Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Ascension Data & Analytics, LLC*, File No. 192 3126**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Ascension Data & Analytics, LLC ("Respondent").

The proposed consent order ("Proposed Order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's Proposed Order.

Respondent is a Delaware company with its principal place of business in Texas. Respondent provides data, analytics, and technology services to other companies in its corporate family and their service providers relating to residential mortgages.

In early 2017, as part of work for a related company, Respondent hired a vendor to conduct Optical Character Recognition on a set of documents pertaining to 37,000 residential mortgages. The documents contained the personal information of 60,593 consumers. The type of personal information included names, dates of birth, Social Security numbers, loan information, credit and debit account numbers, drivers' license numbers, and credit files. Before providing the documents to the vendor, Respondent did not take steps to make sure the vendor was capable of protecting the personal information in the documents. Furthermore, Respondent did not require the vendor by contract to protect the documents or the consumer information contained therein.

From January 2018 to January 2019, the vendor inadvertently exposed the information from the mortgage documents online, by misconfiguring a cloud server and storage location containing information from the documents. As a result, anyone who could figure out the web address of the server or storage location could view and download the contents. The server and storage location were accessed by fifty-two unauthorized computers during the year they were exposed.

The Commission's proposed one-count complaint alleges that Respondent violated the Standards for Safeguarding Customer Information Rule ("Safeguards Rule") of the Gramm-Leach-Bliley Act ("GLB Act"). The Safeguards Rule requires financial institutions, which includes companies like Respondent, to implement a comprehensive information security program that contains certain elements.

The proposed complaint alleges that Respondent violated the Safeguards Rule by failing to include two of the required elements in its information security program. First, the proposed complaint alleges, Respondent did not oversee service providers, by failing to take reasonable steps to choose service providers capable of safeguarding personal information, and failing to require those service providers by contract to maintain the safeguards. Second, the proposed complaint alleges, Respondent failed to identify risks to the security of personal information, and assess whether any safeguards it had in place were sufficient. Respondent did not satisfy this

element of the Safeguards Rule because it failed to consider risks related to many service providers, and did not conduct risk assessments before September 2017.

The Proposed Order contains provisions designed to prevent Respondent from engaging in the same or similar acts or practices in the future. Part I of the Proposed Order prohibits Respondent from violating the Safeguards Rule.

Part II of the Proposed Order requires Respondent to establish and implement, and thereafter maintain, a comprehensive data security program that protects the security of Covered Information, the definition of which is modeled off the definitions of the Safeguards Rule.

Part III of the Proposed Order requires Respondent to obtain initial and biennial data security assessments for ten years.

Part IV of the Proposed Order requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part III.

Part V of the Proposed Order requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its data security program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI of the Proposed Order requires Respondent to notify the Commission any time it is required to make a notification to a state or local government that personal information has been breached or disclosed.

Parts VII through X of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Part XI states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.