This document is scheduled to be published in the
Federal Register on 10/31/2019 and available online at
https://federalregister.gov/d/2019-23809, and on **govinfo.gov**

[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 172 3118]

Retina-X Studios, LLC; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement; Request for Comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write: "Retina-X Studios, LLC; File No. 172 3118" on your comment, and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Jacqueline Connor (202-326-2844),

Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR § 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for October 22, 2019), on the World Wide Web, at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Retina-X Studios, LLC; File No. 172 3118" on your comment. Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the https://www.regulations.gov website.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online through the https://www.regulations.gov website.

If you prefer to file your comment on paper, write "Retina-X Studios, LLC; File No. 172 3118" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania

Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at https://www.regulations.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and

must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Retina-X Studios, LLC ("Retina-X") and individual Respondent James N. Johns, Jr. (collectively, "Respondents").

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.

From 2007 to 2018 Retina-X developed and sold various products and services, each with the means to allow a purchaser to monitor, often surreptitiously, another person's activities on that person's mobile device. James N. Johns, Jr. is the registered agent and sole member of Retina-X. Individually or in concert with others, Mr. Johns controlled or had the authority to control, or participated in the acts and practices alleged in the proposed complaint.

Respondents' mobile device monitoring products and services included MobileSpy, PhoneSheriff, and TeenShield. These monitoring products and services had varying capabilities and costs. Purchasers were often required to jailbreak or root (i.e., actions to bypass various restrictions implemented by the operating system on and/or the manufacturer of mobile devices) the device user's mobile device prior to installing Respondents' monitoring products and services. Jailbreaking or rooting a mobile device exposes a mobile device to various security vulnerabilities and likely invalidates any warranty that a mobile device manufacturer or carrier provides.

All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device, and could remotely monitor the device user's activities from an online dashboard. By default, Respondents' monitoring products and services disclosed to the device user that they were being monitored (e.g., an icon on a monitored mobile device). However, purchasers could turn off this feature so that the monitoring products and services could run surreptitiously, meaning that the device user was unaware that he or she was being monitored. Respondents provided

purchasers with instructions on how to remove the icon that would confirm that monitoring products and services were installed on a particular mobile device.

Device users surreptitiously monitored by Respondents' monitoring products and services could not uninstall or remove Respondents' monitoring products and services because they did not know that they were being monitored. Device users often had no way of knowing that Respondents' monitoring products and services were being used on their phone. Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for legitimate purposes, such as to monitor employees or children.

Moreover, Respondents did not take steps to secure the personal information collected from purchasers and device users being monitored. Respondents outsourced most of their product development and maintenance to a service provider. Respondents engaged in a number of practices that, taken together, failed to provide reasonable data security to protect the personal information collected from consumers. As a result of these unreasonable data security practices, Respondents were breached twice.

The Commission proposed 5-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act and the Children's Online Privacy Protection Rule. The first count alleges that Respondents unfairly sold monitoring products and services that required jailbreaking or rooting, without taking reasonable steps to ensure that the monitoring products and services would only be used for legitimate and lawful purposes by the purchaser.

The second to fourth counts allege that Respondents deceived consumers about Respondents' data security practices by falsely representing that consumers' personal

information collected through MobileSpy, PhoneSheriff, and TeenShield, and stored in Respondents' databases was confidential, private, and safe. The fifth count alleges that Respondents violated the Children's Online Privacy Protection Rule by failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children through the TeenShield product. Respondents failed to implement appropriate security procedures to protect the personal information collected from consumers, including children, such as by: (1) failing to adopt, implement, or maintain security standards, policies, procedures or practices; (2) failing to conduct security testing of mobile applications that could be exploited to gain unauthorized access to consumers' sensitive personal information for well-known and reasonably foreseeable vulnerabilities; (3) failing to contractually require their service providers to adopt and implement information security standards, policies, procedures or practices; (4) failing to perform adequate oversight of service providers; and (5) failing to adopt and implement written information security standards, policies, procedures, or practices that would apply to the oversight of their service providers.

The proposed order contains provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I of the proposed order prohibits Respondents from selling a monitoring product unless: (1) the monitoring product does not circumvent security protections implemented by the mobile device operating system or manufacturer; (2) prior to the sale of the monitoring product, express written attestation is obtained from the purchaser that the monitoring product stating that the monitoring product will be used for legitimate and lawful purposes; and (3) documentation is obtained proving that the purchaser is an

authorized user on the monitored mobile device's service carrier account. The proposed order also requires that Respondents display an application icon, including the name of the monitoring product, when the monitoring product is on the mobile device. Moreover, a clear and conspicuous notice must be presented when the application icon is clicked.

Part II of the order restrains Respondents from distributing monitoring products unless Respondents have: (1) a home page notice stating that the monitoring product may only be used for legitimate and lawful purposes by authorized users; and (2) a purchase page notice stating that the monitoring product may only be used for legitimate and lawful purposes by authorized users, and that installing or using the monitoring product for any other purpose may violate local, state, and/or federal law.

Part III of the proposed order prohibits Respondents from violating the Children's Online Privacy Protection Rule. Part IV of the proposed order prohibits Respondents from misrepresenting the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of consumers' personal information. Part V requires that Respondents' delete all personal information collected from a monitoring product prior to entry of the proposed order within 120 days.

Part VI of the proposed order prohibits Respondents, and any business that a Respondent controls, directly, or indirectly, from transferring, selling, sharing, collecting, maintaining, or storing personal information unless Respondents establish and implement, and thereafter maintain, a comprehensive information security program that protects the security confidentiality, and integrity of such personal information. Part VII requires Respondents to obtain initial and biennial data security assessments for twenty years. Part VIII of the proposed order requires Respondents to disclose all material facts

to the assessor and prohibits Respondents from misrepresenting any fact material to the assessments required by Part VII. Part IX requires Respondents to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program), that Respondents have implemented the requirements of the proposed order, are not aware of any material noncompliance that has not been corrected or disclosed to the Commission, and includes a brief description of any covered incident involving unauthorized access to or acquisition of personal information. Part X requires Respondents to submit a report to the Commission of their discovery of any covered incident.

Parts XI through XIV of the proposed order are reporting and compliance provisions, which including recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part XV 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.

By direction of the Commission.

April J. Tabor,

Acting Secretary.

[FR Doc. 2019-23809 Filed: 10/30/2019 8:45 am; Publication Date: 10/31/2019]