**1723118**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

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

**In the Matter of**

**RETINA-X STUDIOS, LLC, a limited liability company, and**

**JAMES N. JOHNS, JR., individually and as sole member of RETINA-X STUDIOS, LLC.**

**DECISION AND ORDER**

**DOCKET NO. C-4711**

## DECISION

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

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

## Findings

1. The Respondents are:

    a. Respondent Retina-X Studios, LLC, a Florida limited liability company with its principal place of business at 731 Duval Station Road, Suite 107, Box 203, Jacksonville, Florida 32218.

    b. Respondent James N. Johns, Jr. the registered agent and sole member of Respondent Retina-X Studios, LLC. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of Retina-X Studios, LLC. His principal place of business is the same as that of Retina-X Studios, LLC.

2. 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. "Child" or "Children" means an individual under the age of 13.

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 is made in 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 representation that requires the disclosure 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. "Collects" or "Collection" means, for the purposes of Provision III of this Order, the gathering of any Personal Information from a Child by any means, including but not limited to:

1. Requesting, prompting, or encouraging a Child to submit Personal Information online;

2. Enabling a Child to make Personal Information publicly available in identifiable form; or

3. Passive tracking of a Child online.

D. "Covered Business" means Corporate Respondent, any business that Corporate Respondent controls, directly or indirectly, and any business that Individual Respondent controls, directly or indirectly.

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

F. "Disclose" or "Disclosure" means, with respect to Personal Information:

1. The release of Personal Information Collected by an operator from a Child in identifiable form for any purpose, except where an operator provides such information to a person who provides Support for the Internal Operations of the Web Site or Online Service; and

2. Making Personal Information Collected by an operator from a Child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

G. "Internet" means collectively the myriad of computer and telecommunication facilities, including equipment and operating software, which comprises the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

H. "Jailbreak(ing) or Root(ing)" includes any action that bypasses a restriction by the Mobile Device manufacturer or operating system.

I. "Mobile Device" means any portable computing device that operates using a mobile operating system, including but not limited to, any smartphone, tablet, wearable, or sensor, or any periphery of any portable computing device.

J. "Monitoring Product or Service" means any software application, program, or code that that can be installed on a user's Mobile Device to track or monitor that user's activities on the Mobile Device, including but not limited to, the user's text messages, web browser history, geolocation, and photos.

K. "Online Contact Information" means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat identifier.

L. "Operator" means any person who operates a Web site located on the Internet or an online service and who Collects or maintains Personal Information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is Collected or maintained, or offers products or services for sale through the Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States, or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation.

M. "Parent" includes a legal guardian.

N. "Person" means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

O. "Personal Information" means individually identifiable information from or about an individual consumer, including:

1. A first and last name;

2. A home or other physical address;

3. An email address;

4. A telephone number;

5. A Social Security number;

6. A driver's license or other government issues identification number;

7. A financial account number;

8. Credit or debit card information;

9. Date of birth;

10. Online Contact Information as defined in 16 C.F.R. § 312.2;

11. A screen or user name where it functions in the same manner as Online Contact Information, as defined in 16 C.F.R. § 312.2;

12. A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

13. A photograph, video, or audio file;

14. Geolocation information sufficient to identify street name and name of a city of town; or

15. Information concerning a Child or the parents of that Child that the Operator Collects online from the Child and combines with an identifier described in this section.

P. "Respondents" means Corporate Respondent and Individual Respondent, individually, collectively, or in any combination.

1. "Corporate Respondent" means Retina-X Studios, LLC, and its successors and assigns.

2. "Individual Respondent" means James N. Johns, Jr.

Q. "Support for the Internal Operations of the Web Site or Online Service" means:

1. Those activities necessary to:

    a. Maintain or analyze the functioning of the Web site or online service;

    b. Perform network communications;

    c. Authenticate users of, or personalize the content on, the Web site or online service;

    d. Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

    e. Protect the security or integrity of the user, Web site, or online service;

    f. Ensure legal or regulatory compliance; or

    g. Fulfill a request of a Child as permitted by 16 C.F.R. §§ 312.5(c)(3) and (4).

2. So long as the information Collected for the activities listed in paragraphs (1)(a) – (g) of this definition is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

R. "Web site or online service directed to Children" means a commercial Web site or online service, or portion thereof, that is targeted to Children.

1. In determining whether a Web site or online service, or a portion thereof, is directed to Children, the Commission will consider its subject matter, visual content, user of animated characters or Child-oriented activities and incentives, music or other audio content, age of models, presence of Child celebrities or celebrities who appeal to Children, language or other characteristics of the Web site or online service, we well as whether advertising promoting or appearing on the Web site or online service is directed to Children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

2. A Web site or online service shall be deemed directed to Children when it has actual knowledge that it is Collecting Personal Information directly from users of another Web site or online service directed to Children.

3. A Web site or online service that is directed to Children under this criteria set forth in paragraph (1) of this definition, but that does not target Children as its primary audience, shall not be deemed directed to Children if it:

    a. Does not Collect Personal Information from any visitor prior to Collecting age information; and

    b. Prevents the Collection, use, or disclosure or Personal Information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of 16 C.F.R. Part 312, attached hereto as Appendix A.

4. A Web site or online service shall not be deemed directed to Children solely because it refers or links to a commercial Web site or online service directed to Children by using information location tools, including a directory, index, reference, pointer, or hypertext link

## I. MONITORING PRODUCTS AND SERVICES

**IT IS ORDERED** that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, promoting, selling, or distributing a Monitoring Product or Service unless Respondents comply with the following:

A. **Mobile Device Security:** No Monitoring Product or Service's functionality may require circumventing security protections implemented by the Mobile Device operating system or manufacturer, such as by Jailbreaking or Rooting a Mobile Device.

B. **Registration Attestation and Documentation:** Prior to the sale or distribution of any Monitoring Product or Service, Respondents must obtain:

    a. An express written attestation from the purchaser that it will use the Monitoring Product or Service for legitimate and lawful purposes by authorized users.

        i. The express written attestation must state the legitimate and lawful purpose for which the purchaser is using the device, which may include only the following:

            1. Parent monitoring a minor Child;

            2. Employer monitoring an employee who has provided express written consent to being monitored; or

            3. Adult monitoring another adult who has provided express written consent to being monitored;

ii. Respondents cannot provide purchasers with written attestation language;

iii. Respondents cannot suggest, direct, or otherwise assist, purchasers in submitting fraudulent written attestations; and

b. Documentation proving that the purchaser is an authorized user on the monitored Mobile Device's service carrier account.

C. **Icon Notice:** The Monitoring Product or Service must display an application icon, accompanied by the name of the Monitoring Product or Service adjacent to the application icon. The consumer must be able to click on the application icon to a page on which Respondents present a Clear and Conspicuous notice stating:

i. The name and material functions of the Monitoring Product or Service;

ii. That the Monitoring Product or Service is running on the user's Mobile Device; and

iii. Where and how the user can contact Respondents for additional information, or to resolve an issue of improper installation of the Monitoring Product or Service.

b. Exception to the Icon Notice Requirement:

i. Respondents may program the Monitoring Product or Service to allow the purchaser of the Monitoring Product or Service to disable the Icon Notice only if the purchaser attests, prior to installation, that the purchaser is the legal guardian or parent of a minor Child, and that the Monitoring Software or Product will be installed on a Mobile Device predominantly used by the minor Child.

## II. ADDITIONAL WARNINGS AND NOTICES

**IT IS FURTHER ORDERED** that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, promoting, selling, or distributing Monitoring Products or Services unless Respondents provide the purchaser with the following notices:

A. Home Page Notice: The home page of any Internet website advertising the Monitoring Product or Service must Clearly and Conspicuously provide notice that the Monitoring Product or Service may only be used for legitimate and lawful purposes by authorized users, and that installing or using the Monitoring Product or Service for any other

purpose may violate local, state, and/or federal law. The foregoing notice must be placed such that it can be viewed on the screen first seen by a potential purchaser who lands on the home page.

B. Purchase Page Notice: Respondents may not complete the sale of a Monitoring Product or Service unless Respondents provide the purchaser with Clear and Conspicuous notice the Monitoring Product or Service may only be used for legitimate and lawful purposes by authorized users, and that installing or using the Monitoring Product or Service for any other purpose may violate local, state, and/or federal law.

## III. INJUNCTION CONCERNING THE COLLECTION OF PERSONAL INFORMATION

**IT IS FURTHER ORDERED** that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with being an operator of any Web site or online service directed to Children or of any Web site or online service with actual knowledge that it is Collecting or maintaining Personal Information from a Child, are hereby permanently restrained and enjoined from violating the Children's Privacy Protection Rule, 16 C.F.R. Part 312, including but not limited to failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information from Children.

A copy of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, is attached hereto as Appendix A.

## IV. PROHIBITION AGAINST MISREPRESENTATIONS

**IT IS FURTHER ORDERED** that Respondents, and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of Personal Information.

## V. DATA DELETION

**IT IS FURTHER ORDERED** that within one hundred twenty (120) days after entry of this Order, Respondents and Respondents' offers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must destroy all Personal Information collected from a Monitoring Product or Service prior to entry of this Order. Provided, however, that such Personal Information need not be destroyed, and may be disclosed, to the extent requested by a government agency or required by law, regulation, or court order, including without limitation as required by rules applicable to the safeguarding of evidence in pending litigation.

## VI. MANDATED INFORMATION SECURITY PROGRAM

**IT IS FURTHER ORDERED** that each Covered Business shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, each Covered Business 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 its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its information security program at least once every twelve months and promptly after any 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 months and promptly following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision VI.D. Each safeguard shall 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 unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Respondents' safeguards shall also include:

1. Technical measures to monitor all of Respondents' networks and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks;

2. Technical measures to secure Respondents' web applications and mobile applications and address well-known and reasonably foreseeable vulnerabilities, such as cross-site scripting, structured query language injection, and other risks identified by Respondents through risk assessments and/or penetration testing;

3. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) requiring authentication to access them, and (b) limiting employee or service provider access to what is needed to perform that employee's job function;

4. Encryption of all Personal Information on Respondents' computer networks; and

5. Establishing and enforcing policies and procedures to ensure that all service providers with access to Respondents' network or access to Personal Information are adhering to Respondents' Information Security Program.

F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, 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 months and promptly following a Covered Incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of each of Respondents' network(s) once every four (4) months and promptly after any Covered Incident, and penetration testing of each Covered Business's network(s) at least once every twelve (12) months and promptly after any Covered Incident;

H. Select and retain service providers capable of safeguarding Personal Information they receive from each Covered Business, and contractually require service providers to implement and maintain safeguards for Personal Information; and

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

## VII. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

**IT IS FURTHER ORDERED** that, in connection with compliance with Provision VI of this Order titled Mandated Information Security Program, Respondents 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. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product, attorney client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Respondents shall provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission

with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion.

C. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.

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

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Retina-X Studios, LLC, FTC File No. 172 3118." All subsequent biennial Assessments shall be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

## VIII. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

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

A. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondents have implemented and maintained the Information Security Program required by Provision VI of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-

Provisions VI.A-I; or (3) identification of any gaps or weaknesses in the Information Security Program; and

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

## IX. ANNUAL CERTIFICATION

**IT IS FURTHER ORDERED** that in connection with compliance with Provision VI of this Order titled Mandated Information Security Program, Respondents shall:

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

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711."

## X. COVERED INCIDENT REPORTS

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

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

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

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

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

E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect 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 each materially different notice required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711."

## XI. ORDER ACKNOWLEDGMENTS

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

A. Each Respondent, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten (10) years after entry of this Order, the Individual Respondent, for any business that such Respondent, individually or collectively with any other Respondent, is the majority owner or controls directly or indirectly, and the Corporate Respondent, must deliver a copy a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order, and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reporting. Delivery must occur within seven (7) days of entry 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 a Respondent delivered a copy of this Order, that Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

## XII. COMPLIANCE REPORT AND NOTICES

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

A. One year after entry of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:

1. Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Respondent; (b) identify all of the Respondents' businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if he knows or should know due to his own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondents made to comply with the Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, the Individual Respondent must: (a) identify all telephone numbers and all physical, postal, email and Internet addresses, including all residences; (b) identify all business activities, including any business for which Individual Respondent performs services whether as an employee or otherwise and any entity in which Individual Respondent has any ownership interest; and (c) describe in detail Individual Respondent's involvement in each such business, including title, role, responsibilities, participation, authority, control, and any ownership.

B. For 10 years after the issuance date of this Order, each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any changes in the following:

1. Each Respondent must report any change in: (a) any designated point of contact; or (b) the structure of Corporate Respondent or any entity that Respondent has any ownership interest in or control 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.

2. Additionally, Individual Respondent must report any change in: (a) name, including aliases or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Individual Respondent performs services whether as an employee or otherwise and (ii) any entity in

which Individual Respondent has any ownership interest and over which Individual Respondent has direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.

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

D. Any submission to the Commission required by this Order to 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: "United States v. Retina-X Studios, LLC, FTC File No. 172 3118, Docket No. C-4711."

## XIII. RECORDKEEPING

**IT IS FURTHER ORDERED** that Respondents must create certain records for ten (10) years after entry of this Order, and retain each such record for 5 years. Specifically, Corporate Respondent and Individual Respondent, for any business that such Respondent, individually or collectively with any other Respondent, is a majority owner or controls directly or indirectly, 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; address; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

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

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

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

F. A copy of each unique advertisement or other marketing material.

## XIV. COMPLIANCE MONITORING

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

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

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview any employee or other person 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 s or any individual or entity affiliated with Respondents, without the necessity of identification of 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.

D. Upon written request from a representative of the Commission, any consumer reporting agency must furnish consumer reports concerning the Individual Respondent, pursuant to Section 604(2) of the Fair Credit Reporting Act, 15 U.S.C. §1681b(a)(2).

## XV. 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 March 26, 2040, 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. The Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order is 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.

April J. Tabor
Acting Secretary

SEAL;
ISSUED: March 26, 2020