UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:

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

3. Proposed Respondents waive:
    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 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 each Proposed Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and

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 RETINAX STUDIOS, LLC.	DECISION AND ORDER DOCKET NO. C-

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

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 act 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.

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

VI. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that

5. Establishing and enforcing policies and procedures to ensure that all service providers with access to Respondents network or access to Personal Information 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 Respondent knows or has 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, 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. 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, Respondent 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 (ust1enhe2.1 Pe2.1 i2,1.15 Td [(a)4(u)-4 (s)-5 (t)- 1

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,

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

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

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: