Andrew Smith
Director of the Bureau of Consumer Protection
Federal Trade Commission
Prepared Remarks for Retina-X Studios, LLC Press Call
October 22, 2019

Today we are announcing the Federal Trade Commission's first case involving a stalking app. I'm particularly pleased to be joined today by Commissioner Slaughter, as well as the National Network to End Domestic Violence, an organization that, among other things, provides indispensable resources to survivors of domestic violence and their allies.

Stalking apps, also known as stalkerware, are spyware that secretly monitor another person's smartphone. According to our complaint, Retina-X Studios, LLC, and its owner James Johns, developed and sold three apps that allowed purchasers to surreptitiously monitor almost everything on the mobile devices on which they were installed, all without the knowledge or permission of the mobile device's user.

Retina-X's products were sold through the company's websites, and were not available in the Apple App Store or Google Play Store. Purchasers of Retina-X's products often needed to circumvent the device's security features, such as by jailbreaking or rooting the mobile device, in order to install the software on the device. Jailbreaking or rooting is a way to give a user unrestricted or administrative access to the phone. This can expose a mobile device to various security vulnerabilities, and also probably invalidates any warranty that a manufacturer or carrier provides. Retina-X instructed purchasers on how to hide the monitoring apps installed on the mobile devices, so that the mobile device users would never know that one of Retina-X's products was being used to stalk them. Once installed, the purchaser could remotely monitor the user's activity on the phone from an online dashboard provided by Retina-X. The Retina-X apps monitored a huge amount of phone activity, including precise GPS locations, text messages sent and received, and all photos stored on the phone. In the wrong hands, this information could be used to stalk, harass, and abuse a person.

We allege three separate law violations:

First, we allege that Retina-X engaged in unfair practices under the FTC Act by selling monitoring apps that required circumventing security protections on the mobile device, *and* doing so without taking reasonable steps to ensure that the products would only be used for legitimate and lawful purposes by the purchaser.

Second, we allege that Retina-X engaged in deceptive practices under the FTC Act by misrepresenting that personal information collected through a monitoring product and stored in their databases would remain confidential, private, and safe.

Third, in some cases, Retina-X's apps collected information from kids. We allege that Retina-X failed to comply with the Children's Online Privacy Protection Act, or COPPA, by failing to establish and maintain reasonable security procedures to protect their personal information.

Going forward, Retina-X and Mr. Johns are prohibited from selling any monitoring app that requires circumventing security protections on a phone – such as jailbreaking or rooting. For any other monitoring app, the purchaser must attest that they are using the app for a legitimate and lawful purpose, and must provide documentation showing that they are the account holder of the device that's being monitored. Retina-X and Mr. Johns are also prohibited from transferring, selling, sharing, collecting, maintaining, or storing personal information in the future unless they implement and maintain a comprehensive information security program. They also must delete any data they collected from consumers prior to our settlement, are required to comply with COPPA, and are prohibited from misrepresenting how they handle consumers' personal information.

I'd like to thank Jacqueline Connor, Megan Cox, and Yan Lau from the FTC for their work on this case. With that, I will turn the microphone over to Commissioner Slaughter, who has more to say about the importance of today's action for consumers and businesses.