**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of Support King, LLC and Scott Zuckerman, Matter No. 192 3003***

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Support King, LLC, formerly d/b/a SpyFone.com ("Corporate Respondent"), and Scott Zuckerman ("Individual Respondent") (collectively, "Respondents").

The Commission has placed the proposed consent order ("Proposed Order") 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.

Support King has sold various monitoring products and services, each of which allowed a purchaser to monitor surreptitiously another person's activities on that person's mobile device. Scott Zuckerman is the president, founder, resident agent, and chief executive of Support King. Individually or in concert with others, Mr. Zuckerman controlled or had the authority to control, or participated in the acts and practices alleged in the proposed complaint.

Respondents' monitoring products and services included SpyFone for Android Basic, Premium, Xtreme, and Xpress. These monitoring products and services had varying capabilities and costs. Purchasers of these products had to take steps to bypass numerous restrictions implemented by the operating system or the mobile device manufacturer on the monitored mobile device during installation. To enable certain functions of the monitoring products and services, purchasers had to gain administrative privileges, exposing mobile devices to various security vulnerabilities.

All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device for installation, and then the purchaser could remotely monitor the device user's activities from an online dashboard. Once installed, the monitoring products and services ran surreptitiously, meaning that the device user was unaware that he or she was being monitored. The SpyFone software would 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[.]"

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 phones. Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for legitimate purposes.

Moreover, Respondents did not take steps to secure the personal information collected from device users being monitored despite stating, "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 databases to store your encrypted personal information." Respondents engaged in a number of practices that, taken together, failed to provide reasonable data security to protect the personal information collected from device users.

As a result of these unreasonable data security practices, in August 2018, an unauthorized third party accessed Respondents' server, gaining access to the data of approximately 2,200 consumers. Respondents then disseminated a notice to purchasers following the unauthorized access, representing that Respondents 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. In reality, Respondents did not partner with any data security firms or coordinate with law enforcement authorities.

The Commission's proposed three-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act. The first count alleges that Respondents unfairly 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.

The second count alleges Respondents deceived consumers about Respondents' data security practices by falsely representing that it would take all reasonable precautions to safeguard customer information, including by using their database to store consumers' personal information encrypted. Respondents failed to implement appropriate security procedures to protect the personal information they collected from consumers, such as by: (1) failing to encrypt personal information stored on Respondents' server; (2) failing to ensure access to Respondents' server was properly configured so that only authorized users could access consumers' personal information; (3) failing to adequately assess and address vulnerabilities of its Application Programing Interfaces (APIs); (4) transmitting purchasers' passwords for their SpyFone accounts in plain text; and (5) failing to contractually require its service provider to adopt and implement data security standards, policies, procedures or practices.

The third count alleges Respondents deceived consumers about Respondents' data breach response, when Respondents stated they were partnering with leading data security firms to investigate the data breach and coordinating with law enforcement authorities, when in fact Respondents did not.

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 requires Respondents to disable immediately all access to any information collected through a monitored mobile device, and immediately to cease collection of any data through any monitoring software.

Part II requires that within 30 days of the entry of the Proposed Order, Respondents must delete all consumer data collected.

Part III of the Proposed Order requires Respondents to provide notice on all of Support King's websites, and to provide notice through emails to purchasers and trial users, stating that the FTC alleged Support King sold illegal monitoring products and services, that Support King agreed to disable the software, and that Respondents' previous notice of June 2020 was inaccurate. Respondents must also provide notice to each user of a monitored device, through an on-screen notification, informing the user that Support King collected information from his or her phone, and that the phone may not be secure.

Part IV of the Proposed Order bans Respondents from licensing, advertising, marketing, promoting, distributing, selling, or assisting in any of the former, any monitoring product or service to consumers.

Part V of the Proposed Order prohibits Respondents from making any misrepresentations about the extent to which Respondents work with privacy or security firms, or the extent to which Respondents maintain and protect the privacy, security, confidentiality, and integrity of personal information.

Part VI of the Proposed Order prohibits Corporate Respondent, and any Covered Business (any business controlled, directly or indirectly, by either Corporate Respondent or Individual Respondent) from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it establishes and implements, and thereafter maintains, 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 for any Covered Business that collects personal information online. 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 following their discovery of any covered incident.

Parts XI through XIV of the Proposed Order are reporting and compliance provisions, which include 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 twenty (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.