1923126

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of	**DECISION AND ORDER**
ASCENSION DATA & ANALYTICS, LLC, a limited liability company.	**DOCKET NO. C-4758**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade 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*.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Safeguards Rule and the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

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

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Business" means Respondent or any business that Respondent controls.

B. "Covered Incident" means any instance in which any United States federal, state, or local law or regulation requires a Covered Business to notify any U.S. federal, state, or local government entity that information from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.

C. "Covered Information" means (1) Personally Identifiable Financial Information; and (2) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any Personally Identifiable Financial Information that is not publicly available.

D. "Personally Identifiable Financial Information" means any information:

    1. A consumer provides to obtain a financial product or service;

    2. About a consumer resulting from any transaction involving a financial product or service; or

    3. A Covered Business otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.

E. "Respondent" means Ascension Data & Analytics, LLC, a Delaware limited liability company, and its successors and assigns.

F. "Vendor" means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Information from, by, or at the direction of a Covered Business through its provision of services directly to a Covered Business.

Provisions

I. GLB Rule Violations

IT IS ORDERED that Respondent, and Respondent's officers, agents, employees and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not violate any provision of the Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314, a copy of which is attached hereto as Exhibit A.

II. Mandated Data Security Program

IT IS FURTHER ORDERED that each Covered Business must not transfer, sell, share, collect, maintain, or store Covered Information unless it establishes and implements, and thereafter maintains, a comprehensive data security program ("Data Security Program") that protects the security of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Data Security Program;

B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its Data Security Program at least once every twelve (12) months and promptly after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the Data Security Program;

D. Assess and document, at least once every twelve (12) months and promptly following a Covered Incident, internal and external risks to the security of Covered Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information. Each such assessment must evaluate risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, such as network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

E. Design, implement, maintain, and document safeguards that control the internal and external risks identified in response to sub-Provision II.D. Each safeguard must be based on the volume and sensitivity of the Covered Information at risk, and the likelihood that the risk could be realized and result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information. Each Covered Business's safeguards must also include:

    1. Require each Vendor to:

a. Before the Covered Business provides access to Covered Information:

i. Provide documentation of its information security policies and practices related to protecting any Covered Information that may be obtained from the Covered Business;

ii. Describe in writing how and where the Covered Information will be maintained and what safeguards are in place or will be implemented to protect it;

b. Update in writing the information required by sub-Provision II.E.1.a when there is a material change or at least once every twelve (12) months; and

c. Implement measures to assess the cybersecurity risk to Covered Information obtained from the Covered Business that is stored on the Vendor's networks, if any, and if any is stored, provide documentation to the Covered Business of the scope of the measures and their results, including, at least once every twelve (12) months and promptly after a Covered Incident: (i) vulnerability scanning; and (ii) penetration testing;

2. Maintain all documentation provided by each Vendor pursuant to sub-Provision II.E.1 for a period of five (5) years from when it was provided; and

3. At least once every twelve (12) months, and promptly following a Covered Incident involving a Vendor, conduct written assessments of each Vendor to determine the continued adequacy of their safeguards to control the internal and external risks to the security of Covered Information. The level of the assessment for each Vendor should be commensurate with the risk it poses to the security of Covered Information.

4. Provided, however, that sub-Provisions II.E.1-3 are not required of any Covered Business for a Vendor that receives, maintains, processes, or otherwise is permitted access to only names and/or property addresses, and to no other Covered Information, from, by, or at the direction of the Covered Business.

F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security of Covered Information, and modify the Data Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and promptly following a Covered Incident, and modify the Data Security Program based on the results;

H. Select and retain Vendors capable of safeguarding Covered Information they access through or receive from Covered Businesses, and contractually require Vendors to implement and maintain safeguards for Covered Information; and

I. Evaluate and adjust the Data Security Program in light of any changes to its operations or business arrangements, a Covered Incident, or any other circumstances that each Covered Business knows or has reason to know may have an impact on the effectiveness of the Data Security Program. At a minimum, each Covered Business must evaluate the Data Security Program at least once every twelve (12) months and modify the Data Security Program based on the results.

III. Data Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Data Security Program, Respondent must obtain, for each Covered Business, initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Data Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for ten (10) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must: (1) determine whether each Covered Business has implemented and maintained the Data Security Program required by Provision II of this Order, titled Mandated Data Security Program; (2) assess the effectiveness of each Covered Business's implementation and maintenance of sub-Provisions II.A-I; (3) identify any gaps or weaknesses in the Data Security Program; and (4) identify specific evidence (including, but not limited to documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by a Covered Business's management. The Assessment must be signed by the Assessor and must state that the Assessor conducted an independent review of the Data Security Program, and did not rely solely on assertions or attestations by a Covered Business's management.

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit its initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Ascension Data & Analytics, LLC, FTC File No. 1923126." All subsequent biennial Assessments must be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Data Security Assessments by a Third Party, must:

A. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether the Covered Business has implemented and maintained the Data Security Program required by Provision II of this Order, titled Mandated Data Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-I; or (3) identification of any gaps or weaknesses in the Data Security Program; and

B. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege.

V. Annual Certification

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Data Security Program, Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each Covered Business responsible for each Covered Business's Data Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement,

Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Ascension Data & Analytics, LLC, FTC File No. 1923126."

VI. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, for any Covered Business, within a reasonable time after the date of discovery of a Covered Incident, but in any event no later than ten (10) days after the date the Covered Business first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Ascension Data & Analytics, LLC, FTC File No. 1923126."

VII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision VIII of this Order titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

VIII. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address, and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, and the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by

concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Ascension Data & Analytics, LLC, FTC File No. 1923126."

IX. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order and retain each such record for five (5) years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;

D. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of a Covered Business, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Covered Businesses' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

E. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to a Covered Business's compliance with this Order;

F. For five (5) years from the date created or received, all records, whether prepared by or on behalf of a Covered Business, that address compliance by a Covered Business with this Order or lack thereof; and

G. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

X. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XI. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on December 22, 2041, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than twenty (20) years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Chair Khan not participating, Commissioner Slaughter dissenting.

April J. Tabor
Secretary

SEAL
ISSUED: December 22, 2021