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

REPLY

1. The Plaintiff admits the allegations contained in paragraphs 4, 6, 7, 13, 14, 15 and 22 of the Statement of Defence.

2. The Plaintiff denies all other allegations contained in the Statement of Defence.

3. Some eight years after the data breach occurred, the Defendants continue to deny responsibility to Canadians and persist in alleging that they had appropriate security safeguards and deny that the data breach was in any way caused by their failure to address vulnerabilities and inadequacies that existed before the incident. The Defendants persist in denying all allegations in the claim despite numerous government investigations that have concluded that Equifax had serious IT deficiencies that led directly to the data breach, as follows:

(a) In September 2017, the US Senate released a 67-page report entitled "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach." Key findings included:

(i) Equifax had no formal patching policy prior to 2015, and its first standalone policy revealed a backlog of over 8,500 vulnerabilities.

(ii) Equifax failed to follow its policy requiring critical vulnerabilities to be patched within 48 hours, specifically regarding the Apache Struts alert.

(iii) Missing inventory and ineffective scanning prevented the location and patching of the vulnerable software until August 2017.

(iv) Expired SSL certificates prevented traffic decryption and monitoring, delaying breach detection by 78 days.

(v) Hackers moved laterally due to unencrypted credentials and a lack of network segmentation, and Equifax lacked real-time file-change detection tools.

(vi) Equifax waited six weeks from detection to public announcement to determine the full scope of affected individuals.

(vii) Key internal chat records created during the breach response were not preserved, leaving an incomplete record of events.

(b) On August 30, 2018, the US Government Accountability Office released a 40-page report on the Equifax data breach. Key findings included:

(i) Attackers exploited an unpatched Apache Struts vulnerability in Equifax's online dispute portal.

(ii) Four key factors facilitated the attack: identification failures (out-of-date vulnerability notifications, incomplete scans), detection failures (expired digital certificate), poor network segmentation, and weak data governance (unencrypted credentials, unrestricted query frequencies).

(c) In December 2018, the US House of Representatives Committee on Oversight and Government Reform released a 96-page report on the Equifax data breach. Key findings included:

(i) Systems remained unpatched for months, allowing attackers to exploit the vulnerability and infiltrate Equifax's internet-facing ACIS portal for 76 days.

(ii) Complex, legacy IT infrastructure and a lack of accurate software and asset inventories led to ineffective or absent patch management, file integrity monitoring, and network segmentation.

(iii) Attackers installed web shells, harvested unencrypted credentials, and accessed 48 databases, extracting 265 datasets containing PII, while an expired SSL certificate hindered monitoring tools for 19 months.

(iv) Organizational and governance failures were noted, including the Chief Security Officer reporting to legal rather than IT, leading to fragmented accountability.

(v) Patch Management and Certificate Management policies existed but lacked role assignments, enforcement, and automation.

(d) On April 9, 2019, the Office of the Privacy Commissioner of Canada ("**OPC**") released a 162-paragraph report which assessed the Defendants' compliance with PIPEDA following the breach. Key findings included:

(i) Equifax Inc. failed to implement appropriate security safeguards for Canadian personal information, including deficiencies in vulnerability management, network segregation, basic information security practices, and oversight.

(ii) Equifax Inc. did not adhere to its own retention policies, resulting in stale Canadian data remaining accessible from 2010 onward.

(iii) Equifax Canada lacked adequate accountability over personal information processed by Equifax Inc., evidenced by the absence of a formal written arrangement, robust monitoring, clear roles, and timely breach coordination.

(iv) Equifax Canada failed to obtain valid, express consent from Canadians for the collection and disclosure of sensitive personal information to Equifax

Inc., as privacy notices did not clearly disclose transfers to a US-based processor.

(v) Safeguards at Equifax Canada itself were insufficient, with inadequate oversight mechanisms, ineffective vulnerability management, and systemic weaknesses in basic security practices.

(vi) Post-breach measures offered to Canadians, such as limited credit monitoring, did not provide enduring protection against identity theft, unlike the credit freeze service offered in the US.

4. The OPC found that the Defendants breached several provisions of PIPEDA. These breaches included the Safeguards Principle (4.7), as Equifax Inc. and Equifax Canada failed to protect personal information with security safeguards appropriate to the sensitivity of the information. Equifax Inc. also failed to implement its retention policies, meaning personal information was not destroyed or erased when no longer required, which breached the Retention and Destruction Requirements (Principle 4.5) Furthermore, Equifax Canada failed to demonstrate adequate accountability for protecting personal information collected by Equifax Inc. and disclosed by Equifax Canada to Equifax Inc., breaching the Accountability Principle (4.1). The Consent Principle (4.3) was breached because Equifax Canada did not obtain adequate consent from Canadians for the collection and disclosure of their personal information to Equifax Inc. Finally, Equifax Canada did not implement adequate post-breach safeguards to protect against unauthorized use of compromised personal information, breaching Principle 4.7.1 related to post-breach safeguards.

5. As a trusted steward of personal information, and as part of its obligations to maintain strict security safeguards and accepted industry standards, among other things, Equifax had a contractual obligation to comply with applicable privacy legislation, including PIPEDA. Equifax expressly incorporated PIPEDA Principle 4.1.3 in its Privacy Policy and breached PIPEDA Principle 4.1.3, as found by the OPC. Equifax failed to comply with PIPEDA, as found by the OPC, and breached its contracts with the contract-only and combined subclasses. Equifax failed to comply with PIPEDA for the access-only subclass.

6. This Court has jurisdiction to adjudicate claims under the *Privacy Act* in Manitoba and Newfoundland & Labrador pursuant to constitutional principles established by the Supreme Court of Canada in *Sanis Health v. British Columbia*, 2024 SCC 40, and by the BC Court of Appeal in *Campbell v. Capital One Financial Corporation*, 2024 BCCA 253.

August 11, 2025

SOTOS LLP
55 University Avenue, Suite 600
Toronto ON M5J 2H7

Jean-Marc Leclerc (LSO # 43974F)
jleclerc@sotos.ca
Adil Abdulla (LSO # 82095E)
aabdulla@sotos.ca

Tel: 416-977-0007
Fax: 416-977-0717

Lawyers for the Plaintiff

TO: **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.

ALINA OWSIANIK
Plaintiff

-and-

EQUIFAX CANADA CO. et al.
Defendants

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

ONTARIO
SUPERIOR COURT OF JUSTICE

PROCEEDING COMMENCED AT TORONTO

Proceeding under the *Class Proceedings Act,* 1992

REPLY

SOTOS LLP
55 University Avenue, Suite 600
Toronto ON M5J 2H7

Jean-Marc Leclerc (LSO # 43974F)
jleclerc@sotos.ca
Adil Abdulla (LSO # 82095E)
aabdulla@sotos.ca

Tel: 416-977-0007

Lawyers for the Plaintiff

Email for parties served:
Laura Cooper: lcooper@fasken.com