TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

http://oversight.house.gov

October 2, 2017

The Honorable Trey Gowdy
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On September 27, 2017, representatives of Equifax briefed Democratic and Republican staff from our Committee on the massive data breach that exposed the personal information of millions of consumers. Based on that briefing, I am writing today to request that we send a bipartisan request for documents to the Computer Emergency Readiness Team (US-CERT) and the National Cybersecurity and Communications Integration Center as part of our continuing investigation into this breach.

During the briefing last week, Equifax representatives conceded that the company failed to heed an alert that was sent by US-CERT on March 8, 2017, explicitly warning about a specific vulnerability on the company's systems through a web-application known as "Apache Struts." According to Equifax, US-CERT recommended that the company install a specific patch to address this vulnerability, but the company failed to do so at that time. As a result, cyber attackers were able to exploit this vulnerability to gain access to hundreds of millions of sensitive consumer files and documents from May 13, 2017, to July 29, 2017—the date that Equifax finally detected the breach.

Equifax also informed our staff that the company's General Counsel did not inform the Federal Bureau of Investigation (FBI) about the breach until the following Wednesday, August 2, 2017. It is unclear why the company waited three days to inform the FBI, and it is also unclear whether Equifax contacted US-CERT during this time, particularly since the agency had warned specifically about this vulnerability months earlier. Equifax informed our staff that they could not confirm whether the company's General Counsel contacted anyone else in law enforcement or internally about the breach.

Finally, Equifax confirmed to our staff that the company waited from the date the company discovered the breach, July 29, until nearly six weeks later, on September 7, to finally inform the public that their personal information may have been compromised. Equifax conceded that the FBI never instructed or directed the company to withhold from the public information about the breach. It remains unclear whether US-CERT had any communications with the company during this timeframe.

To further investigate these matters, I propose that we send a bipartisan request for the following documents to the National Cybersecurity and Communications Integration Center and US-CERT:

(1) a copy of the March 8, 2017, alert sent by US-CERT to Equifax and all corresponding communications and recommendations relating to the "Apache Struts" vulnerability; and

(2) all communications between the agency and Equifax officials from March 1, 2017, to the present.

The massive data breach at Equifax exposed the personal information of over a hundred million consumers. It is critical, as part of our Committee's examination of this breach, that we obtain documents and information from all involved parties and witnesses, including US-CERT.

Thank you for your consideration of this request.

Sincerely,

Elijah E. Cummings
Ranking Member