OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

OFFICE OF THE ATTORNEY GENERAL
STATE OF CONNECTICUT

OFFICE OF THE ATTORNEY GENERAL
COMMONWEALTH OF PENNSYLVANIA

September 8, 2017

SENT VIA: E-mail & First Class Mail

Phyllis B. Sumner
King & Spalding LLP
1180 Peachtree Street
Atlanta, GA 30309
PSumner@KSLAW.com

Re: Equifax Breach

Dear Attorney Sumner:

Thank you for speaking with our offices today regarding the recently disclosed data breach that occurred at Equifax. As we discussed, we are deeply troubled by this incident, given that it appears that the highly sensitive, private information of 143 million U.S. residents—nearly half of the nation's population — was compromised. Indeed, early indications suggest that this may be the largest and most damaging data breach to date.

Based on the information provided by Equifax, we understand that criminals were able to exploit a website application vulnerability, and that the unauthorized access occurred from mid-May through July 2017. Equifax has further disclosed that the exposed information includes names, Social Security numbers, birth dates, addresses and, in some instances, drivers' license numbers. In addition, you have indicated that credit card numbers for at least 209,000 U.S. consumers, as well as certain documents with personal identifying information for at least 182,000 U.S. consumers, were accessed.

This incident and, in particular, the extent and sensitivity of the information involved, raises serious questions about the effectiveness of Equifax's measures to protect the confidentiality of the private information that it is entrusted with. This is particularly alarming given that many of our residents that have relied on Equifax to help them guard against identity theft are now at a significant risk of identity theft.

Critical facts remain unclear, including how the breach occurred, when Equifax became aware of the breach, why it has delayed public notification until now, if and when impacted consumers will receive direct notice of the breach, and what remedial steps including protection of impacted consumers Equifax has taken.

Accordingly, we request that you provide our offices with answers to the following questions:

1. Please describe in detail the facts and circumstances of the breach, including a timeline of events leading to the discovery of the July 29th breach (including when executive leadership was made aware of the breach), the public announcement of the breach, the website application vulnerability that was exploited, and Equifax's efforts to investigate and mitigate the breach.

2. Please identify the manner in which the information subject to the breach was stored on the network involved and what technical, administrative, and physical safeguards were in place to prevent unauthorized access to such information.

3. In particular, please indicate whether encryption was employed to prevent unauthorized access to such information, and if so, explain the type of encryption used and whether and how such encryption may have been compromised.

4. Please describe the efforts taken to determine whether and how personal information was exfiltrated from Equifax's networks or servers.

5. Please provide the date by which Equifax expects notification letters or other direct and personalized notifications to be sent to affected individuals.

6. Please provide an outline of any plan, policies, and/ or procedures that Equifax currently has in place, or is developing, to prevent a future breach and a timeline for implementing any such plans, policies or procedures.

7. Please describe in detail the basis for Equifax's public assurance that it has found no evidence to date of any unauthorized activity on the company's core consumer or commercial credit reporting databases.

8. Please provide a copy of any internal or third party investigative report or audit performed by or for Equifax relative to this breach.

9. Please describe the steps Equifax has taken to protect the individuals affected by this breach, including a detailed description of the credit monitoring/identity theft protection services offered, and how and when notification to affected consumers is or will be made.

10. Please explain the delay between the date of the discovery of the breach and the public announcement of the breach.

11. Please explain why consumers are not able to sign up immediately for TrustedID Premier. We have tested the enrollment process and have been told to come back to the website after September 12.

We understand from news reports that you are currently working with law enforcement to investigate this matter. To the extent that a law enforcement agency believes your response to any question above may impede an on-going criminal investigation, we ask that you please alert us immediately, including by identifying such agency making the request in your response. We are sensitive to the need to avoid any potential interference with a criminal investigation.

Please provide the requested information no later than October 5, 2017. The information should be sent to our attention at the below addresses.

On behalf of our Offices, we appreciate your anticipated cooperation and look forward to hearing from you.

Very truly yours,

/s/ Matthew W. Van Hise
Matthew W. Van Hise
Assistant Attorney General
Consumer Privacy Counsel
Illinois Attorney General's Office
Consumer Fraud Bureau
500 South Second Street
Springfield, IL 62706
(217) 782-4436
mvanhise@atg.state.il.us

/s/ Matthew F. Fitzsimmons
Matthew F. Fitzsimmons
Department Head
Privacy and Data Security Department
Office of the Attorney General
110 Sherman Street
Hartford, Connecticut 06105
(860) 808-5400
Matthew.Fitzsimmons@ct.gov

/s/ John M. Abel
John M. Abel
Senior Deputy Attorney General
Bureau of Consumer Protection
Office of Attorney General
15th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 783-1439
jabel@attorneygeneral.gov