

2. Proposed Respondents neither admit nor deny any of the allegations in the draft Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondents admit the facts necessary to establish jurisdiction.
3. Proposed Respondents waive:
 - a. Any further procedural steps;
 - b. The requirement that the Commission's Decision contain a statement of findings of fact and conclusions of law; and
 - c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.
4. Propost Agreement.7i

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.

DECISION

The Federal

Respondents and BCP thereafter executed an Agreement Containing Consent Order (ACCO) and a Consent Order (CO) that, in addition to the Commission's jurisdiction, and 2) waivers and other provisions as required by the

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should be issued against Respondents. The Commission of party (BC) accepted and consideration of public comments. The Commission duly considered any comments received from interested P

in conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, the following Findings, and issues the following Order:

Findings

1. The Respondents are:
 - a. Respondent Support King, LLC (“Support King”), also formerly doing business as SpyFone.com, 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.
 - b. 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.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

- A. **“Clear(ly) and Conspicuous(ly)”** means that a required disclosure is difficult to miss (, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- B. “**Corporate Respondent**” means Support King, LLC, also formerly d/b/a SpyFone.com, and its successors and assigns.
- C. “**Covered Business**” means Corporate Respondent, any business that Corporate Respondent controls, directly or indirectly, and any business that Individual Respondent controls, directly or indirectly.
- D. “**Covered Incident**” means any instance in which any United States federal, state, or local law or regulation requires Respondents to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondents from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- E. “**Individual Respondent**” means Scott Zuckerman.
- F. “**Respondents**” means the Individual Respondent and the Corporate Respondent, individually, collectively, or in any combination.
- G. “**Internet**” means collectively the myriad of computer and telecommunication facilities, including equipment and operating software, which comprises the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

- H. **“Mobile Device”** means any portable computing device that operates using a mobile operating system, including but not limited to, any smartphone, tablet, wearable, or sensor, or any periphery of any portable computing device.
- I. **“Monitoring Product or Service”** means any software application, program, or code that can track or monitor a user’s activities on a Mobile Device, including but not limited to, the user’s text messages, web browser history, geolocation, and photos.
- J. **“Person”** means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.
- K. **“Personal Information”** means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or other physical address; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other government issued identification number; (g) a financial account number; (h) credit or debit card information; (i) a date of birth; (j) a persistent identifier that can be used to recognize a user over time and across different Web sites or online services, such as a user name, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; (k) photograph, video, audio file, or contents of email or other messages; and (l) geolocation information sufficient to identify street name and name of a city or town.
- L. **“Purchaser”** means any Person who buys or subscribes to, including on a trial basis, any Monitoring Product or Service provided by Respondents.

Provisions

I. COLLECTION OF INFORMATION

IT IS ORDERED that Respondents, and all other Persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, immediately disable all access to any information collected by or through a monitored Mobile Device and immediately cease collection of any data through any Monitoring Product or Service installed before the date of entry of this Order.

II. DATA DELETION

IT IS FURTHER ORDERED that within thirty (30) days after entry of this Order, Respondents and Respondents’ officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this Order, must

destroy all Personal Information collected from a Monitoring Product or Service sold or distributed by Respondents prior to entry of this Order.

III. NOTICE TO PAST PURCHASERS AND MOBILE DEVICE USERS

IT IS FURTHER ORDERED that Respondents must:

Someone may have secretly monitored your phone.

The Federal Trade Commission has alleged that Support King sold illegal monitoring products, which may have been installed on this phone. The software has been disabled.

This phone may still not be secure. Photos, emails, texts, and location were collected from this phone.

For details, visit [\[hyperlink to FTC blog\]](#) or call 877-382-4357.

For help, call the National Domestic Violence Hotline
800-799-

- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision VI.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Such safeguards must include:
 - 1. Training of all of Respondents' employees, at least once every twelve (12) months, on how to safeguard Personal Information;
 - 2. Technical measures to monitor all of Respondents' networks and systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks;
 - 3. Technical measures to secure Respondents' web applications and mobile applications and address well-known and reasonably foreseeable vulnerabilities identified by Respo Resp (tio)2 (n.s)-1 (. (l)-1 (.ch (a31 (k, a)-1]TJk (s)-1 (e)-1 (t)-2 (s)-1 (e)-1 (t)-

- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results.
- H. Select and retain service providers capable of safeguarding Personal Information they receive from each Covered Business, and contractually require service providers to implement and maintain safeguards for Personal Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to Respondents' operations or business arrangements, a Covered Incident, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, each Covered Business must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

VII. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision VI of this Order titled Mandated Information Security Program, for any Covered Business that collects Personal Information online, Respondents must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product, attorney client privilege, statutory exemption, or any similar claim.
- B. For each Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the Person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first one-hundred eighty (180) days after the issuance date of the Order for the initial Assessment; and (2) each two (2)-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire Assessment period: (1) determine whether each Covered Business has implemented and maintained the Information Security Program required by Provision VI of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of each Covered Business's implementation and maintenance of sub-Provisions VI.A-

noncompliance with, the Security Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews

IX. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that Respondents must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each Covered Business responsible for each Covered Business's Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Support King, LLC, FTC File No. 192 3003."

X. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondents, for any Covered Business, within a reasonable time after the date of Respondents' discovery of a Covered Incident, but in any event no later than twenty-one (21) days after the date Respondents first notify any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if he knows or should know due to his own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondents made to comply with the Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, the Individual Respondent must: (a) identify all telephone numbers and all physical, postal, email and Internet addresses, including all residences; (b) identify all business activities, including any business for which Individual Respondent performs services whether as an employee or otherwise and any entity in which Individual Respondent has any ownership interest; and (c) describe in detail Individual Respondent's involvement in each such business, including title, role, responsibilities, participation, authority, control, and any ownership.

B. For ten (10) years after entry of this Order, each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any changes in the following:

1. Each Respondent must report any change in: (a) any designated point of contact; or (b) the structure of Corporate Respondent or any entity that Respondent has

identification of prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

- D. Upon written request from a representative of the Commission, any consumer reporting agency must furnish consumer reports concerning the Individual Respondent, pursuant to Section 604(1) of the Fair Credit Reporting Act, 15 U.S.C. §1681b(a)(1).

XV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B.