UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

In the Matter of **1HEALTH.IO INC., a corporation, also d/b/a VITAGENE, INC.**	**FILE NO. 1923170** **AGREEMENT CONTAINING CONSENT ORDER**

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of 1Health.io Inc., also doing business as Vitagene, Inc. and Vitagene, a corporation ("Proposed Respondent"). The Commission's Bureau of Consumer Protection ("BCP") has prepared a draft of an administrative Complaint ("draft Complaint"). BCP and Proposed Respondent, individually or through its duly authorized officers, enter into this Agreement Containing Consent Order ("Consent Agreement") to resolve the allegations in the attached draft Complaint through a proposed Decision and Order to present to the Commission, which is also attached and made a part of this Consent Agreement.

IT IS HEREBY AGREED by and between Proposed Respondent and BCP, that:

1. The Proposed Respondent is 1Health.io Inc., also doing business as Vitagene, Inc. and Vitagene ("Vitagene"), a Delaware corporation with its principal office or place of business at 201 Spear Street, Suite 1100, San Francisco, California 94105. Proposed Respondent changed its name from Vitagene, Inc. to 1Health.io Inc. in October 2020.

2. Proposed Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondent admits the facts necessary to establish jurisdiction.

3. Proposed Respondent waives:

   a. Any further procedural steps;

   b. The requirement that the Commission's Decision contain a statement of findings of fact and conclusions of law; and

   c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.

4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the draft Complaint, will be placed on the public record for thirty (30) days and information about them publicly released. Acceptance does not constitute final approval, but it serves as the basis for further actions leading to final disposition of the matter.

Thereafter, the Commission may either withdraw its acceptance of this Consent Agreement and so notify the Proposed Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and serve its Complaint (in such form as the circumstances may require) and decision in disposition of the proceeding, which may include an Order. *See* Section 2.34 of the Commission's Rules, 16 C.F.R. § 2.34 ("Rule 2.34").

5. If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Proposed Respondent: (1) issue its Complaint corresponding in form and substance with the attached draft Complaint and its Decision and Order and (2) make information about them public. Proposed Respondent agrees that service of the Order may be effected by its publication on the Commission's website (ftc.gov), at which time the Order will become final. *See* Rule 2.32(d). Proposed Respondent waives any rights it may have to any other manner of service. *See* Rule 4.4.

6. When final, the Decision and Order will have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other Commission orders.

7. The Complaint may be used in construing the terms of the Decision and Order. No agreement, understanding, representation, or interpretation not contained in the Decision and Order or in this Consent Agreement may be used to vary or contradict the terms of the Decision and Order.

8. Proposed Respondent agrees to comply with the terms of the proposed Decision and Order from the date that Proposed Respondent signs this Consent Agreement. Proposed Respondent understands that it may be liable for civil penalties and other relief for each violation of the Decision and Order after it becomes final.

1HEALTH.IO INC., D/B/A VITAGENE, INC.

By:_____
Mehdi Maghsoodnia
Chief Executive Officer

Date:_____

FEDERAL TRADE COMMISSION

By:_____
James Trilling
Attorney, Bureau of Consumer Protection

By:_____
Elisa Jillson
Attorney, Bureau of Consumer Protection

APPROVED:

Jason R. Parish Jonathan D. Janow Buchanan Ingersoll & Rooney PC Attorneys for Proposed Respondent	Ben Wiseman Acting Associate Director Division of Privacy and Identity Protection
	Samuel Levine Director Bureau of Consumer Protection
Date:	Date:

1923170

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Lina M. Khan, Chair
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of **1HEALTH.IO INC., a corporation, also d/b/a VITAGENE, INC.**	**DECISION AND ORDER** **DOCKET NO. C-**

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 Act.

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 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 thirty (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 1Health.io Inc., also d/b/a Vitagene, Inc. and Vitagene ("Vitagene"), a Delaware corporation with its principal office or place of business at 201 Spear Street, Suite 1100, San Francisco, California 94105. Respondent changed its name from Vitagene, Inc. to 1Health.io Inc. in October 2020.

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. "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 a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of: (1) each category of Personal Information that Respondent will disclose to third parties; (2) the specific purpose(s) for the disclosures of each category of Personal Information; (3) each category of third party to which such disclosures will be made; (4) a simple, easily-located means for the consumer to withdraw consent; (5) any limitations on the consumer's ability to withdraw consent; and (6) all other information material to the provision of consent. The Clear and Conspicuous disclosure must be separate from any "privacy policy," "terms of service," "terms of use," "consent for research," or other similar document.

   The following do 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 substantial effect of subverting or impairing user autonomy, decision-making, or choice.

B. "Clear and Conspicuous" 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 Customer" means any customer identified by Respondent as having had potentially exposed as of July 1, 2019, his or her Health Information that Respondent stored in the Amazon Web Services Simple Storage Service Datastore.

D. "Covered Incident" means any incident: (1) that results in Respondent notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization; or (2) in which Health Information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

E. "Covered Service Provider" means a person or entity that (i) uses or receives Health Information collected by or on behalf of Respondent for and at the direction of Respondent and no other individual or entity; (ii) does not disclose the Health Information, or any individually identifiable information derived from it, to an individual or entity other than Respondent; and (iii) does not use the Health Information for any purpose other than performing the services specified in the Covered Service Provider's contract with Respondent. Covered Service Provider

includes any subcontractor to such Covered Service Provider bound by contract to data processing terms no less restrictive than the terms to which the Covered Service Provider is bound.

F. "Health Information" means individually identifiable information relating to the health or genetics of an individual, including information: (1) concerning the propensity of that individual to develop a health condition; (2) concerning an analysis of the individual's DNA, RNA, chromosomes, proteins, or metabolites, in whole or in part; or (3) relating to the past, present, or future physical or mental health or conditions of an individual or the provision of health care to an individual.

G. "Personal Information" means information from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as a user identifier or a screen name; (4) a telephone number; (5) a financial account number; (6) credit or debit card information; (7) 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 (8) Health Information.

H. "Respondent" means 1Health.io Inc., also d/b/a Vitagene, Inc. and Vitagene, a corporation, and its successors and assigns.

I. "Third Party" means any individual or entity other than: (1) a payment processor, laboratory, insurance company, insurance verification provider, hospital, or healthcare provider that Respondent has contractually obligated to limit the use and retention of Health Information to that which is directed by the individual who is identifiable by the Health Information; (2) an individual or entity to which Respondent discloses Health Information consistent with the Health Information Portability and Accountability Act ("HIPAA") of 1996, Pub. L. 104-191, 110 Stat. 1936, to the extent that HIPAA applies to the Health Information; (3) a Covered Service Provider; (4) an individual or entity to which Respondent discloses Health Information at the written direction of a customer who has obtained consent for that disclosure from the individual who is identifiable by the Health Information; or (5) an entity that purchases assets that include Health Information collected by Respondent, *provided, however*, that Health Information is not sold to the purchasing entity as a stand-alone asset, Respondent does not sell any Health Information to more than one purchasing entity, and the purchasing entity agrees by contract with the selling entity to be bound by: (a) Respondent's privacy policy in effect when such Health Information was collected and agrees to obtain Affirmative Express Consent of the individual who is identifiable by the Health Information before applying to the Health Information any policies or practices that are material changes from such privacy policy; and (b) the requirements set forth in Provision II of this Order, including the exclusions set forth within this definition.

Provisions

I. Prohibition against Misrepresentations

IT IS ORDERED that Respondent; Respondent's officers, agents, and 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 any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent meets or exceeds industry-standard security or privacy practices;

B. The extent to which Respondent stores any Health Information with any other element of Personal Information;

C. The extent to which, or the purposes for which, Respondent collects, uses, discloses, maintains, deletes, or destroys a consumer's: (1) physical DNA sample or (2) Personal Information upon request;

D. The extent to which Respondent is a member of, adheres to, complies with, is certified by, or otherwise participates in any privacy or security program sponsored by a government entity or any third party, including any self-regulatory or standard-setting organization;

E. The extent to which Respondent otherwise protects the privacy, security, availability, confidentiality, or integrity of Personal Information; or

F. The extent to which Respondent has received approval or authorization for its claims, products, or services from any government agency.

II. Affirmative Express Consent for Disclosure of Health Information to Third Parties

IT IS FURTHER ORDERED that Respondent; Respondent's officers, agents, and 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, shall not, unless required by law, disclose to any Third Party any Health Information unless Respondent obtains the Affirmative Express Consent of the individual who is identifiable by the Health Information.

III. Destruction of Saliva Samples

IT IS FURTHER ORDERED that, on or before thirty (30) days after the issuance of this Order, Respondent and Respondent's officers, agents, and employees must:

A. Instruct any laboratory that collected physical DNA saliva samples pursuant to a contract with Respondent to destroy any such sample that the laboratory has retained for more than 180 days after Respondent accepted the results of the laboratory's analysis of the sample;

and

B. Provide a written statement to the Commission, sworn under penalty of perjury, confirming that Respondent has given such instructions, and append to that statement true and correct copies of any such written instructions.

IV. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, and any business that Respondent controls directly, or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Personal Information, must, within sixty (60) days of issuance of this order, establish and implement, and thereafter maintain, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondent must, at a minimum:

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

B. Provide the written program and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

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

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the: (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of Personal Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision IV.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of Personal Information. Such safeguards must also include:

1. Policies, procedures, and technical measures to systematically inventory Personal Information in Respondent's control;

2. Policies, procedures, and technical measures to log and monitor access to repositories of Personal Information in Respondent's control;

3. Data access controls for all repositories of Personal Information in Respondent's control, such as: (a) restricting inbound connections to approved IP addresses and (b) requiring authentication to access them; and

4. Encryption, or at least equivalent protection, of all Health Information in Respondent's control that is reasonably linkable to an individual consumer, computer, or device, including in transit and at rest. To the extent that Respondent satisfies this requirement with at least equivalent protection rather than encryption, such protection shall be reviewed and approved by the qualified employee or employees designated to coordinate and be responsible for the Information Security Program;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after a Covered Incident, and penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Personal Information; and

I. Evaluate and adjust the Information Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision IV.D of this Order, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

V. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision IV of this Order, titled Mandated Information Security Program, Respondent must obtain 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 Information 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. The assessor may not withhold any documents from the Commission on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory protection, 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, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his 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 two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

1. Determine whether Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program;

2. Assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions IV.A-I;

3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

5. Identify specific evidence (including 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: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds

one or more safeguards required under Provision IV of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

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 an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure 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 1Health.io Inc., FTC File No. 1923170." Respondent must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

VI. 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 V of this Order, titled Information Security Assessments by a Third Party, must:

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

B. Provide or otherwise make available to the Assessor information about Respondent's network(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. 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 Respondent has implemented and maintained the Information Security Program required by Provision IV of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IV.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

VII. Annual Certification

IT IS FURTHER ORDERED that, 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 Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent 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 all Covered Incidents during the certified period. 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 1Health.io Inc., FTC File No. 1923170."

VIII. Covered Incident Reports

IT IS FURTHER ORDERED that, within: (1) ten (10) days of any notification to a United States federal, state, or local government entity of a Covered Incident; or (2) ten (10) business days of discovery that individually identifiable Health Information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization, Respondent 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 was affected by the Covered Incident;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Personal 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 any materially different notice sent by Respondent 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 1Health.io Inc., FTC File No. 1923170."

IX. Monetary Relief

IT IS FURTHER ORDERED that:

A. Respondent must pay to the Commission $75,000.

B. Such payment must be made within eight (8) days of the effective date of this Order by electronic fund transfer in accordance with instructions provided by a representative of the Commission.

X. Additional Monetary Provisions

IT IS FURTHER ORDERED that:

A. Respondent relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission to enforce its rights to any payment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.

C. The facts alleged in the Complaint establish all elements necessary to sustain an action by or on behalf of the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.

D. All money paid to the Commission pursuant to this Order may be deposited into a fund administered by the Commission or its designee to be used for relief, including consumer redress and any attendant expenses for the administration of any redress fund. If a representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after redress is completed, the Commission may apply any remaining money for such other relief (including consumer information remedies) as it determines to be reasonably related to Respondent's practices alleged in the Complaint. Any money not used is to be deposited to the U.S. Treasury. Respondent has no right to challenge any activities pursuant to this Provision.

E. In the event of default on any obligation to make payment under this Order, interest, computed as if pursuant to 28 U.S.C. § 1961(a), shall accrue from the date of default to the date of payment. In the event such default continues for ten (10) days beyond the

date that payment is due, the entire amount will immediately become due and payable.

F. Each day of nonpayment is a violation through continuing failure to obey or neglect to obey a final order of the Commission and thus will be deemed a separate offense and violation for which a civil penalty shall accrue.

G. Respondent acknowledges that its Taxpayer Identification Numbers (Social Security or Employer Identification Number), which Respondent has previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

XI. Customer Information

IT IS FURTHER ORDERED that Respondent must directly or indirectly provide sufficient customer information to enable the Commission to efficiently administer consumer redress to all Covered Customers. Respondent represents that it has provided this redress information to the Commission. If a representative of the Commission requests in writing any information related to redress, Respondent must provide it, in the form prescribed by the Commission representative, within fourteen (14) days.

XII. 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, agents, and representatives having managerial responsibilities for 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 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.

XIII. Compliance Reports and Notices

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

A. Ninety (90) days after entry of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, describing in detail its compliance with Provision III of this Order, titled Destruction of Saliva Samples. The report shall include, for each laboratory that Respondent instructed to destroy physical DNA saliva samples, a statement setting forth in detail the laboratory's response to Respondent, if any, including, but not limited to, whether the laboratory destroyed such saliva samples and, if not, why the laboratory did not destroy such saliva samples, to the extent that the laboratory provided such information to Respondent.

B. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent 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 Respondent; (2) identify all of Respondent's 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, what Personal Information is collected, and the means of advertising, marketing, and sales; (4) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the material changes Respondent 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.

C. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) 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; or (3) ownership of Respondent's assets where such assets include Health Information, even if such change in ownership does not otherwise require the submission of a compliance notice.

D. 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.

E. 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.

F. 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 1Health.io Inc., FTC

File No. 1923170."

XIV. 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, the costs incurred in generating those revenues, and resulting net profit or loss;

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 concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to privacy, security, availability, confidentiality, or integrity of Personal Information;

E. A sample copy of each different document relating to any attempt by Respondent to obtain the Affirmative Express Consent of consumers and copies of any documents demonstrating such consent provided by consumers, as required by Part II of this Order;

F. 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 Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and

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

XV. 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 any 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.

XVI. 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 twenty (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 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.

Secretary

SEAL:
ISSUED:

Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of 1Health.io Inc.,* File No. 1923170**

The Federal Trade Commission ("Commission" or "FTC") has accepted, subject to final approval, an agreement containing a consent order from 1Health.io Inc. (formerly known as, and doing business as, Vitagene, Inc.) ("Vitagene").

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.

Since 2015, Vitagene has sold "DNA Health Test Kits" to consumers. In each DNA Health Test Kit, Vitagene instructs the consumer to provide a saliva sample by mail. Vitagene contracts with a testing lab to analyze the sample and map a portion of the consumer's genetic code.

Vitagene combines the testing lab's DNA analysis with the consumer's answers to an online "health questionnaire" that probes the individual's health history, lifestyle, and family health history. Using this information, Vitagene generates reports about the consumer's health and wellness ("Health Reports") and ancestry. Vitagene also sells to the consumer Health Reports that it creates by using the consumer's answers to an online "lifestyle questionnaire" and raw DNA data that the consumer sends to Vitagene after the consumer has obtained DNA tests from certain companies other than Vitagene. The retail cost for a package that includes a Health Report has ranged from $29 to $259, with higher-priced packages including add-ons such as subscriptions to personalized vitamin packs and nutritional coaching.

The Health Reports that Vitagene creates contain numerous facts about the consumer's genetics and health. For example, one type of Health Report first lists the consumer's name, date of birth, and referring doctor or dietician, and then identifies salient genotype data, pertinent questionnaire answers, and, based on the genotype data and questionnaire answers, the level of risk for having or developing certain health conditions, such as high LDL cholesterol, high triglycerides, obesity, or blood clots.

As part of its information technology infrastructure, Vitagene stores consumers' health and genetic information in the Amazon Web Services ("AWS") Simple Storage Service (the "Amazon S3 Datastore") in virtual containers, called "buckets." The files Vitagene has stored in Amazon S3 Datastore buckets include, among other things, consumers' Health Reports; genotype data called single-nucleotide polymorphisms ("SNPs"), which are the most common type of genetic variation among people; and other raw genotype data.

The proposed complaint alleges that, despite the fact that Vitagene has stored consumers' sensitive personal information in the Amazon S3 Datastore, Vitagene did not uniformly apply basic safeguards to the data in each of its Amazon S3 Datastore buckets. In particular, the proposed complaint alleges that, in or about 2016, Vitagene created a publicly accessible bucket in which the company stored Health Reports for at least 2,383 consumers and a publicly

accessible bucket in which it stored raw genetic data (sometimes accompanied by first name) for at least 227 consumers. The proposed complaint alleges that Vitagene's failure to use access controls to restrict access to this sensitive data, encrypt it, log or monitor access to it, or inventory it, to help ensure ongoing security resulted in Vitagene publicly exposing the data until July 2019. According to the proposed complaint, between July 2017 and June 2019, Vitagene received at least three warnings that it was storing consumers' unencrypted health, genetic, and other personal information in publicly accessible buckets.

The proposed complaint alleges that Vitagene changed its name from Vitagene, Inc. to 1Health.io Inc. in October 2020. According to the proposed complaint, the company published revised privacy policies in April and December 2020 that apply to all of the company's customers, including those who purchased products and services from the company solely before April 2020. The proposed complaint alleges that, compared to Vitagene's previous privacy policy, the company's 2020 privacy policies significantly expand the types of third parties with whom, and the purposes for which, the company may share consumers' sensitive personal information. The company did not provide direct notice to consumers of the change, but it also did not implement the expanded sharing.

The proposed five-count complaint alleges that Vitagene violated Section 5(a) of the FTC Act by misrepresenting the company's data security and privacy practices, and by unfairly making material retroactive changes to the company's policies regarding third-party sharing of sensitive personal information.

Proposed complaint Count I alleges that Vitagene deceived consumers by misrepresenting that it exceeded industry-standard security practices. On a webpage that Vitagene devoted to describing its privacy practices, Vitagene claimed that "[w]e use the latest technology and exceed industry-standard security practices to protect your privacy." The proposed complaint alleges that Vitagene's public exposure of consumers' Health Reports, raw genetic data, and other personal information in AWS S3 buckets until July 2019 contradicted this claim.

Proposed complaint Count II alleges that Vitagene deceptively claimed on multiple webpages that it stored consumers' DNA results without name or any other common identifying information. The proposed complaint alleges that this claim was deceptive because Vitagene stored consumers' DNA results with their names and other common identifying information.

Proposed complaint Count III alleges that Vitagene deceptively claimed that it would remove all of a consumer's information if the consumer requested deletion of his or her data. Vitagene made this claim on a webpage that Vitagene devoted to describing its privacy practices. The proposed complaint alleges that the claim was deceptive because, from approximately 2016 through July 1, 2019, Vitagene's lack of a data inventory made it impossible for the company to search comprehensively in response to consumers' requests for Vitagene to delete their data.

Proposed complaint Count IV alleges that Vitagene deceived consumers by claiming on multiple webpages that it destroys consumers' physical DNA saliva samples shortly after analysis of them. The proposed complaint alleges that this claim was deceptive because, beginning in approximately December 2016, Vitagene did not have a contract provision with its genotyping laboratory partner requiring such destruction.

Proposed complaint Count V alleges that it was unfair for Vitagene to post on its websites in April and December 2020 revised privacy policies that describe materially expanded practices for the company's sharing of consumers' sensitive health and genetic information with third parties—including the information of consumers who purchased products and services from Vitagene solely before April 2020—without taking any additional steps to notify consumers or obtain consumers' consent.

The proposed order contains provisions to address Vitagene's conduct and prevent it from engaging in the same or similar acts or practices in the future.

Part I of the proposed order prohibits Vitagene from misrepresenting (1) the extent to which it meets or exceeds industry-standard security or privacy practices, (2) the extent to which it stores any Health Information (as defined in the order) with any other element of Personal Information (as also defined in the order), (3) the extent to which, or the purposes for which, it collects, uses, discloses, maintains, deletes, or destroys a consumer's (i) physical DNA sample or (ii) Personal Information upon request, (4) it is a member of, adheres to, complies with, is certified by, or otherwise participates in, any privacy or security program sponsored by a government entity or third party, (5) the extent to which it otherwise protects the privacy, security, availability, confidentiality, or integrity of Personal Information, or (6) it has received approval or authorization for its claims, products, or services from any government agency.

Part II prohibits Vitagene from disclosing Health Information to any Third Party (as defined in the order) unless the company obtains the Affirmative Express Consent (as also defined in the order) of the individual who is identifiable by the Health Information.

Part III requires Vitagene to instruct any laboratory that collected physical DNA samples pursuant to a contract with Vitagene to destroy any such sample that the laboratory retained for more than 180 days after Vitagene accepted the results of the analysis of the sample.

Part IV requires Vitagene to establish, implement, and maintain a comprehensive information security program that protects the security, confidentiality, and integrity of Personal Information. Part V requires Vitagene to obtain initial and biennial data security assessments from a third-party assessor for twenty years.

Part VI requires Vitagene to disclose all material facts to the assessor and prohibits Vitagene from misrepresenting any fact material to the assessments required by Part V. Part VII requires Vitagene to submit to the Commission an annual certification that Vitagene 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 VIII requires Vitagene to submit a report to the Commission if it discovers any Covered Incident (as defined in the order).

Part IX requires Vitagene to pay $75,000 in monetary relief. Part X provides that the Commission may use Vitagene's monetary relief payment to provide, and pay expenses related to the administration of, consumer redress. Part XI requires Vitagene to provide the Commission customer information to enable the Commission to efficiently administer consumer redress.

Parts XII-XV are reporting and compliance provisions. Part XII requires Vitagene to acknowledge receipt of the order and distribute it to persons with responsibilities relating to the subject matter of the order. Part XIII requires Vitagene to submit an initial compliance report to the Commission and notify the Commission of changes in Vitagene's corporate status. Part XIV requires Vitagene to create and retain certain documents relating to its compliance with the order. Part XV requires that Vitagene provide the Commission additional information or compliance reports, as requested.

Part XVI 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.