms, limitations, and usage framework
P-16 Borrowell “About”: company overview, services, and general operations
P-17 Complaints (bundle): complaints involving Borrowell, KOHO, Mogo, Fairstone, and Credit Karma
P-18 LinkedIn profile of the Applicant: professional information and background
P-19 OPC/PIPEDA Investigation Findings (2019-001): report/investigation by the Office of the Privacy Commissioner (Equifax)
P-20 FTC Report 2023–2024 (bundle): documentation on fraud and identity theft practices
P-21 Equifax Market Pulse (H1 2025): increase in credit card fraud and fraud trends (Oct. 2025)
P-22 FCAC (Gov. of Canada): importance of reporting fraud, data, and increase in losses (2024)
P-23 Canadian Anti-Fraud Centre Fraud Prevention Month 2025: campaign, statistics, and top frauds of 2024
P-24 Canada.ca Real estate fraud: explanations, prevention, and remedies
P-25 Equifax press release (Nov. 21, 2025): joining the Canadian Anti-Scam Coalition (CASC)
P-26 Sue Hutchison publication (Equifax Canada): public message on fraud and estimated losses
P-27 ISO 27001 (article): ISO/IEC 27001 compliance, data security, and customer trust (Canada)

Notice to attend a case management conference

Within 20 days following the filing of the protocol mentioned above, the Court may summon you to a case management conference in order to ensure the proper conduct of the proceeding. Failing that, the protocol will be deemed accepted.

MONTRÉAL, January 22, 2026

TWIN LISBET INC.
Me Amal Sebti
Attorney for the Applicant
79 rue Bresoles, Suite 111,
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

NOTICE OF PRESENTATION
(Articles 146 and 574 of the *Code of Civil Procedure*)
(Section 55 of the *Regulation of the Superior Court of Québec in Civil Matters*)

TO :
EQUIFAX CANADA CO.
EQUIFAX INC.

TAKE NOTICE that this Application for authorization to institute a class action and to be appointed as representative Applicant will be presented before the Superior Court at the Montréal Courthouse, located at 1 Notre-Dame Street East, Montréal, on a date to be determined by the Coordinating Judge of the Class Actions Division.

PLEASE ACT ACCORDINGLY.

MONTRÉAL, January 22, 2026

TWIN LISBET INC.
Me Amal Sebti
Attorney for the Applicant
79 rue Bresoles, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

CANADA

PROVINCE OF QUÉBEC
DISTRICT OF MONTRÉAL

N°: 500-06-000002-267

SUPERIOR COURT
(Class Actions Division)

SOLOMON ABUDARHAM

Applicant

v.

EQUIFAX CANADA CO.
EQUIFAX INC.

Defendants

CERTIFICATE OF REGISTRATION IN THE NATIONAL CLASS ACTIONS REGISTRY

(Section 55 of the *Regulation of the Superior Court of Québec in Civil Matters*)

The Applicant, through their undersigned counsel, certifies that the Application for authorization to institute a class action and to be appointed as representative Applicant will be registered in the National Class Actions Registry.

MONTRÉAL, January 22, 2026

TWIN LISBET INC.
Me Amal Sebti
Attorney for the Applicant
79 rue Bresoles, Suite 111
Montréal, Québec, H2Y 1V7
Telephone: (514) 993 6920
Telecopier: (579) 279 8845
Email: sebtiamal@twinlisbet.com

500-06-000002-267

(CLASS ACTION)
SUPERIOR COURT
DISTRICT OF MONTRÉAL

SOLOMON ABUDARHAM

Applicant

v.

EQUIFAX CANADA CO.
EQUIFAX INC.

Defendants

ORIGINAL

TWIN LISBET
Law firm.
Cabinet d'avocats.

Me Amal Sebti
TWIN LISBET INC.
Lawyers
79 Bresoles Street, Suite 111
Montréal, Québec, H2Y 1V7
Email : sebtiamal@twinlisbet.com
Téléphone : (514) 993 6920
Fax : (579) 279 8845

File No.: 22012026
Involved Code: BT1993