192 3126

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **ASCENSION DATA & ANALYTICS, LLC, a limited liability company.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission, having reason to believe that Ascension Data & Analytics, LLC, a limited liability company, has violated the provisions of the Commission's Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 *et seq.*; and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Ascension Data & Analytics, LLC ("Ascension" or "Respondent") is a Delaware limited liability company with its principal place of business at 701 Highlander Boulevard, Suite 510, Arlington, Texas 76015.

2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondent's Business Activities

3. Respondent is an analytics company that provides data, analytics, and system-based technology services and products to other companies in its corporate family in connection with mortgages. Respondent's many services include systems development, such as the creation of document management systems, automation of data-driven decision-making, and case management task scheduling; creating valuation models and comparative market analyses; and various due diligence reviews or analyses, such as title searches, analyses of foreclosure dockets, and risk analyses related to the foregoing.

4. In or around 2017, Respondent contracted to provide the following services for a related company in connection with due diligence for residential mortgages: (a) building and maintaining a document management system for use in storing, indexing, tracking, organizing, and displaying mortgage documents; (b) valuation review services, which included creating automated valuation models and conducting comparative market analyses; (c) reviewing and analyzing loan servicing comments; (d) compliance reviews related to loan originations; and (e) collateral reviews of imaged documents.

5. Respondent's work for the related company included hiring an unaffiliated company to process the mortgage documents of borrowers relating to approximately 37,000 mortgages. These documents included mortgage applications and various associated documents, such as tax returns, that contained information about 60,593 consumers. The types of personal information in the documents included names, dates of birth, Social Security numbers, loan information, credit and debit account numbers, drivers' license numbers, credit files, or other personal and financial information of borrowers, as well as of family members and others whose information was included in the mortgage applications.

Breach of Customer Information

6. In February 2017, Respondent contracted with an unaffiliated company, PairPrep, Inc., doing business as OpticsML ("OpticsML"), to conduct Optical Character Recognition ("OCR") scanning on the mortgage documents.

7. Per its own policies, Respondent was required to vet the security measures of OpticsML to ensure it could properly protect the sensitive personal information of consumers. However, Respondent did nothing to assess OpticsML's security measures.

8. Despite never vetting OpticsML's security, Respondent provided it with the aforementioned mortgage documents, which contained the personal information of tens of thousands of consumers, including sensitive financial information.

9. OpticsML stored the contents of the documents on a cloud-based server and in a separate cloud-based storage location. But, in doing so, OpticsML misconfigured both the server and the storage location, leaving the sensitive personal information of tens of thousands of consumers exposed to anyone on the internet for a year, beginning in January 2018. As a result, all that was needed to view or download this personal information was the internet address of the server or the storage location; no password was required.

10. The information sat unprotected until about January 2019, when media reports revealed that this information was publicly exposed online.

11. During the year the server and the storage location were unsecured, approximately 52 unauthorized IP addresses accessed them. Most of these IP addresses were associated with computers outside the United States, including addresses from Russia and China.

Gramm-Leach-Bliley Act Safeguards Rule

12. Respondent is a financial institution, as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), because it is significantly engaged in, among other things, data processing, 12 C.F.R. § 225.28(b)(14); financial and investment advisory services, § 225.28(b)(6); and real estate settlement services, § 225.28(b)(2)(viii). Respondent is subject to the GLB Safeguards Rule, 16 C.F.R. Part 314, because it is a financial institution that handles and maintains nonpublic personal information, as defined by 16 C.F.R. § 313.3(n), that pertains to customers of other financial institutions that provide such information to Respondent.

13. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive information security program that is written in one or more readily accessible parts, and that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue, including:

a. Designating one or more employees to coordinate the information security program;

b. Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks;

c. Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;

d. Overseeing service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information, and requiring service providers by contract to implement such safeguards; and

e. Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

Respondent Failed to Oversee Service Providers

14. Since at least September 2016, Respondent has failed to take reasonable steps to select service providers capable of maintaining appropriate safeguards for the personal information Respondent provided.

15. Since at least July 2016, Respondent maintained a "Third Party Vendor Risk Management" policy describing the due diligence Respondent required for service providers.

The policy recommends numerous steps Respondent's Chief Information Security Officer (CISO) and business managers were to take to evaluate service providers, such as having service providers provide their policies and procedures and fill out an information security questionnaire.

16. Despite its policy, Respondent has not taken any formal steps to evaluate whether service providers could reasonably protect the personal information Respondent had entrusted to them. For example, before Respondent provided documents containing consumers' sensitive personal information to OpticsML, Respondent did not take any of the steps described in its own policy to evaluate OpticsML's security capabilities.

17. Since at least September 2016, Respondent has also failed to require service providers by contract to implement appropriate safeguards for personal information that Respondent provided to those service providers. Instead, Respondent's service provider contracts have only included an agreement that "any nonpublic personal information . . . shall be protected from disclosure with all the provisions of the Gramm-Leach-Bailey [sic] Act," and not disclosed by either party without prior written consent. But these clauses did not make clear that the service providers, including OpticsML, were responsible for protecting the information in accordance with the GLB's Safeguards Rule, or that they were even subject to the rule. Respondent's service provider contracts failed to specify safeguards that service providers must implement, or otherwise require them to take reasonable steps to secure personal information.

18. Indeed, Respondent's service provider contracts do not satisfy its Third Party Vendor Risk Management policy, which requires Respondent to "contractually require its third party vendors to implement appropriate measures" with respect to customer information.

Respondent Failed to Adequately Assess Risk

19. Respondent has also failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control those risks.

20. Prior to September 2017, Respondent did not conduct adequate risk assessment. During this time, Respondent also did not assess risks related to its service providers, even though its "Third Party Vendor Risk Management" policy required its CISO to "complete a quantitative assessment of risk" for each service provider.

21. In September 2017 and again in October 2018, another company in Respondent's corporate family arranged for a third-party security company to conduct technology risk assessments of the corporate family, which included some evaluation of Respondent's security and risks. However, those assessments were limited to a small subset of Respondent's service providers, and did not assess the security of a long list of other service providers, including OpticsML.

Count 1
Violation of the GLB Safeguards Rule

22. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A). Respondent handles and maintains nonpublic personal information, as defined by 16 C.F.R. § 313.3(n), about customers of financial institutions.

23. As set forth in Paragraphs 14-18, Respondent has failed to oversee service providers.

24. As set forth in Paragraphs 19-21, Respondent has failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and failed to assess the sufficiency of any safeguards in place to control those risks.

25. Therefore, the conduct set forth in Paragraphs 23-24 is a violation of the Safeguards Rule, 16 C.F.R. Part 314.

THEREFORE, the Federal Trade Commission this ___ day of _____ 2020, has issued this complaint against Respondent.

By the Commission, Commissioner Chopra dissenting, Commissioner Slaughter not participating.

April J. Tabor
Acting Secretary

SEAL: