UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of **Gravy Analytics, Inc., a corporation,** **and** **Venntel, Inc., a corporation.**	**DECISION AND ORDER** **Docket No. C-____**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished Respondents 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 Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit 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 Respondents had violated 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

The Respondents are:

a. Respondent Gravy Analytics, Inc., a Delaware corporation with its principal office or place of business at 44679 Endicott Dr Suite 300, Ashburn, VA 20147.

b. Respondent Venntel, Inc., a Delaware corporation with its principal office or place of business at 2201 Cooperative Way, Suite 600, Herndon, Virginia 20171. Venntel is a wholly-owned subsidiary of Gravy Analytics.

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

ORDER

Definitions

For the purpose of this Order, the following definitions apply:

A. "**Affirmative Express Consent**" means any freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by an affirmative action, following a Clear and Conspicuous Disclosure to the individual of: (1) the categories of information that will be collected; (2) the purpose(s) for which the information is being collected, used, or disclosed; (3) the hyperlink to a document that describes the types of entities to whom the Covered Information is disclosed; and (4) the hyperlink to a simple, easily-located means by which the consumer can withdraw consent and that Clearly and Conspicuously describes any limitations on the consumer's ability to withdraw consent. The Clear and Conspicuous Disclosure must be separate from any "privacy policy," "terms of service," "terms of use," or other similar document.

The following does not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or

2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.

B. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

C. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) Location Data; (3) an email address or other online contact information; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) credit or debit card information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; or (10) socio-economic or demographic data. Deidentified information is not Covered Information.

D. "**Data Product**" means any model, algorithm, or derived data, in Respondents' custody or control, developed, in whole or part, using Historic Location Data. Data Product includes but is not limited to any derived data produced via inference (manual or automated) or predictions such as audience segments.

E. **"Deidentified" or "Deidentifiable"** means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Respondents must, at a minimum:

1. Have implemented technical safeguards that prohibit reidentification of the person to whom the information may pertain;

2. Have implemented business processes that specifically prohibit reidentification of the information, including by buyers, customers, or other entities to whom Respondents provide the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified information; and

4. Make no attempt to reidentify the information.

F. **"Historic Location Data**" means any Location Data that Respondents collected from consumers without consumers' Affirmative Express Consent.

G. "**Location Data**" means any data that may reveal a mobile device's or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, cell tower information, or precise location information inferred from basic service set identifiers (BSSIDs), WiFi Service Set Identifiers (SSID) information, or Bluetooth receiver information, and any unique persistent identifier combined with any such data, such as a mobile advertising identifier (MAID) or identifier for advertisers (IDFA). Data that: (1) reveals only a mobile device or consumer's coarse location data (e.g., zip code or census block location with a radius of at least 1,850 feet), or (2) is used for (a) Security Purposes, (b) National Security purposes conducted by federal agencies or other federal entities, or (c) response by a federal law enforcement agency to an imminent risk of death or serious bodily harm to a person, is not Location Data.

H. "**National Security"** means the national defense, foreign intelligence and counterintelligence, international and internal security, and foreign relations. This includes countering terrorism; combating espionage and economic espionage conducted for the benefit of any foreign government, foreign instrumentality, or foreign agent; enforcing export controls and sanctions; and disrupting cyber threats that are perpetrated by nation states, terrorists, or their agents or proxies.

I. "**Raw Format**" means the format in which Location Data is originally supplied, prior to any form of processing, extraction, or analysis taking place.

J. "**Respondents**" means Gravy Analytics, Inc. ("Gravy") and Venntel, Inc. ("Venntel"), and their successors and assigns.

K. "**Security Purposes"** means preventing, detecting, protecting against, or responding to data security incidents, including cybersecurity incidents, identity theft, fraud, phishing, harassment, malicious or deceptive activities, or preserving the integrity or security of systems.

L. "**Sensitive Locations**" means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices;

(5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (8) military installations, offices, or buildings.

M. "**Sensitive Location Data**" means any consumer Location Data associated with a Sensitive Location.

N. "**Third-Party Incident**" means the sharing by a third party of Respondents' Location Data, in violation of a contractual requirement between Respondents and the third party.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondents and Respondents' officers, agents, employees, 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 the advertising, promotion, offering for sale, sale, or distribution of any product or service, must not misrepresent, in any manner, expressly or by implication:

A. The extent to which Respondents review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt in controls;

B. The extent to which Respondents collect, use, maintain, disclose, or delete any Covered Information; and

C. The extent to which the Location Data that Respondents collect, use, maintain, or disclose is Deidentified.

II. Prohibitions on the Use, Sale, or Disclosure of Sensitive Location Data

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, and employees, whether acting directly or indirectly, must not sell, license, transfer, share, disclose, or otherwise use in any products or services Sensitive Location Data associated with the Sensitive Locations that Respondents have identified within 90 days of the effective date of this Order as part of the Sensitive Locations Data Program established and maintained pursuant to Provision III below.

Provided, however, that the prohibitions in this Provision II do not apply if Respondents: (i) use Sensitive Location Data to convert such data into data that (a) is not Sensitive Location Data or (b) is not Location Data; or (ii) have a direct relationship with the consumer related to the Sensitive Location Data, the consumer has provided Affirmative Express Consent, and the Sensitive Location Data is used to provide a service directly requested by the consumer.

III. Sensitive Location Data Program

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must establish and implement, and thereafter maintain, a Sensitive Location Data Program to develop a comprehensive list of Sensitive Locations and to prevent the use, sale, licensing, transfer, sharing, or disclosure of Sensitive Location Data as provided in Provision II above. To satisfy this requirement, Respondents must, at a minimum:

A. Document in writing the components of the Sensitive Location Data Program as well as the plan for implementing and maintaining the Sensitive Location Data Program;

B. Identify a senior officer, such as a Chief Privacy Officer or Chief Compliance Officer, to be responsible for the Sensitive Location Data Program. The senior officer will be approved by and report directly to the board of directors or a committee thereof or, if no such board or equivalent body exists, to the principal executive officer of Respondents;

C. Provide the written program and any evaluations thereof or updates thereto to Respondents' board of directors or governing body or, if no such board or equivalent body exists, to the principal executive officer of Respondents at least every twelve months;

D. Develop and implement procedures to identify Sensitive Locations to be used by Respondents in preventing the sale, license, transfer, use, or other sharing or disclosure of Sensitive Location Data as provided in Provision II above. If a building or place is identified as including both a Sensitive Location and a non-Sensitive Location, Respondents may associate Location Data with the non-Sensitive Location only;

E. Assess, update, and document, at least once every three months, the accuracy and completeness of Respondents' list of Sensitive Locations. Respondents' assessments must include:

    1. Verifying that Respondents' list includes Sensitive Locations known to Respondents;

    2. Identifying and assessing methods, sources, products, and services developed by Respondents or offered by third parties that identify Sensitive Locations;

    3. Updating its list of Sensitive Locations by selecting and using the methods, sources, products, or services developed by Respondents or offered by third parties that are accurate and comprehensive in identifying Sensitive Locations;

    4. Considering new categories of Sensitive Locations, not enumerated in the definition of Sensitive Locations, such as those based on an announcement by a self-regulatory association. Respondents must determine whether to add the newly identified categories to Respondents' list of Sensitive Locations and, as applicable, complete these additions within the time frames specified in Section III.G; and

5. Documenting each step of this assessment, including the reasons Respondents selected the methods, sources, products, or services used in updating Respondents' list of Sensitive Locations.

F. Implement policies, procedures, and technical measures designed to prevent Respondents from using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data as provided in Provision II above, and monitor and test the effectiveness of these policies, procedures, and technical measures at least once every three months. Such testing must be designed to verify that Respondents are not using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data;

G. Initiate the process of deleting or rendering non-sensitive Sensitive Location Data associated with locations included in the list developed pursuant to Subparts D and E, within 2 days of adding the location to the list of Sensitive Locations, and complete the process within 30 days of initiation, except where retention is needed to fulfill an allowed purpose as provided in Provision II above. The time period to complete this process may be extended by additional 30 days periods (not to exceed 90 total days) when reasonably necessary, provided the Respondents document at each interval, the reasons for the extension and the progress made, and Respondents must not use, provide access to, or disclose Sensitive Location Data during the process of deleting or rendering non-sensitive, for any other purpose; and

H. Evaluate and adjust the Sensitive Location Data Program in light of any changes to Respondents' operations or business arrangements, or any other circumstance that Respondents know or have reason to know may have an impact on the Sensitive Location Data Program's effectiveness. At a minimum, Respondents must evaluate the Sensitive Location Data Program every twelve months and implement modifications based on the results.

IV. Other Location Data Obligations

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must establish and implement and thereafter maintain policies, procedures, and technical measures designed to prevent Respondents or recipients of Respondents' Location Data, for any such Location Data received after the effective date of this Order, from (i) associating such data with (a) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars, and nightlife, or (b) locations of public gatherings of individuals during political or social demonstrations, marches, and protests; or (ii) using such Location Data to determine the identity or the location of an individual's home, i.e., the location of any individual's private residences (e.g., single family homes, apartments, condominiums, townhomes) (together, "Prohibited Uses").

Respondents must identify a senior officer, such as a Chief Privacy Officer or Chief Compliance Officer, to be responsible for these policies, procedures, and technical measures. With respect to recipients of Respondents' Location Data, such policies, procedures, and technical measures shall include:

1. Contractual prohibitions against recipients of Respondents' Location Data from using Respondents' Location Data in whole or in part to associate a specific individual with the locations identified above, and contractual obligations on recipients of Respondents' Location Data requiring such recipients to impose equivalent prohibitions on any third parties to whom the recipient resells, transfers, or discloses Respondent's Location Data in its Raw Format;

   Provided, however, reselling does not include a recipient receiving Location Data on behalf of a designated end user, for which end user Respondents have implemented policies, procedures, and technical measures required by this Provision IV, and the end user has (a) contractually agreed to the prohibitions against reselling; and (b) contractually agreed not to engage in Prohibited Uses;

2. Marking techniques, such as seeding or salting, designed to detect recipients' non-compliance with any contractual prohibitions against resale or re-license of Respondents' Location Data;

3. Assessing and documenting recipients' compliance at least once every twelve months for as long as the recipient retains a copy of Respondents' Location Data; and

4. Terminating relationships with recipients for non-compliance.

V. Third-Party Incident Reports

IT IS FURTHER ORDERED that within 30 days of any Respondent's determination that a Third-Party Incident has occurred, Respondents must submit a report to the Commission. The report must include, to the extent possible:

A. The estimated date range when the Third-Party Incident occurred;

B. A description of the facts relating to the Third-Party Incident, including the causes of the Third-Party Incident, if known, and participants;

C. A description of each type of information that was affected by the Third-Party Incident;

D. The numbers of consumers whose information was affected by the Third-Party Incident;

E. The acts Respondents has taken to date to remediate the Third-Party Incident and protect Covered Information from further exposure or access; and

F. Unless otherwise directed by a Commission representative in writing, Respondents must submit all Third-Party Incident reports to the Commission under penalty of perjury as specified in the Section of this Order titled "Compliance Report and Notices."

VI. Limitations on Collection, Use, Maintenance, and Disclosure of Location Data

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, 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, must not:

A. Collect, use, maintain, or disclose Location Data from devices where a consumer has enabled the mobile operating system privacy settings to opt out of, limit, or otherwise decline targeted advertising or tracking, without a record satisfying the requirements in Provision VII.B, documenting the consumer's consent.

B. Within 90 days of the effective date of this Order, collect, use, maintain, or disclose an individual's Location Data without a record satisfying the requirements in Provision VII.B, documenting the consumer's consent obtained prior to Respondents' collection or use of Location Data.

VII. Supplier Assessment Program

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must implement a program designed to ensure that consumers have provided consent for the collection and use of all data that may reveal a mobile device or consumer's precise location, obtained by Respondents, including by implementing and maintaining a "Supplier Assessment Program." In connection with the Supplier Assessment Program, Respondents must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Supplier Assessment Program;

B. Conduct an initial assessment either within 30 days of a third party entering into data sharing agreements with Respondents (or, for parties with existing data-sharing agreements, within 30 days of the effective date of this Order) or within 30 days of the initial date of data collection from such a third party, and thereafter annually, designed to confirm that consumers provide Affirmative Express Consent if feasible or to confirm that consumers specifically consent to the collection, use, and disclosure of all data that may reveal a mobile device or a consumer's precise location;

C. Create and maintain records of the suppliers' responses obtained by Respondents under the Supplier Assessment Program; and

D. Cease from using, selling, licensing, transferring, or otherwise sharing or disclosing all data that may reveal a mobile device or consumer's precise location for which consumers have not provided consent, as provided in Provision VII.B above.

VIII. Disclosures to Consumers

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, 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, must provide a Clear and

Conspicuous means for consumers to request the identity of any entity, business, or individual as to which Respondents have knowledge that consumers' Location Data was sold, transferred, licensed, or otherwise disclosed. Respondents may require consumers to provide Respondents with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

Provided however, that the Disclosure requirements in this Provision VIII do not apply if Respondents provide consumers with a Clear and Conspicuous method to submit a request to delete their Location Data from the commercial databases of all recipients of such Location Data, expressly instruct (or contractually require) such recipients to honor such requests sent or made available to them by Respondents, expressly request (or contractually demand) written confirmation of deletion of the identified Location Data, and provide consumers with written confirmation of such deletion requests or instructions sent to recipients and written confirmation of deletion from recipients (where confirmed), no later than 90 days after the receipt of consumers' requests. Respondents may require consumers to provide Respondents with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

IX. Withdrawing Consent

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, 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, must provide a simple, easily-located means for consumers to withdraw consent to Respondents' use or disclosure of their device's Location Data. Such means may include a Clear and Conspicuous notice or link to an applicable operating system or device setting. Respondents may require consumers to provide Respondents with information necessary to complete such requests, but Respondents must not use, provide access to, or disclose any information collected for such a request for any other purpose.

X. Obligations When Consent is Withdrawn

IT IS FURTHER ORDERED that Respondents, and Respondents' officers, agents, employees, 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, must cease using and disclosing all Location Data associated with a specific device within 15 days after Respondents receive notice that the consumer has withdrawn their consent through the means required by Provision IX.

XI. Location Data Deletion Requests

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, 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, must implement and maintain a simple and Clear and Conspicuous means for consumers to request that Respondents delete

Location Data that Respondents previously collected about their mobile device, and delete such Location Data within 30 days of receipt of such request unless a shorter period for deletion is required by law. Respondents shall create and maintain a process by which a deletion request provided to one Respondent is treated as notice to both Respondents. Respondents may require consumers to provide Respondents with information necessary to complete such requests, but must not use, provide access to, or disclose any information collected for a deletion request for any other purpose.

XII. Data Retention Limits

IT IS FURTHER ORDERED that Respondents, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 60 days of the effective date of this Order, document, adhere to, and make publicly available through a link on the home page of their website(s), in a manner that is Clear and Conspicuous, a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information;

B. Within 60 days of the effective date of this Order, Respondents shall provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s); and

C. Prior to collecting or using any new type of information related to consumers that was not being collected as of the issuance date of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision entitled Data Retention Limits, Respondents must update its retention schedule setting forth: (1) the purpose or purposes for which the new information is collected; (2) the specific business needs for retaining the new information; and (3) a set timeframe for deletion of the new information that precludes indefinite retention.

XIII. Deletion

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, 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, must, unless prohibited by law:

A. Within 60 days after the effective date of this Order, delete or destroy all Historic Location Data, and provide a written statement to the Commission, pursuant to Provision XVI.D, confirming that all such information has been deleted or destroyed;

B. Within 90 days after the effective date of this Order, (i) inform Respondents' customers that received Historic Location Data within 3 years prior to the issuance date of this Order, of the FTC's requirement in Provision XIII.A that the FTC requires such data to be deleted, Deidentified, or rendered non-sensitive, and (ii) Respondents shall promptly submit, within 10 days of sending to its customers, all such notices to the Commission under penalty of perjury as specified in the Provision of this Order titled "Compliance Report and Notices"; and

C. Within 90 days after the effective date of this Order, delete or destroy all Data Products, and provide a written statement to the Commission, pursuant to Provision XVI.D, confirming such deletion or destruction.

Provided however, Respondents shall have the option to retain Historic Location Data and related Data Products if Respondents have obtained records in accordance with Provision VII showing that consumers consented to the collection, use, and disclosure of their Historic Location Data within 90 days after the effective date of this Order, or if within such time period Respondents ensure such Historic Location Data and Data Product is Deidentified or rendered non-sensitive in accordance with Provision III, and provided that the Historic Location Data and Data Product is subject to the obligations in Provision IV.

XIV. Mandated Privacy Program

IT IS FURTHER ORDERED that Respondents, and any business that Respondents control directly or indirectly, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within 60 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program (the "Program") that protects the privacy of such Covered Information. To satisfy this requirement, Respondents must at a minimum do the following:

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

B. Provide the written program, and any evaluations thereof or updates thereto to Respondents' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondents responsible for the Program at least once every 12 months;

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

D. Assess and document, at least once every 12 months, internal and external risks to the privacy of Covered Information that could result in the unauthorized collection, maintenance, use, disclosure of, or provision of access to Covered Information.

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondents identify to the privacy of Covered Information identified in response to Provision XIV.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk

could be realized and result in the unauthorized collection, maintenance, use, disclosure of, or provision of access to Covered Information.

F. On at least an annual basis, provide privacy training programs for all employees and independent contractors responsible for handling or who have access to Covered Information, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;

G. Test and monitor the effectiveness of the safeguards at least once every 12 months, and modify the Program based on the results; and

H. Evaluate and adjust the Program in light of any changes to Respondents' operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in Provision XIV.D of this Order, or any other circumstances that Respondents know or have reason to believe may have an impact on the effectiveness of the Program or any of their individual safeguards. At a minimum, Respondents must evaluate the Program at least once every 12 months and modify the Program based on the results.

XV. Acknowledgments of the Order

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

A. Respondents, within 10 days after the effective date of this Order, must submit to the Commission acknowledgments of receipt of this Order sworn under penalty of perjury.

B. For 5 years after the issuance date of this Order, Respondents 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 this Order, and all agents and representatives having managerial responsibilities for the conduct related to the subject matter of this Order; and (3) any business entity resulting from any change in structure as set forth in Provision XVI titled Compliance Report and Notices. Delivery must occur within 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 Respondents delivered a copy of this Order, Respondents must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XVI. Compliance Report and Notices

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

A. One year after the issuance date of this Order, each of the Respondents must submit a compliance report, sworn under penalty of perjury, in which the Respondents must:

(1) 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 Respondents; (2) identify all of the Respondents' businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how the Respondents are in compliance with each Provision of this Order, including a discussion of all of the changes the Respondents made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. The Respondents must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of the Respondents or any entity that Respondents have 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. The Respondents must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against either Respondent within 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 Gravy Analytics, Inc. & Venntel, Inc., FTC File No. 212-3035.

XVII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 5 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, Respondents must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services, 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 of all consumer complaints that relate to the collection, use, maintenance, or disclosure of Covered Information, whether received directly or indirectly, such as through a third party, and any response;

D. For 5 years from the date received, copies of communications from law enforcement, if such communications request information or documents relating to Respondents' compliance with this Order;

E. A copy of each widely disseminated representation by either of the Respondents that describes the extent to which Respondents (i) review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt-in controls; (ii) the extent to which Respondents collect, use, maintain, disclose, or delete any Covered Information; and (iii) the extent to which the Location Data that Respondents collect, use, maintain, or disclose is Deidentified;

F. Records showing that Respondents have met the consent requirements set forth in Provision XIII for retaining Historic Location Data;

G. Records showing the Respondents' implementation of Supplier Assessment Program required by Provision VII;

H. Records showing Respondents' implementation of the Sensitive Location Data Program required by Provision III;

I. Records showing Respondents' processing of consumer deletion requests as provided in Provision VIII; and

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

XVIII. Compliance Monitoring

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

A. Within 14 days of receipt of a written request from a representative of the Commission, the Respondents 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 Respondents. Respondents must permit representatives of the Commission to interview anyone affiliated with Respondents 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 Respondents or any individual or entity affiliated with Respondents, 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.

XIX. 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 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 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 20 years;

B. This Order's application to any Respondents that are 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 Respondents 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.

April J. Tabor
Secretary

SEAL:
ISSUED: