belonging to a set of internal high-profile users, such as Uber executives. During this time, Uber did not otherwise monitor internal access to personal information unless an employee specifically reported that a co-worker had engaged in improper access. The proposed complaint alleges that Uber's representation that it closely monitored and audited internal access to consumers' personal information was false or misleading in violation of Section 5 of the FTC Act in light of Uber's subsequent failure to monitor and audit such access between August 2015 and May 2016.

The proposed complaint also alleges that Uber failed to provide reasonable security for consumer information stored in a third-party cloud storage service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). Uber stores a variety of files in the Amazon S3 Datastore that contain sensitive personal information, including full and partial back-ups of Uber databases. These back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, email addresses, phone numbers, driver's license numbers and trip records with precise geolocation information.

From July 13, 2013 to July 15, 2015, Uber's privacy policy described the security measures Uber used to protect the personal information it collected from consumers, stating that such information "is securely stored within our databases, and we use standard, industry-wide commercially reasonable security practices such as encryption, firewalls and SSL (Secure Socket Layers) for protecting your information—such as any portions of your credit card number which we retain… and geo-location information." Additionally, Uber's customer service representatives offered assurances about the strength of Uber's security practices to consumers who were reluctant to submit personal information to Uber.

As described below, the proposed complaint alleges that the above statements violated Section 5 of the FTC Act because Uber engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information in the Amazon S3 Datastore. Specifically, Uber allegedly:

- Until approximately September 2014, failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Uber (1) permitted engineers to access the Amazon S3 Datastore with a single, shared AWS access key that provided full administrative privileges over all data stored there; (2) failed to restrict access to systems based on employees' job functions; and (3) failed to require multi-factor authentication for access to the Amazon S3 Datastore;

- Until approximately September 2014, failed to implement reasonable security training and guidance;

- Until approximately September 2014, failed to have a written information security program; and

- Until approximately March 2015, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, rather than encrypting the information.

As a result of these failures, on or about May 12, 2014, an intruder was able to gain access to Uber's Amazon S3 Datastore using an access key that one of Uber's engineers had posted to GitHub, a code-sharing site used by software developers. This key was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore. The intruder accessed one file that contained sensitive personal information belonging to Uber Drivers, including over 100,000 unencrypted names and driver's license numbers, 215 unencrypted names and bank account and domestic routing numbers, and 84 unencrypted names and Social Security numbers. Uber did not discover the breach until September 2014, at which time Uber took steps to prevent further unauthorized access.

The proposed consent order contains provisions designed to prevent Uber from engaging in similar acts and practices in the future.

Part I of the proposed order prohibits Uber from making any misrepresentations about the extent to which Uber monitors or audits internal access to consumers' Personal Information or the extent to which Uber protects the privacy, confidentiality, security, or integrity of consumers' Personal Information.

Part II of the proposed order requires Uber to implement a mandated comprehensive privacy program that is reasonably designed to address privacy risks related to Uber's