

Court File No. CV-17-00582551-00CP

**ONTARIO
SUPERIOR COURT OF JUSTICE**

B E T W E E N:

ALINA OWSIANIK

Plaintiff

- and -

EQUIFAX CANADA CO. and EQUIFAX, INC.

Defendants

Proceeding under the *Class Proceedings Act, 1992*, SO 1992, c 6

**STATEMENT OF DEFENCE TO
THIRD FRESH AS AMENDED STATEMENT OF CLAIM**

1. The defendants, Equifax Canada Co. and Equifax Inc., incorrectly named in the Third Amended Statement of Claim dated April 29, 2025 (the “**Claim**”) as Equifax, Inc. (together, the “**Defendants**”), admit the allegations contained in paragraph 12 of the Claim.
2. The Defendants have no knowledge in respect of the allegations contained in the first sentence of paragraph 10 of the Claim.
3. Except as may be expressly admitted otherwise herein, the Defendants deny all of the other allegations contained in the Claim. The Defendants specifically deny that the Plaintiff is entitled to any of the relief claimed in paragraph 1 of the Claim.

The Defendants

4. The Defendant, Equifax Inc. (“**Equifax US**”) is incorporated in Georgia and is headquartered in Atlanta, Georgia. Equifax US is a parent corporation that provides, through its subsidiaries, credit reporting, identity and fraud prevention services, and other services to businesses and consumers.

5. The Defendant, Equifax Canada Co. (“**Equifax Canada**”), a Nova Scotia corporation, is a subsidiary of Equifax US. Equifax Canada is a registered Canadian credit reporting agency and provides credit monitoring and other ancillary products to Canadian consumers. The credit monitoring and other ancillary products provided by Equifax Canada are delivered through Equifax Canada’s affiliate, Equifax Consumer Solutions (“**ECS**”), an Equifax US subsidiary located in the United States.

Subscription Products and One Time-Reports

6. During the relevant time period, Equifax Canada offered credit monitoring and identity theft products through its website to persons in Canada for purchase through a monthly subscription model, which included each of the following products: (a) Equifax Complete Advantage; (b) Equifax Complete Premier; (c) Equifax Complete Friends and Family; and (d) Equifax Identity Pro (“**Subscription Products**”).¹

¹ The Claim defines Subscription Products as “(i) Equifax Complete Advantage, (ii) Equifax Complete Premier, (iii) Equifax Complete Friends and Family, or (iv) any other Equifax products offering credit monitoring and identity theft protection.” The only other Equifax product offering credit monitoring and identity theft protection is Equifax Identity Pro.

7. The Plaintiff, Alina Owsianik, purchased Equifax Complete Premier in or around June 2013, then purchased the Equifax Complete Advantage Plan in or around November 2016.

8. During the period from May 1, 2017 to August 1, 2017, approximately 318,300 persons in Canada had Subscription Products that were active and in force. The information of only a small subset of these persons was affected in the Incident as defined below.

9. During the relevant time period, Equifax Canada also offered one-time reports, which do not operate on a subscription model or include monitoring or identity theft features (**“One-Time Reports”**).

10. Upon purchasing a Subscription Product or a One-Time Report, the Plaintiff and Class Members (as defined in the Claim) entered into agreements with the Defendants and/or their affiliates (the **“Agreements”**) and agreed to the Equifax Canada Privacy Policy. The Agreements and the Equifax Canada Privacy Policy were updated and amended from time to time.

The Incident

11. On July 29, 2017, Equifax US discovered that it had experienced an incident involving criminal unauthorized access to certain information about Class Members that it held, including that of some Canadian residents (the **“Incident”**).

12. Equifax US acted immediately to stop the unauthorized access. Equifax US promptly engaged Mandiant, a leading, independent cybersecurity firm to conduct a

comprehensive forensic review to determine the scope of the unauthorized access, including the specific data impacted. Equifax US also reported the Incident to law enforcement.

13. On September 7, 2017, Equifax US publicly announced the Incident. The announcement stated that U.S. consumers were potentially impacted and set out the categories of information that were accessed for U.S. consumers. The announcement also stated that there was unauthorized access to some information relating to certain Canadian residents.

14. On September 15, 2017, Equifax US issued a press release that set out additional details regarding the Incident, including that the Incident occurred through an exploitation of a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax US online dispute portal web application.

15. On September 19, 2017, Equifax Canada provided an update about the Incident for Canadians, noting that the investigation was ongoing.

16. The Defendants cooperated with the investigation by the Office of the Privacy Commissioner of Canada (the “**OPC**”) into the Incident. The OPC subsequently released a Report of Findings dated April 9, 2019 (the “**OPC Report**”). The Defendants do not admit fault, liability or the truth of the findings, claims or arguments set out in the OPC Report.

17. On October 2, 2017, Equifax US announced that: (a) information relating to approximately 8,000 Canadians was impacted in the Incident and, (b) some of the individuals with affected credit cards in the September 7, 2017 announcement were persons with Canadian addresses.

18. Equifax Canada also updated its website to provide information about the Incident, answers to questions about the Incident, and information about the steps that concerned Canadians could take.

19. Subsequently, Equifax Canada announced that approximately 11,670 Canadians were in the group of individuals with affected credit cards, bringing the total of affected Canadians to about 19,000. Approximately 1,273 out of the 19,000 affected Canadians had active and in force Subscription Products during the period from May 1, 2017 to August 1, 2017.

20. The affected information of the approximately 19,000 Canadians was provided to Equifax Canada by certain Canadian customers who purchased Subscription Products or One-Time Reports. Equifax Canada provided the information to ECS for ECS to deliver the products to Canadian consumers through ECS's platform and technology.

21. Equifax Canada sent notification letters to each of the approximately 19,000 Canadians, including information about the Incident, what steps Canadians could take, and offering them twelve months of free credit monitoring (Equifax Complete Premier), alerts and identity theft insurance. In each case, the notification letters informed the recipient of what specific information of theirs was potentially accessed. Equifax Canada subsequently offered an additional ten years of credit monitoring to Canadians who had signed up for the credit monitoring offered by Equifax Canada in connection with the Incident. The Plaintiff signed up for the credit monitoring offered by Equifax Canada and has an active subscription to Equifax Complete Premier.

22. The Plaintiff was sent a notification letter by Equifax Canada on October 17, 2017 advising her of the Incident and that her social insurance number, name, address, date of birth, phone number, email address, username, password, and secret question/secret answer had been impacted by the Incident. Equifax Canada stated in the letter that it believed the username, password, and secret question/secret answer were several years old and were login credentials for use of Equifax Canada's direct-to-consumer internet website.

23. Contrary to the allegations in the Claim (including the allegations at paragraphs 7 and 25), the Defendants at all relevant times had security safeguards appropriate to the sensitivity of the affected information, including physical, organizational and technical measures, to protect the affected information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

24. In respect of the allegations at, *inter alia*, paragraphs 8, 22, 25, 26 and 27 of the Claim, the Defendants acted reasonably and diligently upon becoming aware of opportunities to enhance their information security controls. The Defendants specifically deny that the Incident was in any way caused by the Defendants' failure to address the vulnerabilities and inadequacies allegedly found to exist before the Incident.

No Negligence

25. The Defendants deny the allegations, including in paragraph 32 of the Claim, that they failed in any duty owed to the Plaintiff or the Class Members or that they were negligent with respect to the Incident. The Defendants at all times met or exceeded the standard of care in respect of the creation and maintenance of appropriate security measures, including

establishing adequate security safeguards in in collecting, using, retaining and disclosing the Plaintiff's and Class Members' information.

26. Further and in any event, the Plaintiff and Class Members have suffered no damages as a result of the Incident.

27. The Defendants deny that any damages alleged by the Plaintiff or Class Members (which damages are denied) were caused or contributed to by any alleged breach of duty by the Defendants or anyone for whom the Defendants are responsible for at law.

28. To the extent that the Plaintiff or any Class Member suffered any damages as a result of the Incident, which is denied, such damages were caused by the negligent or criminal acts or omissions of the unauthorized hackers or others for whom the Defendants are not responsible at law.

29. To the extent that the Plaintiff or any Class Member suffered any damages as a result of the Incident, which is denied, such damages are excessive, non-compensable, and too remote to be recoverable at law, and the Plaintiff or Class Member caused and contributed to their own harm, or risk of harm, by their own conduct, including by releasing their personal information routinely in daily life in various circumstances, and/or by failing to accept the credit monitoring and related services offered by the Defendants after the Incident. The Defendants further rely on their pleading at paragraphs 50 to 56 herein.

No Breach of Contract

30. The Defendants plead and rely upon the provisions of the Agreements in effect at the relevant times.

31. The Defendants complied with their obligations pursuant to the Agreements with respect to the collection, use, disclosure and safeguarding of the Plaintiff's and Class Members' personal information.

32. The Defendants' commitments to privacy in the Privacy Policy referred to at paragraph 34 of the Claim were not a guarantee that unauthorized access by a third party would never occur.

33. The Defendants at all material times took reasonable efforts to protect the Plaintiff's and Class Members' personal information.

34. In any event, the Defendants deny that any alleged breach of their contractual obligations (which is denied) caused or contributed to the Incident or to any of the Plaintiff's and Class Members' alleged losses (which are denied). The Plaintiff and Class Members have suffered no damages as a result of any alleged breach of contract by the Defendants, or as a result of the Incident.

35. In the alternative, if the Plaintiff and or any Class Members did suffer any damages, which is denied, the damages claimed are excessive, non-compensable, and too remote to be recoverable in law, and the Plaintiff and Class Members failed to take any or all reasonable steps to mitigate such damages. The Defendants further rely on their pleading at paragraphs 50 to 56 herein.

36. Moreover, the damages claimed by the Plaintiff and Class Members are excluded pursuant to the limitation of liability provisions in the applicable Agreements.

37. In response to the allegation at paragraph 38 of the Claim, the Defendants deny that the repayment of fees paid is available to the Plaintiff and Class Members, including because the Plaintiff and Class Members have no legitimate interest in preventing the Defendants from earning their profits from the Subscription Products and any such profits were earned through the Defendants' performance of the services for which the Plaintiff and Class Members contracted.

38. The Defendants are not liable to the Plaintiff or Class Members for breach of contract as alleged in the Claim or otherwise.

No Breach of Provincial Privacy Statutes

39. The Defendants deny the Plaintiff's allegations with respect to the *Privacy Act* of each of British Columbia, Manitoba, Newfoundland & Labrador, and Saskatchewan and the Quebec law.

40. The claim under the Quebec privacy statute, an *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, cannot be asserted because at all material times, the legislation did not establish a statutory tort or other civil cause of action.

41. The Ontario Superior Court of Justice lacks jurisdiction to adjudicate claims under the *Privacy Act* in Manitoba and Newfoundland & Labrador. The legislation in these provinces confers exclusive jurisdiction upon the respective superior court in each province.

42. In addition, the Plaintiff's claims do not disclose and, in the alternative, cannot establish, causes of action pursuant to the privacy statutes.

43. The Plaintiff has not pleaded that the Defendants willfully or without claim of right violated the privacy of the Class Members; in any event, the Defendants did not do so. The Defendants did not undertake any acts with the intention of, or for the purpose of, invading the Plaintiff's or Class Members' privacy. The Defendants did not do anything "without a claim of right"; the Defendants did not act without lawful authority in respect of any acts or omissions they are alleged to have committed, nor is such an allegation pleaded.

44. None of the *Privacy Acts* (or the privacy protections set out in the *Civil Code of Québec*, CQLR c CCQ-1991) impose liability in respect of a defendant's failure to protect a plaintiff's confidential information (the confidential nature of which is, in any event, denied) from third party intruders.

No Breach of Consumer Protection Legislation

45. The Defendants deny that they engaged in a prohibited practice or otherwise breached any obligations pursuant to the Equivalent Consumer Protection Statutes as defined in the Claim.

46. The Defendants did not make false or misleading representations in relation to their security measures. The Defendants represented only that they would implement reasonable safeguards with respect to users' privacy and security. The Defendants did not make any representations that those safeguards would guarantee that unauthorized access would never occur; the Defendants did implement those reasonable safeguards.

47. The Defendants deny that rescission is available to the Plaintiff and Class Members under the Equivalent Consumer Protection Statutes, including because the return of

goods or services is not possible as the services purchased were fully performed and cannot be returned to the Defendants.

48. In any event, the Plaintiff and Class Members have not suffered any loss as a result of the Incident. The Defendants specifically deny that the Plaintiff and Class Members are entitled to damages or to rescission under the Equivalent Consumer Protection Statutes. The Defendants further rely on their pleading at paragraphs 50 to 56 herein.

49. Contrary to paragraph 50 of the Claim, the Defendants deny that it is in the interests of justice to dispense with the notice requirements pursuant to the Equivalent Consumer Protection Statutes, and accordingly, deny that an order waiving the notice requirements should be granted.

No Causation or Damages

50. The Defendants deny that the Plaintiff and Class Members have suffered the damages alleged in the Claim or at all, and the Defendants put the Plaintiff and Class Members to the proof thereof.

51. In the alternative, if any of the Plaintiff or Class Members have suffered any damage, which is denied, any such damage was neither caused nor contributed to by any act or omission by the Defendants or anyone for whom the Defendants are responsible at law. Any such damage was caused or contributed by the acts of third parties, and/or, among other things, by the fact of the Plaintiff's and Class Members' personal information, or some of it, having been publicized voluntarily by the Plaintiff, Class Members or third parties, or compromised in prior or subsequent incidents unrelated to the one at issue in the Claim.

52. Further, and in the alternative, if any Plaintiff or Class Member has suffered any damage as a result of the Incident, which is denied, the Plaintiff or Class Member failed to take steps to mitigate his or her damages, including, among other things, by failing to enrol in the credit monitoring protection and related services provided by the Defendants.

53. In the alternative, if Plaintiff and Class Member did suffer any damages, which is denied, the damages claimed are excessive, non-compensable, and too remote to be recoverable in law.

54. Moreover, as pleaded above, the damages claimed by the Plaintiff and Class Members are excluded pursuant to the limitation of liability provisions in the applicable Agreements.

55. The Defendants deny that there is any basis in fact or law for a claim for potential damages that Class Members may suffer in the future.

56. If this Court finds that damages are owed, the Defendants deny that they can be assessed on an aggregate basis.

No Punitive Damages

57. The Defendants deny that they have acted in any fashion that would justify an award of punitive, exemplary or aggravated damages as claimed at paragraph 1(d) of the Claim.

Dismissal of Action

58. The Defendants ask that this action be dismissed with costs.

July 31, 2025

FASKEN MARTINEAU DuMOULIN LLP

Barristers and Solicitors
333 Bay Street, Suite 2400
Bay Adelaide Centre, Box 20
Toronto ON M5H 2T6

Laura F. Cooper (LSO: 35426A)

lcooper@fasken.com
Tel: 416 865 5471

Alex D. Cameron (LSO: 54079T)

acameron@fasken.com
Tel: 416 865 4505

Vera Toppings (LSO: 55683Q)

vtoppings@fasken.com
Tel: 416 865 5136

Pavel Sergeyev (LSO: 73043A)

psergeyev@fasken.com
Tel: 416 868 3443

Carolyn Flanagan (LSO: 76989K)

cflanagan@fasken.com
Tel: 416 865 4381

Lawyers for the Defendants,
Equifax Canada Co. and Equifax Inc.

TO: **SOTOS LLP**
55 University Ave., Suite 600
Toronto ON M5J 2H7
Tel: 416 977 0007
Fax: 416 977 0717

Jean-Marc Leclerc (LSO: 43974F)
jleclerc@sotos.ca

Adil Abdulla (LSO: 82095E)
aabdulla@sotos.ca

Lawyers for the Plaintiff

ALINA OWSIANIK

-and-
Plaintiff

EQUIFAX, INC. et al.

Defendants

Court File No. CV-17-00582551-00CP

E-Service Detail:

Jean-Marc Leclerc, Sotos LLP (jleclerc@sotos.ca)

Adil Abdulla, Sotos LLP (aabdulla@sotos.ca)

**ONTARIO
SUPERIOR COURT OF JUSTICE**

Proceeding commenced at Toronto

Proceeding under the *Class Proceedings Act, 1992*

STATEMENT OF DEFENCE

FASKEN MARTINEAU DuMOULIN LLP

Barristers and Solicitors
333 Bay Street, Suite 2400
Bay Adelaide Centre, Box 20
Toronto ON M5H 2T6

Laura F. Cooper (LSO: 35426A)

lcooper@fasken.com
Tel: 416 865 5471

Alex D. Cameron (LSO: 54079T)

acameron@fasken.com

Vera Toppings (LSO: 55683Q)

vtoppings@fasken.com

Pavel Sergeyev (LSO: 73043A)

psergeyev@fasken.com

Carolyn Flanagan (LSO: 76989K)

cflanagan@fasken.com

Lawyers for the Defendants,
Equifax Canada Co. and Equifax Inc.