[Letterhead of Equifax Inc.]

September 24, 2012

Via EDGAR and ELECTRONIC MAIL

Mr. Larry Spirgel
Assistant Director
United States Securities and Exchange Commission
Division of Corporate Finance
100 F. Street, N.E.
Washington, D.C. 20549

Re: Equifax Inc.
Form 10-K for the Fiscal Year Ended December 31, 2011
Filed February 23, 2012
File No. 001-06605

Dear Mr. Spirgel:

Below please find the response of Equifax Inc. (the "Company") to the comment of the staff (the "Staff") of the United States Securities and Exchange Commission (the "Commission") set forth in your letter dated September 7, 2012 to the Company. For the convenience of the Staff, the Company has restated the comment in italics.

Form 10-K for Fiscal Year Ended December 31, 2011

Risk Factors, page 15

Security breaches and other disruptions to our information technology ..., page 17

1. *We note you disclose that disruptions to your information technology networks and infrastructure may be vulnerable to damage, disruptions, or shutdowns due to various events, including cyber attacks and other security breaches. If you have experienced any cyber attacks, security breaches or other similar events in the past, in future filings, beginning with your next Form 10-Q, please confirm that you will state that fact in order to provide the proper context for your risk factor disclosure. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm for additional information.*

Company Response:

The Company will modify its risk factor disclosure in subsequent filings, beginning with the next Form 10-Q for the quarter ended September 30, 2012, to reflect the Staff's comment, substantially as indicated in the underlined language below:

Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.

In the ordinary course of business, we rely upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including business-to-business and business-to-consumer electronic commerce and internal accounting and financial reporting systems. Additionally, we collect and store sensitive data, including intellectual property, proprietary business information, the proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. The secure operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.

Despite our substantial investment in security measures and business continuity plans, our information technology networks and infrastructure or those of our third party vendors and other service providers could be vulnerable to damage, disruptions or shutdowns due to attacks by hackers or breaches due to employee error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events.

We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. Although we have not experienced any material breach of cybersecurity, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, significant losses, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations. Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Also, our third party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

We hope that the foregoing has been responsive to the Staff's comments. If you have any questions related to this letter, please contact me at (404) 885-8045.

* * * * *

The Company hereby acknowledges that:

- The Company is responsible for the adequacy and accuracy of the disclosure in the filing;
- Staff comments or changes to disclosure in response to Staff comments do not foreclose the Commission from taking any action with respect to the filing; and
- The Company may not assert Staff comments as a defense in any proceeding initiated by the Commission or any person under the federal securities laws of the United States.

* * * * *

Sincerely,

/s/Dean C. Arvidson

Dean C. Arvidson
Senior Vice President, Deputy General
Counsel and Corporate Secretary
Equifax Inc.

cc: Richard F. Smith
Chairman and Chief Executive Officer

Kent E. Mast
Corporate Vice President and Chief Legal Officer

Lee Adrean
Corporate Vice President and Chief Financial Officer