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, LL ("Respondent")

The proposed consent order ("Proposed Order") has been placed on the public record for [illegible] receipt of comments by interested persons. Comments received during this period will [illegible] 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. [illegible] big 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 O

element of the afeguards ule because it failed to consider risks related to many service providers, and did not conduct risk assessments before eptember 2017.

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

Part II of the Proposed Order requires espondent to establish and implement, and thereafter maintain, a comprehensive data security program that protects the security of overed [illegible] the definition of which is modeled off the definitions of the afeguards ule.

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

Part [illegible] of the Proposed Order requires espondent to disclose all material facts to the assessor and prohibits espondent from misrepresenting any fact material to the assessments required by Part III.

Part [illegible] requires espondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its data security program) that espondent has complied with the requirements of the Order and is not aware of any material [illegible] that has not been corrected or disclosed to the ommission.

Part VI of the Proposed Order requires espondent to notify the ommission any time it is required to make a notification to a state or local government that personal information has been [illegible] or disclosed.

Parts VII through X of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring espondent to provide uringg