Exhibit 99.1

EQUIFAX'S STATEMENT FOR THE RECORD
REGARDING THE EXTENT OF THE CYBERSECURITY INCIDENT
ANNOUNCED ON SEPTEMBER 7, 2017

Over the past several months, congressional committees have requested information from Equifax regarding the extent of the cybersecurity incident that Equifax reported on September 7, 2017. Accordingly, Equifax submits this statement to supplement the company's responses regarding the extent of the incident impacting U.S. consumers.

As announced on September 7, 2017, the information stolen by the attackers primarily included:

- names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers of 143 million U.S. consumers (since updated)
- credit card numbers of approximately 209,000 consumers
- certain dispute documents with personal identifying information of approximately 182,000 consumers
- limited personal information for certain United Kingdom and Canadian residents.

As earlier statements made clear, the company's forensics experts found no evidence that Equifax's U.S. and international core consumer, employment and income, or commercial credit reporting databases were accessed as part of the cyberattack. Furthermore, Equifax offered a comprehensive support package to impacted consumers on September 7, 2017.

The attackers stole consumer records from a number of database tables with different schemas, and the data elements stolen were not consistently labeled. For example, not every database table contained a field for driver's license number, and for more common elements like first name, one table may have labeled the column containing first name as "FIRSTNAME," another may have used "USER_FIRST_NAME," and a third may have used "FIRST_NM." With assistance from Mandiant, a cybersecurity firm, forensic investigators were able to standardize certain data elements for further analysis to determine the impacted consumers and Equifax's notification obligations.

As a result of its analysis of the standardized data elements, including using data not stolen in the attack, the company was able to confirm the approximate number of impacted U.S. consumers for each of the following data elements: name, date of birth, Social Security number, address information, gender, phone number, driver's license number, email address, payment card number and expiration date, TaxID, and driver's license state. As stated above, Equifax notified the public on September 7, 2017 of the primary data elements that were stolen. With respect to the data elements of gender, phone number, and email addresses, U.S. state data breach notification laws generally do not require notification to consumers when these data elements are compromised, particularly when an email address is not stolen in combination with further credentials that would permit access. The chart that follows provides the approximate number of impacted U.S. consumers for each of the listed data elements.

Data Element Stolen	Standardized Columns Analyzed[1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number[2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number[3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

The data described above is not additional stolen data, and it does not impact additional consumers. The table reflects a summary of the company's analysis of data stolen in last year's cybersecurity incident. This includes the extra measures the company took to confirm the

1 The attackers accessed records across numerous database tables with different schemas. Forensic investigators were able to standardize certain columns containing various types of information for further analysis to determine the impacted consumers and Equifax's notification obligations. The full list of standardized columns is SSN, First Name, Last Name, Middle Name, Suffix, Gender, Address, Address2, City, State, ZIP, Phone, Phone2, DL #, DL License State, DL Issued Date, D.O.B., Canada SIN, Passport #, CC Number, Exp Date, CV2, TaxID, Email Address, Full Name.

2 This represents the number of individuals who are part of the impacted population because their SSN was stolen. The impacted population included individuals with a SSN not stolen together with a name in jurisdictions that require notification in such circumstances (e.g., Indiana). Individual Tax ID numbers (ITINs) were generally housed in the same field as the SSNs. For clarity, all ITINs stored in the SSN field were included in the 145.5 million impacted population and consumers could use their ITIN in the lookup tool to see if they were affected. For approximately 97,500 individuals, the additional "TaxID" field contained a value that was stolen together with a SSN included in the lookup tool.

3 This includes the 2.4 million individuals whose partial driver's license information and name were stolen, as described in the company's announcement on March 1, 2018.

identities of U.S. consumers whose partial driver's license information was stolen but who were not in the previously identified affected population, as announced on March 1, 2018. Equifax identified these consumers by referencing other information in proprietary company records that the attackers did not steal, and by engaging the resources of an external data provider.

Through the company's analysis, Equifax believes it has satisfied applicable requirements to notify consumers and regulators. It does not anticipate identifying further impacted consumers, as it has now completed analysis of government issued identification numbers stolen together with names. It should be noted that the additional analysis also confirmed that some of the standardized columns had no real data in the data fields (specifically the data fields for passport numbers, CV2s, and driver's license issue dates).

Separately from the elements described above, which were contained within database tables and files, and as previously reported in the company's press releases[4] and responses to congressional questions, the attackers also accessed images uploaded to Equifax's online dispute portal by approximately 182,000 U.S. consumers. As a national credit reporting agency, Equifax has a statutory obligation to facilitate disputes for consumers.

Between October and December 2017, Equifax notified by direct mail the consumers who had uploaded information to the dispute portal that their dispute information was accessed. In order to provide complete information to consumers regarding their accessed images, Equifax provided these consumers individualized notifications with a list of the specific files they had uploaded onto Equifax's dispute portal and the dates of those uploads.

As part of the dispute process, some consumers may have uploaded government-issued identifications through the portal. Because the company directly notified each impacted consumer, the company had not previously analyzed the government-issued identifications contained in the images uploaded in the dispute portal. In response to congressional inquiry, we recently completed a manual review of the images that were uploaded by the impacted consumers. The chart that follows provides the approximate number of images of valid government-issued identifications.

Government-Issued Identification	Approx. # of Images Uploaded
Driver's License	38,000
Social Security or Taxpayer ID Card	12,000
Passport or Passport Card	3,200
Other[5]	3,000

The data described above is not additional stolen data, and it does not impact additional consumers. The table reflects a summary of the company's recent analysis of government-issued identifications that were uploaded by consumers to Equifax's online dispute portal and stolen by the attackers.

4 *See, e.g.,* Equifax press releases dated September 7, 2017, https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 and September 15, 2017, https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

5 Includes other types of identification documents such as military IDs, state-issued IDs and resident alien cards.

Equifax is committed to working with Congress and providing accurate information about the cybersecurity incident reported on September 7, 2017. Please let us know if you have questions about the information provided in this statement.