EQUIFAX

1550 Peachtree Street, N.W.
Atlanta, Georgia 30309
(404) 885-8000

August 14, 2018

**VIA EDGAR**

Ms. Kathleen Krebs
Division of Corporation Finance
United States Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549

**Re: Equifax Inc.**
**Form 10-K for the Fiscal Year Ended December 31, 2017**
**Filed March 1, 2018**
**File No. 001-06605**

Dear Ms. Krebs:

We have reviewed the comment letter dated July 31, 2018 from the staff ("Staff") of the Securities and Exchange Commission related to the above-mentioned filing by Equifax Inc. (the "Company"). In this letter, we are providing a response to the Staff's comment. To assist your review, we have included the text of the Staff's comment below in italicized type followed by the Company's response.

Form 10-K filed March 1, 2018

Business
2017 Cybersecurity Incident, page 2

1. *In future filings, please expand your disclosure of the 2017 cybersecurity incident to discuss the origins of the cybersecurity breach and the material events that transpired once the company received notice on March 8, 2017 of the Apache Struts software vulnerability, or tell us why such disclosure is inappropriate. In this regard, we note the material information provided by your former Chief Executive Officer in his October 3, 2017 Congressional Testimony detailing the origins of the cybersecurity breach and the company's related actions.*

Response

In preparing our detailed disclosures regarding the 2017 cybersecurity incident, we did not believe it was material to investors to include a discussion of the origins of the incident and the events that transpired once the Company received notice of the Apache Struts vulnerability in March of 2017. However, we will add the disclosure bolded and underlined below in future filings (beginning with our Form 10-Q for the quarter ended September 30, 2018) in light of the Staff's comment.

Set forth below is an excerpt from Company's Form 10-Q for the quarter ended June 30, 2018, filed July 26, 2018, which included the Company's latest disclosure regarding the 2017 cybersecurity incident. Bolded and underlined language is proposed additional disclosure in response to the Staff's comment.

In fiscal 2017, we experienced a cybersecurity incident following a criminal attack on our systems that involved the theft of certain personally identifiable information of U.S., Canadian and U.K. consumers. Criminals exploited **a software vulnerability in** a U.S. website application ~~vulnerability~~ to gain unauthorized access to our network. **In March 2017, the U.S. Department of Homeland Security distributed a notice concerning the software vulnerability. We undertook efforts to identify and remediate vulnerable systems; however, the vulnerability in the website application that was exploited was not identified by our security processes. We discovered unusual network activity in late-July 2017 and upon discovery, promptly investigated the activity and, once identified as potential unauthorized access, acted to stop the intrusion and engaged a leading, independent cybersecurity firm to conduct a forensic investigation to determine the scope of the unauthorized access, including the specific information potentially impacted.** Based on our forensic investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, payment card numbers for approximately 209,000 U.S. and Canadian consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. The investigation also determined that personal information of approximately 19,000 Canadian consumers was impacted and approximately 860,000 potentially affected U.K. consumers were contacted regarding access to personal information. No evidence was found that the Company's core consumer, employment and income, or commercial reporting databases were accessed.

Please contact me at (404) 885-8000 if you have any questions or would like any additional information regarding this matter.

Sincerely,

/s/ John J. Kelley III

John J. Kelley III
Corporate Vice President, Chief Legal Officer
and Corporate Secretary

cc: Mark W. Begor, Chief Executive Officer
John W. Gamble, Jr., Corporate Vice President and Chief Financial Officer
John B. Beckman, Esq., Hogan Lovells US LLP
William Johnson, Esq., King & Spalding LLP