1723118

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. 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,

DOCKET NO. C-4711

COMPLAINT

The Federal Trade Commission, having reason to believe that Retina-X Studios, LLC, a limited liability company, and James N. Johns, Jr., individually and as sole member of Retina-X Studios, LLC (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act ("FTC Act") and the Children's Privacy Protection Rule ("Rule" or "COPPA Rule"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. Respondent James N. Johns, Jr. ("Johns") is the registered agent and sole member of Retina-X. Individually or in the concert of others, he controlled or had the authority to control, or participated in that acts and practices of Retina-X, including the acts and practices alleged in this complaint. His principal office of place of business is the same as that of Retina-X.

3. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

RESPONDENTS' BUSINESS ACTIVITIES

4. As recently as April 2018, Respondents developed and sold various monitoring 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 or computer (the "device user"). Respondents offered various monitoring products and services with varying capabilities and costs.

a. **MobileSpy:** Respondents' MobileSpy mobile device monitoring product and service ("MobileSpy") was marketed as a product to monitor children or employees. MobileSpy first became available in 2007, and Respondents sold more than 5,700 MobileSpy licenses. Once installed, MobileSpy captured and logged, among other things, the following: text messages; messages sent and received on various messaging services; call history; keys pressed; GPS locations; photos; contact list; screenshots; and browser history. MobileSpy's premium version also permitted monitoring consumers, from a remote online dashboard, to view the monitored mobile device's screen in real time.

b. **PhoneSheriff:** Respondents' PhoneSheriff mobile device monitoring product and service ("PhoneSheriff") was marketed as a product to monitor children. PhoneSheriff first became available in 2011, and Respondents sold more than 4,600 PhoneSheriff licenses. Once installed, PhoneSheriff captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; notes; music files; calendar entries; applications installed; mobile usage summaries; email history; and screenshots of any activity using the Snapchat application.

c. **TeenShield:** Respondents' TeenShield mobile device monitoring product and service ("TeenShield") was marketed as a product to monitor children. TeenShield first became available in 2015, and Respondents sold more than 5,000 TeenShield licenses. As part of the TeenShield for iOS registration process, Respondents collected dates of birth of users being monitored. From February 2016 to October 2017, Respondents collected approximately 950 dates of birth, and about a third of those were for children under the age of 13. Once installed, TeenShield captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; and email history.

5. 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 can expose a mobile device to various security vulnerabilities and likely invalidates any warranty that a mobile device manufacturer or carrier provides.

6. All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device or computer to install the monitoring products and services. Once Respondents' monitoring products and services were installed, the purchaser did not need physical access to the mobile device or computer, and could remotely monitor the device user's activities from an online dashboard.

7. 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.

8. 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. Even if a device user suspected that they were being surreptitiously monitored, they had no way of knowing that Respondents' monitoring products and services were being used on their phone by the purchaser.

9. Despite stating in their terms of services that their monitoring products and services were to be used for monitoring employees or children, Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for such purposes.

10. Moreover, the purported use of the monitoring products and services for employment or child-monitoring purposes is a pretext. Employers or parents would not typically jailbreak or root phones to install Respondents' monitoring products and services, particularly when many other monitoring products are available in the marketplace that do not require jailbreaking or rooting.

INJURY

11. Respondents' monitoring products and services substantially injured device users by enabling purchasers to surreptitiously stalk them. Stalkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and surreptitiously monitor victims' physical movements and online activities. Stalkers and abusers then use the information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause mental and emotional abuse, financial and social harm, and physical harm, including death.

12. Furthermore, victims of stalking experience financial loss both directly and indirectly. Directly, stalkers and abusers can use the information obtained through monitoring products and services to take over a victim's financial accounts, and redirect any (or all) funds to the abuser. Furthermore, victims suffer financial loss in the form of lost warranty coverage resulting from jailbreaking/rooting a mobile device and the purchase of a new mobile device to ensure that they are no longer subject to surreptitious monitoring. Indirectly, victims experience financial loss through the costs associated with therapy or counseling, and moving away from an abuser.

13. Even after stalking or domestic abuse ends, victims continue to experience substantial harms, including injury in the form of depression, anxiety, and safety fears.

14. The sale of Respondents' surreptitious monitoring products and services also substantially injured device users by undermining the mobile device security features provided by their operating system or manufacturer. Installation of Respondents' monitoring products and services required the purchaser to jailbreak or root a user's mobile device by bypassing various restrictions implemented by a mobile device operating system and/or manufacturer. Such jailbreaking or rooting may expose a mobile device to various security vulnerabilities, in part because a jailbroken/rooted phone may not receive security updates. With surreptitious monitoring products and services, these mobile device security risks are compounded by the fact that the device user is unaware that their mobile device has been jailbroken or rooted, and thus does not know that they should implement heightened safeguards to protect the security of their mobile device.

15. These harms were not reasonably avoidable by consumers, as users had no way to know that their mobile devices were being surreptitiously tracked using Respondents' monitoring products and services.

16. These harms are not outweighed by countervailing benefits to consumers or competition.

RESPONDENTS' DATA SECURITY PRACTICES

17. Even assuming Respondents believed that their monitoring products and services were being used for legitimate purposes, including the monitoring of children and employees, Respondents did not take steps to secure the personal information collected from purchasers and device users being monitored. As a result, the personal information collected from purchasers and device users was at risk of unauthorized disclosure and use.

18. Respondents outsourced most of their product development and maintenance to a service provider. The service provider developed Respondents' monitoring mobile applications, developed Respondents' websites (after 2005), managed Respondents' servers, managed Respondents' payment processing through a third party, provided marketing support for Respondents' monitoring products and services (until 2012), and ran customer support for Respondents' monitoring products and services (until 2016).

19. Respondents used a third party cloud storage provider to store photos collected from mobile devices being monitored using PhoneSheriff or TeenShield.

20. Respondents engaged in a number of practices that, taken together, failed to provide reasonable data security to protect the personal information collected from consumers. Among other things, Respondents failed to:

a. Adopt, implement, or maintain written information security standards, policies, procedures or practices;

b. 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;
c. Contractually require their service providers to adopt and implement information security standards, policies, procedures or practices;

d. Perform adequate oversight of service providers; and

e. Adopt and implement written information security standards, policies, procedures, or practices that would apply to the oversight of their service providers.

21. In February 2017, a hacker found unencrypted credentials in the TeenShield Android Package Kit ("APK") for Respondents' cloud storage account. The hacker logged into this account, and once there, the hacker found a screenshot that included the username and password for Respondents' server. The hacker then used those server credentials to log into Respondents' server, where the hacker accessed data collected through the PhoneSheriff and TeenShield monitoring products and services. The data accessed included, among other things, login usernames, encrypted login passwords, text messages, GPS locations, contact lists, apps installed, browser history, and photos. The hacker erased the entire database.

22. Respondents only became aware that they had been breached two months later, in April 2017, when a journalist contacted Respondents. The hacker had contacted the journalist, and provided evidence to the journalist that the hacker had obtained users' data from Respondents.

23. One year later, in February 2018, a hacker again found the credentials for Respondents' cloud storage account, this time in the PhoneSheriff APK. This time, the account credentials were "obfuscated," according to terminology used by Respondents, but the hacker was nevertheless able to decrypt the credentials and access Respondents' cloud storage account.

24. The hacker was able to access photos collected by mobile devices being monitored using PhoneSheriff and TeenShield. The hacker erased Respondents' cloud storage account, deleting all photos contained therein.

25. MobileSpy, PhoneSheriff and TeenShield have not been available for purchase since April 2018. However, Respondents' websites for each of these monitoring products and services remain online.

RESPONDENTS' DATA SECURITY REPRESENTATIONS

26. Since April 2007 Respondents' privacy policy for Mobile Spy has stated (*see* Exhibit A):

> "It is company policy that our customer databases remain confidential and private…Your private information is safe with us."

27. Since April 2011 Respondents' privacy policy for PhoneSheriff has stated (*see* Exhibit B):

> "It is company policy that our customer databases remain confidential and private…Your private information is safe with us."

28. Since December 2015 Respondents' privacy policy for TeenShield has stated (*see* Exhibit C):

> "It is company policy that our customer databases remain confidential and private…Your private information is safe with us."

RESPONDENTS ARE SUBJECT TO THE COPPA RULE

29. The COPPA Rule applies to any operator of a commercial Web site or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. As described above, in Paragraph 4(c), Respondents collected user dates of birth during the TeenShield registration process, many of which indicated that the monitored user was a child under the age of 13. As a result, Respondents had actual knowledge that the TeenShield product was collecting, using, and/or disclosing personal information from children.

30. The COPPA Rule defines "personal information" to include, among other things, a first and last name; a home or other physical address including street name and name of a city or town; online contact information (i.e., an email address or other substantially similar identifier that permits direct contact with a person online, such as an instant messaging user identifiers, screen name, or user name); a persistent identifier such as an IP address that can be used to recognize a user over time and across different Web sites or online services; a photograph, video, or audio file where such file contains a child's image or voice; or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. Through TeenShield, Respondents collected personal information as defined in the Rule, including the content of text messages and emails, email addresses or user names for a child that could be used to contact the child, and photographs and audio files containing a child's image or voice. Respondents also collected information from the child concerning the child that was combined with other identifiers, such as the name or photograph of the child.

31. Among other things, the Rule requires that an operator with actual knowledge, like Respondents as operators of TeenShield, meet specific requirements prior to collecting online, using, or disclosing personal information from children, including but not limited to, establishing and maintaining reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

VIOLATIONS OF THE FTC ACT

COUNT I – UNFAIRNESS

32. As described in Paragraphs 4 to 16, Respondents sold monitoring products and services that required circumventing certain security protections implemented by the Mobile Device operating system or manufacturer, and did so without taking reasonable steps to ensure that the monitoring products and services will be used only for legitimate and lawful purposes by the purchaser. Respondents' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. This practice is an unfair act or practice.

COUNT II – DECEPTION (MOBILESPY)

33. As described in Paragraph 26, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the MobileSpy mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

34. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the MobileSpy mobile device monitoring product and service, and stored in Respondents' databases, was not confidential, private, and safe. Therefore, the representations set forth in Paragraph 33 are false and misleading.

COUNT III – DECEPTION (PHONESHERIFF)

35. As described in Paragraph 27, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the PhoneSheriff mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

36. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the PhoneSheriff mobile device monitoring product and service, and stored in Respondents' databases, was not confidential, private, and safe. Therefore, the representations set forth in Paragraph 35 are false and misleading.

COUNT IV- DECEPTION (TEENSHIELD)

37. As described in Paragraph 28, Respondents have represented, directly or indirectly, expressly or by implication, that consumers' personal information collected through the TeenShield mobile device monitoring product and service, and stored in Respondents' databases, remains confidential, private, and safe.

38. In fact, as set forth in Paragraphs 20 through 24, consumers' personal information collected through the TeenShield mobile device monitoring product and service, and stored in

Respondents' databases, was not confidential, private, and safe. Therefore, the representations as described in Paragraph 37 are false and misleading.

VIOLATION OF THE COPPA RULE

COUNT V – COPPA (TEENSHIELD)

39. Respondents collected personal information from children under the age of 13 through the TeenShield product, which Respondents operated and had actual knowledge that children were being monitored using these online services.

40. In numerous instances, in connection with the acts and practices described above, Respondents collected, used, and/or disclosed personal information from children in violation of the Rule, including by failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, in violation of Section 312.8 of the Rule, 16 C.F.R. § 312.8.

41. Respondents' acts or practices, as described in Paragraph 40 above, violated the COPPA Rule, 16 C.F.R. Part 312.

42. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

43. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-sixth day of March, 2020, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: