STATE of INDIANA
OFFICE OF THE ATTORNEY GENERAL

CURTIS T. HILL, JR.
ATTORNEY GENERAL

September 22, 2017

Equifax Inc.
c/o King & Spaulding LLP
Phyllis B. Sumner
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521

Dear Ms. Sumner:

The massive data breach disclosed by Equifax on Sept. 7, 2017, was an unprecedented assault jeopardizing the personal financial security of more than 140 million Americans and, here in Indiana, leaving more than half of our entire population vulnerable to identity theft and financial ruin.

First and foremost, it is imperative that Equifax cooperate fully with all State and Federal authorities to provide verifiable information that will lead to the identification, apprehension, conviction and disruption of the criminals, terrorists, individuals and/or organizations responsible for this attack.

One finds it nearly impossible to overstate the potential catastrophic injury to our citizens caused by your company's stunning failure to protect highly sensitive data. Unfortunately, your company's initial efforts to contain this crisis have appeared inadequate and mismanaged – or, worse, designed to take advantage of consumers' fears in the wake of the breach. This staggering failure to respond appropriately has only served to compound the innumerable problems already facing victims of the cyberattack against Equifax.

In the aftermath of the breach, Equifax told consumers they had established a website to assist individuals dealing with the fallout. Those who tried to use the site, however, only encountered additional frustration and uncertainty. Some were unable to access the site at all amid a predictable surge in web traffic. Other consumers found they received different responses based on what types of devices they used to access the website. And some citizens learned they could input gibberish into the website and still receive notifications that their information might have been compromised – seemingly indicating no true assessment of users' information was occurring at all.

Perhaps the most troubling aspect of the Equifax response is the company's efforts to charge fees to consumers for services they now need to help protect themselves following the breach. Offering fee-based credit monitoring services to people newly vulnerable through no

200 WEST WASHINGTON STREET, STATEHOUSE 219 ~ INDIANAPOLIS, INDIANA 46204 ~ TELEPHONE (317) 233-6530 ~ FAX (317) 232-7979

fault of their own is disingenuous and patently unfair. Further, attaching conditions to free credit monitoring -- such as mandatory arbitration and waiver of certain rights – also hurts efforts by Equifax to retain any level of consumer confidence.

Further, we have received several reports of consumers being charged or your website indicating that they would be charged for security freezes, commonly referred to as credit freezes. As you should know, Indiana Code 24-5-24-5 requires consumer reporting agencies to place a security freeze on a consumer's credit report no later than five days after receiving the request. In addition, Indiana Code 24-5-24-14 prohibits consumer reporting agencies from charging Indiana residents a fee to place a security freeze on their consumer report unless under limited circumstances. We expect Equifax to abide by Indiana law – and to become more proactive in providing needed assistance and resources to our citizens victimized by this breach. Please be advised that the Office of the Indiana Attorney General will conduct our own complete investigation of this data breach affecting 3.8 million Indiana residents. We will pursue all penalties and remedies available under the law on behalf of our citizens. We expect the full cooperation of Equifax in providing information on the inception and duration of the breach, the security protocols in place during the breach and the conduct of Equifax following the discovery of the breach.

Thank you for your anticipated cooperation.

Sincerely,

Curtis T. Hill Jr.
Indiana Attorney General