192 3003

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina Khan, Chair**
Noah Joshua Phillips
Rohit Chopra
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.**

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.

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

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 ser0 Tc 0 Tw 2. (i)-1 (sk)1 (J2 2 (d)]TJ(m)8 (o)-5 (ni)2oni)-2w (,)Tj( )TTj0 Ts (es o)355 p xd65nx ,

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 .d [

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' personalomecae informato, eers tcae iers tcCt

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 _____day of _____, 20__, has issued this Complaint against Respondents.

By the Commission.

April Tabor
Secretary

SEAL: