**Court File No./N° du dossier du greffe:** CV-17-00582551-00CP

Electronically issued
Délivré par voie électronique : 12-Sep-2017
Toronto

*(Court Seal)*

# *ONTARIO*
# SUPERIOR COURT OF JUSTICE

BETHANY AGNEW-AMERICANO

**Plaintiff**

and

EQUIFAX CANADA CO. and EQUIFAX, INC.

**Defendants**

Proceeding under the *Class Proceedings Act, 1992*

## STATEMENT OF CLAIM

TO THE DEFENDANTS

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiff. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a Statement of Defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the Plaintiff's lawyer or, where the Plaintiff does not have a lawyer, serve it on the Plaintiff, and file it, with proof of service in this court office, WITHIN TWENTY DAYS after this Statement of Claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your Statement of Defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a Statement of Defence, you may serve and file a Notice of Intent to Defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to serve and file your Statement of Defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

TAKE NOTICE: THIS ACTION WILL AUTOMATICALLY BE DISMISSED if it has not been set down for trial or terminated by any means within five years after the action was commenced unless otherwise ordered by the court.

Date _____ Issued by _____
Local Registrar

Address of
court office:

TO: EQUIFAX CANADA CO.
5700 Yonge Street
Suite #1501
Toronto, Ontario M2M 4K2

AND TO: EQUIFAX, INC.
1550 Peachtree Street, N.W.
Atlanta, Georgia 30309
United States of America

# CLAIM

1. The plaintiff claims on her own behalf and on behalf of the Proposed Class (as defined below):

(a) an order pursuant to the *Class Proceedings Act, 1992*, S.O. 1992, c. 6 ("**CPA**") certifying this action as a class proceeding and appointing her as a representative plaintiff for the Proposed Class (as defined below);

(b) an aggregate assessment of damages in the amount of $500 million for:

(i) negligence;

(ii) breach of contract;

(iii) intrusion upon seclusion;

(iv) breach of the *Privacy Act*, R.S.B.C. 1996, c. 373;

(v) breach of *The Privacy Act*, C.C.S.M., c. P125;

(vi) breach of *The Privacy Act*, R.S.S. 1978, c. P-24;

(vii) breach of the *Privacy Act*, R.S.N.L. 1990, c. P-22; and

(viii) breach of the *Civil Code of Quebec*, L.R.Q., c. C-1991, art. 35-40, and *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1;

(c) an order pursuant to s. 25 of the CPA directing individual hearings, inquiries and determinations for class members who have suffered or may have suffered special damages as a result of unlawful conduct by third parties, including identity theft, which may have been occasioned by or attributable to the defendants' breaches as alleged, and all necessary directions relating to the procedures to be followed in conducting hearings, inquiries and determinations;

(d) exemplary, punitive and/or aggravated damages in the amount of $50 million;

(e) interim relief compelling the defendants to give direct notice to affected Canadians that a data breach occurred in relation to their personal information;

(f) prejudgment interest in accordance with section 128 of the *Courts of Justice Act*, R.S.O. 1990, c. C.43, as amended;

(g) postjudgment interest in accordance with section 129 of the *Courts of Justice Act*, R.S.O. 1990, c. C.43, as amended;

(h) the costs of this proceeding, plus all applicable taxes; and

(i) such further and other relief as this Honourable Court may deem just.

## (1) THE NATURE OF THIS ACTION

2. This action arises as a result of an enormous cybersecurity privacy breach impacting millions of North American consumers' most sensitive personal financial information. The defendants are part of a large and well-known credit reporting agency that collects sensitive financial information relating to millions of individuals and businesses. The defendants also

provide credit monitoring services, a primary purpose of which is to provide early warning, detection and prevention of identity theft or fraud.

3. On September 7, 2017, the defendant Equifax, Inc. ("**Equifax U.S.**") issued a PR Newswire press release, announcing that an unauthorized intrusion had occurred in its computer systems between mid-May 2017 through July 2017, impacting approximately 143 million U.S. consumers (approximately 60% of the U.S. adult population) and an undisclosed number of Canadian persons.

4. The press release stated that "a cybersecurity incident" involving a U.S. website application vulnerability led to the exposure of personal information of millions of consumers, including sensitive information such as names, social security numbers, birth dates, addresses, driver's licence numbers, credit card information and other personal information. The stolen information are the "Crown jewels" of personal financial information. The data breach is so sensitive and comprehensive that it allows fraudsters to effect massive financial and personal damage in the form of identity theft and exposure of intimate financial details. These risks will persist many years into the future.

5. The privacy breach is exacerbated by the fact that: the defendants hold themselves out to the public as data security experts whose very purpose is to protect against data breaches; their inadequate steps taken to respond to the data breaches once discovered; their delay in disclosing the security breach to the public; their inept subsequent efforts to inform and assist affected Canadians; and the fact that the defendants have been involved in previous incidents and failures to guard against unauthorized intrusions into their systems.

6. This class proceeding claims damages and relief on behalf of all Canadians affected by Equifax's privacy breaches.

## (2) THE PARTIES

### A. The plaintiff

7. The plaintiff is an individual residing in Cambridge, Ontario. In or about 2016, she purchased Equifax's Complete Premier Plan, paying $19.95 per month for daily credit monitoring and identity theft insurance. She remains a monthly subscriber.

8. The plaintiff seeks to represent the following class (the "**Proposed Class**" or "**Class Members**"):

(a) all persons in Canada whose personal information was stored on Equifax databases and which was accessed without authorization between May 1, 2017 and August 1, 2017 (or such further or different period that is specified as investigation of this case progresses); and

(b) all persons in Canada who purchased from the defendants, their subsidiaries or related companies the following products:

(i) Equifax Complete Advantage,

(ii) Equifax Complete Premier,

(iii) Equifax Complete Friends and Family

(iv) or any other Equifax products offering credit monitoring and identity theft protection,

and whose personal information stored on Equifax databases was accessed without authorization between May 1, 2017 and August 1, 2017 (or such further or different period that is specified as investigation of this case progresses) (the "**Equifax Contractual Claims**").

## B. The defendants

9. Equifax U.S. is an American corporation with its principal place of business in Atlanta, Georgia. Equifax U.S. has global operations or investments in 24 different countries. Equifax U.S. provides credit reporting services and credit protection, fraud management and credit management services. It does so either directly or indirectly through its operations or through the control of its predecessors, affiliates and subsidiaries, including the defendant Equifax Canada Co. ("**Equifax Canada**").

10. Equifax Canada is a Canadian corporation with its principal place of business in Toronto, Ontario. Equifax Canada provides credit reporting services and credit protection, fraud management and credit management services. Equifax Canada is owned and controlled by Equifax U.S.

## C. Equifax's business

11. A primary aspect of Equifax U.S.'s worldwide business operations involves selling credit reporting services for profit. To provide these services, Equifax U.S. and Equifax Canada obtain detailed and sensitive financial information about millions of Canadians and aggregate the information for resale for the purposes of providing credit ratings. Equifax U.S.'s global operations organizes, assimilates and analyzes data on more than 820 million consumers and more than 91

million businesses worldwide. Its database includes data contributed from more than 7,100 employers. Equifax U.S. does not obtain the permission of persons whose data it aggregates and stores in its systems. There is no way to "opt out" of its collection of personal information.

12. Equifax U.S. and Equifax Canada also purport to provide credit protection, fraud management and credit management services. Customers pay Equifax U.S. and Equifax Canada fees in exchange for obtaining protection against credit fraud, identity theft and other risks involving the unauthorized disclosure of personal information.

### (3) PUBLIC DISCLOSURE OF THE DATA BREACH BY EQUIFAX U.S.

13. On September 7, 2017, Equifax U.S. issued a PR Newswire press release (the "**Press Release**"). The Press Release stated that Equifax U.S. "today announced a cybersecurity incident" potentially impacting 143 million U.S. consumers and an undisclosed number of Canadian residents. The Press Release further stated that criminals "exploited a U.S. website application vulnerability" to obtain access to the information between mid-May through July 2017, according to Equifax's investigation. The Press Release stated that the cybersecurity breach involved unauthorized access of Social Security numbers, names, dates of birth, addresses, driver's licences, credit card numbers and other kinds of personal information.

14. The Press Release stated that Equifax U.S. first discovered the data breach on July 29, 2017.

15. The Press Release stated that Equifax U.S. had set up a dedicated website to help consumers determine if their information was impacted and to sign up for credit file monitoring and identity theft protection. Equifax U.S. also set up a dedicated call centre to assist consumers.

In addition, Equifax U.S. stated it would send direct mail notices to customers whose credit card numbers or whose documents containing personal identifying information were impacted.

16. Equifax U.S.'s dedicated website or call centres offered no information whatsoever to help Canadians determine if they were affected by the data breach. While Equifax U.S.'s website explained that Canadians were affected by the breach, Equifax Canada's website and its social media accounts had no information regarding the breach. As of the date of issuance of this claim, neither defendant offered any way for Canadians to assess whether they were impacted by the data breach, despite 1½ months having passed since Equifax first identified the breach.

## (4) CAUSES OF ACTION

### A. Negligence

17. The defendants owed Class Members a duty of care in the collection, retention, use, and disclosure of personal information, and a duty to safeguard the confidentiality of their personal information. The defendants marketed themselves as experts in protecting secure data through statements such as: "[a]s personal data security experts, we're well-equipped to assist your business deal with a data breach."

18. In its privacy policy, Equifax U.S. stated that "[w]e have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax." Equifax further stated that "[a]t

Equifax, protecting the security of the information in our possession is a responsibility we take very seriously." Equifax states on its website that "data and security breaches are scary."

19. The defendants breached the standard of care. Particulars include but are not limited to:

(a) the defendants failed to take adequate steps to ensure that a website application vulnerability would not result in the exposure of extremely sensitive personal information belonging to millions of North American consumers;

(b) the defendants failed to detect the unauthorized breaches when they first occurred mid-May 2017. Cybercriminals were able to access massive amounts of sensitive personal information in Equifax's systems without being detected for approximately six weeks;

(c) subsequent to detecting the existence of the breach on July 29, 2017, Equifax U.S. waited a further 40 days before making a public disclosure of the breach;

(d) after the breach was made public on September 7, 2017, the defendants failed to provide any means for Canadians to determine whether they had been affected by the breach;

(e) the defendants failed to comply with the minimum standards provided in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; and

(f) the defendants failed to take any steps to give notice to Canadians affected by the breach.

20. As a result of the defendants' acts and omissions, Class Members suffered reasonably foreseeable damages and losses, for which the defendants are liable.

21. The continuing failure to notify Canadians whether or not their sensitive personal information was accessed by the hackers causes ongoing and irreparable harm to the individuals whose information was accessed. Because Canadians are not aware of whether their information was accessed, or are unable to confirm that this happened, they are unlikely to take steps to protect themselves from further fraud.

## B. Breach of contract

22. At the time of entering into a contractual relationship with Class Members affected by the Equifax Contractual Claims, the defendants provided a statement of their Privacy Policy which stated:

> **Safeguarding your personal information:**
>
> *Equifax maintains strict security safeguards when storing or destroying your personal information in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.* These standards are in place for all information, regardless of how it is stored and we regularly review, test and enhance our systems to ensure they meet accepted industry standards. We also limit the number of employees who may access your personal information on a need-to-know basis: this means that only employees who would need to discuss your information with you, generate a credit report or other related products or services, or conduct investigations to verify and correct your credit report, would have access to your personal information. We conduct due diligence on, and impose the same high standards that we implement internally for, our members who are permitted to access your information from us.
>
> In the event that we transfer your personal information to a third party in Canada or across borders for processing, we contractually require such third party to protect your personal information in a manner consistent with our privacy safeguarding measures, subject to the law in the third party jurisdiction [emphasis added].

23. This Privacy Policy formed part of the contracts between the defendants and Class Members affected by the Equifax Contractual Claims.

24. As described above, Class Members affected by the Equifax Contractual Claims entered into agreements to pay fees to the defendants to obtain credit protection and fraud management services.

25. It was a term of the contracts of Class Members affected by the Equifax Contractual Claims that Equifax would maintain strict security safeguards when storing and retaining personal information in order to prevent unauthorized access and similar risks. It was a further term of the contracts that the Class Members would be provided with notice if their personal information was disclosed on the Internet, and that they would be provided with protection against identity theft.

26. The defendants breached their contracts with Class Members, exposing their information in a massive cybersecurity breach. The defendants failed to maintain strict security safeguards. The defendants failed to notify Class Members of the cybersecurity breach and failed to protect them against identity theft. The defendants are liable to repay all fees paid by Class Members.

27. The contracts between the defendants and Class Members affected by the Equifax Contractual Claims provide: “This Agreement is made and will be interpreted under Ontario law, and you submit to the exclusive jurisdiction of Ontario courts located in Toronto.”

## C. Intrusion upon seclusion

28. The actions of the defendants constitute intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person, for which the defendants are liable. The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns. Their actions were highly offensive, causing distress and anguish to Class Members, for which the defendants are liable and should pay damages.

## D. Breach of provincial privacy statutes

29. Section 1 of the *Privacy Act*, R.S.B.C. 1996, c. 373 ("**BC Privacy Act**") provides:

> (1) It is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another.
>
> (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
>
> (3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
>
> (4) Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.

30. Section 2 of *The Privacy Act*, C.C.S.M., c. P125 ("**Manitoba Privacy Act**") provides:

> (1) A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.
>
> (2) An action for violation of privacy may be brought without proof of damage.

31. Section 2 of *The Privacy Act*, R.S.S. 1978, c. P-24 ("**Saskatchewan Privacy Act**") provides:

> 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.

32. Section 3 of the *Privacy Act*, R.S.N.L. 1990, c. P-22 ("**Newfoundland and Labrador Privacy Act**") provides:

> (1) 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.
>
> (2) The nature and degree of privacy to which an individual is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties.

33. Articles 35 and 37 of the *Civil Code of Quebec*, L.R.Q., c. C-1991 ("**Quebec Civil Code**") provide:

> 35. Every person has a right to the respect of his reputation and privacy.
>
> The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.
>
> 37. Every person who establishes a file on another person shall have a serious and legitimate reason for doing so. He may gather only information which is relevant to the stated objective of the file, and may not, without the consent of the person concerned or authorization by law, communicate such information to third persons or use it for purposes that are inconsistent with the purposes for which the file was established. In addition, he may not, when establishing or using the file, otherwise invade the privacy or injure the reputation of the person concerned.

34. Section 10 of *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1 ("**ARPPIP**") provides:

> 10. A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

35. As described above, the actions of the defendants constitute intentional or reckless intrusions upon seclusion that would be highly offensive to a reasonable person, for which the defendants are liable. The defendants failed to take appropriate steps to guard against unauthorized access to sensitive financial information involving the Class Members' private affairs or concerns. As a result, the defendants are liable pursuant to the B.C. Privacy Act, the Manitoba Privacy Act, the Saskatchewan Privacy Act, the Newfoundland and Labrador Privacy Act the Quebec Civil Code and the ARPPIP.

## (5) DAMAGES

### A. Damages for breach of privacy

36. As a result of the defendants' actions, Class Members have suffered and will continue to suffer damages, including:

(a) damages resulting from synthetic or fictitious identity fraud schemes;

(b) damage to credit ratings and perceived credit worthiness;

(c) costs incurred to remedy and prevent identity theft;

(d) damage to reputation;

(e) out-of-pocket expenses;

(f) general damages to be assessed in the aggregate; and

(g) special damages caused by unlawful conduct by third parties, including identity theft, occasioned by or attributable to the defendants' breaches as alleged herein.

37. Damages should be awarded on both an aggregate and individual basis. Equifax Canada has acknowledged that "synthetic or fictitious identity schemes cost Canadians potentially $1 billion a year in losses. They are real numbers based on carefully calculated cost analysis." The defendants' acts and omissions, as detailed above, have materially increased the risk to every class member of being victimized by identity theft and have materially increased the quantum of damages that will arise from identify theft to class members.

38. The plaintiff also requests individual hearings under s. 25 of the CPA for special damages pleaded in paragraph 36(g) above.

**B. Punitive damages requested**

39. The defendants' conduct was high-handed, reckless, without care, deliberate, and in disregard of Class Members' rights. They knew or ought to have known that their actions and omissions would have a significant adverse effect on all Class Members.

40. The defendants knew they had been subject to previous hacking efforts, investigations and audits, that they were particularly vulnerable to being hacked, and knew that their systems were a treasure trove for fraudsters. For example:

(a) In 2004, Equifax confirmed that the records of approximately 1,400 consumers in B.C. and Alberta were accessed by criminals posing as legitimate customers;

(b) In August 2006, the Office of the Privacy Commissioner of Canada audited the personal information management practices of Equifax Canada on the basis that there were reasonable grounds to believe that Equifax Canada was contravening a provision of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5;

(c) In 2013, Equifax revealed that hackers had obtained fraudulent access to personal data of celebrities and prominent figures; and

(d) In 2016, Equifax revealed that tax and salary data for hundreds of thousands of employees of a U.S. grocery chain was stolen in a data breach.

### (6) SERVICE OF STATEMENT OF CLAIM OUTSIDE ONTARIO

41. The plaintiff is entitled to serve this claim outside Ontario without a court order pursuant to the following rules of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194 because:

(a) Rule 17.02(f): the claim relates to a contract that was made in Ontario and a breach of contract that was committed in Ontario; and

(b) Rule 17.02(g): the claim relates to a tort committed in Ontario;

(c) Rule 17.02(p): the claim relates to a person ordinarily resident or carrying on business in Ontario.

September 12, 2017

**SOTOS LLP**
180 Dundas Street West
Suite 1200
Toronto ON  M5G 1Z8

David Sterns (LSUC#36274J)
dsterns@sotosllp.com

Louis Sokolov (LSUC#34483L)
lsokolov@sotosllp.com

Jean-Marc Leclerc (LSUC#43974F)
jleclerc@sotosllp.com

Mohsen Seddigh (LSUC# 70744I)
mseddigh@sotosllp.com

Sabrina Callaway (LSUC# 65387O)
scallaway@sotosllp.com

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

Lawyers for the Plaintiff

BETHANY AGNEW-AMERICANO

**Plaintiff**

-and-

EQUIFAX CANADA CO. and EQUIFAX, INC.

**Defendants**

**Court File No./N° du dossier du g** CV-17-00582551-00CP

***ONTARIO***
**SUPERIOR COURT OF JUSTICE**

PROCEEDING COMMENCED AT TORONTO

Proceeding under the *Class Proceedings Act, 1992*

# STATEMENT OF CLAIM

**SOTOS LLP**
180 Dundas Street West
Suite 1200
Toronto ON M5G 1Z8

**David Sterns (LSUC # 36274J)**
**Louis Sokolov (LSUC # 34483L)**
**Jean-Marc Leclerc (LSUC # 43974F)**
**Mohsen Seddigh (LSUC# 70744I)**
**Sabrina Callaway (LSUC# 65387O)**

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

Lawyers for the Plaintiffs