NYC
Consumer
Affairs

Lorelei Salas
Commissioner

42 Broadway
8th Floor
New York, NY 10004

[redacted]

nyc.gov/consumers

September 8, 2017

Rick Smith
Chairman and CEO
Equifax
1550 Peachtree Street NE
Atlanta, GA 30309

As one of the three major consumer credit reporting agencies, millions of Americans rely on you to monitor and protect their finances. In light of the recent cyber-attack on your company which compromised the names, Social Security numbers, birth dates, addresses, and driver's license numbers of nearly 143 million Americans, you have an obligation to act swiftly, definitively and, most importantly, in a way that is most likely to mitigate the potential damage to those impacted.

To date, you have offered consumers: (1) a way to discover whether their information has been compromised, and (2) limited enrollment in your credit monitoring program, TrustedID Premier, for one year. While this is a good start, it is not nearly enough.

First, Equifax must engage in targeted outreach. We have thus far seen no proactive effort on the part of Equifax to notify all affected consumers. Second, Equifax must provide DCA with information that will allow us to conduct extensive outreach and education to New York City consumers to ensure that all victims of this unprecedented and historic breach have the information needed to safeguard themselves and their families from identity theft. Specifically, we request that Equifax provide us with the demographics of all affected New York City consumers, including zip codes and any other pertinent information. Third, Equifax must provide automatic and immediate protection for all consumers it knows has been impacted by the breach. Currently, consumers are expected to: (1) discover that a breach occurred; (2) check Equifax's website to find out whether they have been impacted; (3) apply for enrollment in Equifax's TrustID program, in response to which Equifax merely provides a future "enrollment date"; (4) return on the "enrollment date" and click through a series of links to actually enroll. Equifax has all of the information it needs to protect consumers immediately—it should do so. Finally, however Equifax chooses to automatically and immediately protect impacted consumers, that protection should be given without conditions. Thus, if automatic and immediate protection means enrollment into Equifax's TrustID Premier program, that enrollment should be free of charge, ongoing and not subject to conditions like mandatory arbitration.

Equifax is responsible for this breach and the subsequent exposure of millions of people to identity theft. Yet, it has saddled its victims with a convoluted process that places the burden on them to protect themselves and that will, after only one

NYC
Consumer
Affairs

year, require payment to Equifax for a service only needed because Equifax failed at the very purpose of its job. This is unfair to consumers, and it should be unacceptable to Equifax.

If Equifax refuses to provide the automatic and immediate protection necessitated by its failure to adequately protect the sensitive consumer information in its possession, then Equifax should, at a minimum, extend its free TrustID Premier enrollment period beyond a year, offer it without conditions, and confirm that the protections provided by the program will cover the three month period from May to July 2017, before Equifax discovered the breach, as well as any period a consumer is required to wait before enrolling. As Equifax is aware, the effects of a breach of this magnitude could be felt by affected consumers for years to come.

DCA looks forward to your response.

Regards,

Lorelei Salas
Commissioner, Department of Consumer Affairs