192 3003

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of

SUPPORT KING, LLC, a limited liability company, also formerly d/b/a SpyFone.com, and

SCOTT ZUCKERMAN, individually and as an officer of Support King, LLC

DOCKET NO. C-4756

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Support King, LLC, a limited liability company, and Scott Zuckerman, individually and as an officer of Support King, LLC (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Support King, LLC ("Support King"), also formerly doing business as SpyFone.com ("SpyFone"), is a Puerto Rico limited liability company with a principal office or principal place of business at 5900 Ave Isla Verde, Carolina, Puerto Rico 00979-5746. At all times material to this Complaint, acting alone or in concert with others, Support King has advertised, marketed, distributed, or sold monitoring products and services to consumers throughout the United States.

2. Respondent Scott Zuckerman ("Zuckerman") is the president, founder, resident agent, and chief executive officer of Support King. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had authority to control, or participated in the acts or practices of Support King, including the acts and practices set forth in this Complaint. Among other things, Respondent Zuckerman created Support King's websites, hired service providers for these websites, and signed contracts on behalf of Respondent Support King. His principal office or place of business is the same as that of Support King.

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 Practices

4. Respondents license, market, and sell various monitoring products and services, each of which allows a purchaser to monitor surreptitiously another person's activities on that person's mobile device (the "device user"). These types of surreptitious monitoring apps have been used by stalkers and domestic abusers to monitor their victims' physical movements and online activities, as well as to obtain their sensitive personal information without authorization.

5. Respondents offer or have offered various monitoring products and services with varying capabilities and costs for Android devices (collectively, "SpyFone products and services").

a. **SpyFone for Android Basic:** Respondents' SpyFone for Android Basic ("Android Basic") is marketed as a product to monitor children or employees. Android Basic first became available in 2018, and is sold on a subscription basis for $99.95 for twelve months. Once installed, Android Basic captures and logs, among other things, the following: SMS messages; call history; GPS location and live location; web history; contacts; pictures; calendar; files downloaded on the device; and notifications. It gives purchasers the ability to block apps, receive an app usage report, and also claimed it could spoof text messages so that the purchaser can send text messages that appear to be coming from the monitored device.

b. **SpyFone for Android Premium:** Respondents' SpyFone for Android Premium ("Android Premium") is also marketed as a product to monitor children or employees. Android Premium first became available in 2018, and is sold on a subscription basis for $119.95 for three months, or $199.95 for twelve months. In addition to the functionality included with Android Basic, Android Premium is marketed as able to capture and log or transmit, among other things, the following: emails; video chats; and activity on or through apps, including posts made on social media, contents of messages sent and received, pictures shared on photo apps, and information exchanged on online dating apps.

c. **SpyFone for Android Xtreme:** Respondents' SpyFone for Android Xtreme ("Android Xtreme") is marketed as SpyFone's "most popular" product, and also as a tool to monitor children or employees. Android Xtreme first became available in 2018, and is sold on a subscription basis for $179.95 for three months, or $299.95 for twelve months. In addition to the functionality included with Android Premium, Android Xtreme includes, among other things, a key logger, and live screen viewing. It also includes the ability to remotely take pictures, record audio by turning on the device's microphone, record calls, and send the mobile device commands through SMS, such as commands to vibrate or ring the mobile device.

d. **SpyFone for Android Xpress:** Respondents' SpyFone for Android Xpress ("Android Xpress") was a mobile device sold through at least spring 2019 that came preinstalled with a one-year subscription for Android Xtreme, and started at $495.

Installation and Monitoring

6. Installing the SpyFone products requires that the purchaser have physical access to the device. The products are not available through the Google Play store, and instead must be downloaded from Respondents' website. Purchasers of SpyFone Android products that require installation must take steps to bypass numerous restrictions implemented by the operating system or the mobile device manufacturer on the monitored mobile device. Among other things, SpyFone instructs purchasers to enable the monitored mobile device to allow downloads from "unknown sources" for certain versions of Android. Android warns users "[i]f you download apps from unknown sources, your device and personal information can be at risk. Your device could get damaged or lose data. Your personal information could be harmed or hacked." SpyFone also instructs the purchaser to "disable[] the verification of applications," a security setting that identifies potentially harmful applications by scanning what applications are on the mobile device.

7. To enable certain functions of the SpyFone products, such as viewing outgoing email, purchasers must gain administrative privileges to the mobile device, such as through "rooting" the mobile device, giving the purchaser privileges to install other software on the mobile device that the manufacturer would not otherwise allow. This access enables features of the SpyFone products to function, exposes a mobile device to various security vulnerabilities, and can invalidate warranties that a mobile device manufacturer or carrier provides.

8. SpyFone, unlike most other mobile applications, does not appear as an application with an icon on the mobile device. During the installation process for SpyFone Android products, SpyFone gives the purchaser instructions on further steps he or she can take to hide the product on the device so that the device user will be unaware the device is being monitored. For example, the purchaser can disable notifications that would otherwise appear warning the monitored mobile device user that the SpyFone product captures "everything that is displayed on the screen." After installation, the purchaser is instructed to "[r]eboot the device to hide the application" and is then counseled for "[b]est [d]iscretion" to delete the mobile device's web browsing history, delete the installation file on the mobile device, delete the notification on the mobile device, disable notifications, and "make the application trusted," all steps to ensure the device user never learns of the surreptitious monitoring. The SpyFone software can then only be found by navigating through the device's "Settings," where, according to SpyFone's website, it is labeled as "System Service" in order "to be more stealthy[.]"

9. Once the purchaser installs the SpyFone Android product, he or she does not need physical access to the monitored mobile device, and can remotely monitor the device user's activities from an online dashboard.

10. Despite stating in a disclaimer that its monitoring products and services are designed for monitoring children or employees, Respondents do not take any steps to ensure that purchasers use Respondents' monitoring products and services for such purposes.

11. The purported use of the monitoring products and services for employment or child-monitoring purposes is a pretext. Parents and employers would not typically want the

monitoring product to spoof text messages from the device, a feature SpyFone marketed to its customers, or want to disable security measures on a mobile phone to install Respondents' Android monitoring products and services—particularly when doing so may void a warranty and weaken the mobile device's security. Many other monitoring products are available in the marketplace that do not carry these risks.

12. Device users who are surreptitiously monitored using Respondents' monitoring products and services cannot stop the monitoring because they do not know it is happening. In fact, Respondents instruct the purchasers on how to hide the SpyFone products and services on the mobile device so that device users are unaware they are being monitored.

Respondents' Data Security Practices

13. Since 2018, Respondents have collected personal information about purchasers and device users monitored by SpyFone products and services as described above. This personal information includes, but is not limited to, photos, text messages, web histories, and GPS locations.

14. In 2018 and into 2019, Respondents' Terms of Use for Respondents' monitoring products and services stated, "SpyFone cares about the integrity and security of your personal information. We will take all reasonable precautions to safeguard customer information, including but not limited to contact information, personally identifiable information (PII), and payment details," and "Spyfone uses its database to store your encrypted personal information."

15. Data is collected from a user's mobile device and stored on a server accessible to Respondents ("Respondents' server") once SpyFone products and services are installed on an Android mobile device.

16. After initial setup, all information surreptitiously captured from a device user's mobile device is stored on a separate server that was accessible only by one of Respondents' service providers.

17. Respondents have engaged in a number of practices that failed to provide reasonable data security for consumers' personal information. Among other things, Respondents:

a. Failed to encrypt personal information stored on Respondents' server, including photos, text messages, web histories, and GPS locations;

b. Failed to ensure access to Respondents' server was properly configured so that only authorized users could access consumers' personal information;

c. Failed to adequately assess and address vulnerabilities of its Application Programming Interfaces (APIs), including failing to whitelist IP Addresses that could access the API;

d. Transmitted purchasers' passwords for their SpyFone accounts in plain text; and

e. Failed to contractually require its service provider that stored monitored information from the SpyFone products and services to adopt and implement data security standards, policies, procedures or practices.

18. As a result of some of these failures, in August 2018, an unauthorized third party accessed Respondents' server, thereby gaining access to the data of approximately 2,200 consumers. The information exposed included records collected from the mobile devices, including photos.

19. Respondents disseminated a notice to purchasers following the breach in August 2018 representing that they had "partner[ed] with leading data security firms to assist in our investigation" and that they would "coordinate with law enforcement authorities" on the matter.

20. Respondents did not partner with any data security firms to assist in their investigation of the unauthorized access.

21. Respondents did not work with or coordinate with law enforcement on any aspect of the unauthorized access.

Injury

22. Respondents' SpyFone monitoring products and services substantially injure device users by enabling purchasers to stalk them surreptitiously. Stalkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and monitor surreptitiously 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.

23. Stalking victims 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 stalker or abuser. Indirectly, victims experience financial loss through the costs associated with therapy or counseling, and moving away from an abuser.

24. Even after stalking or domestic abuse ends, victims continue to experience substantial harm, including injury in the form of depression, anxiety, and ongoing fear for one's safety.

25. The sale of Respondents' surreptitious monitoring products and services also substantially injures device users by undermining their mobile devices' security features. Installation of Respondents' Android monitoring products and services requires the purchaser to circumvent certain security features and settings, such as disabling the verification of applications, disabling pop-up notifications, and enabling installation of apps from unknown sources. Such actions could expose a mobile device to various security vulnerabilities, including

outdated operating systems and malware, and consumers may experience lost warranty coverage and need to purchase a new mobile device.

26. With surreptitious monitoring products and services, these mobile device security risks are compounded by the fact that, in most circumstances, the device user is unaware that security features have been compromised, and thus does not know that he or she should implement heightened safeguards to protect the security of his or her mobile device.

27. These harms are not reasonably avoidable by consumers, as device users do not know that their mobile devices are surreptitiously tracked using Respondents' SpyFone monitoring products and services. Even if device users eventually learn that they are being monitored, information from their mobile devices has already been collected by Respondents.

28. These harms outlined above are not outweighed by countervailing benefits to consumers or competition.

COUNT I – UNFAIRNESS
Unfair Sales of Surreptitious Monitoring Devices

29. In numerous instances, Respondents sell or have sold monitoring products and services that operate surreptitiously on mobile devices without taking reasonable steps to ensure that the purchasers use the monitoring products and services only for legitimate and lawful purposes.

30. 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. Therefore, Respondents' acts or practices as described in Paragraph 29 constitute unfair acts or practices.

COUNT II – DECEPTION
Data Security Misrepresentations

31. In numerous instances in connection with the sale of the monitoring products and services, Respondents have represented, directly or indirectly, expressly or by implication, that Respondents will take all reasonable precautions to safeguard customer information, including by using their database to store consumers' personal information encrypted.

32. In truth and in fact, as set forth in Paragraphs 13 through 18, Respondents did not take all reasonable precautions to safeguard customer information and information stored in Respondents' database was not encrypted. Therefore, Respondents' representations as described in Paragraph 31 of this Complaint are false and misleading and constitute deceptive acts or practices.

COUNT III – DECEPTION
Data Breach Response Misrepresentations

33. In numerous instances in connection with the sale of the monitoring products and services, Respondents represented, directly or indirectly, expressly or by implication, that Respondents partnered with leading data security firms to investigate the data breach and coordinated with law enforcement authorities.

34. In truth and in fact, as set forth in Paragraphs 20 and 21, Respondents did not actually partner with leading data security firms or work with law enforcement authorities. Therefore, Respondents' representations as described in Paragraph 33 of this Complaint are false and misleading and constitute deceptive acts or practices.

Violations of Section 5 of the FTC Act

35. 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.

THEREFORE, the Federal Trade Commission, this twentieth day of December 2021, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL