

Complaint

IN THE MATTER OF

**SUPPORT KING, LLC.,
AND
SCOTT ZUCKERMAN**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT.

*Docket No. C-4756; File No. 192 3003
Complaint, September 1, 2021 – Decision, December 20, 2021*

This order addresses a violation of the FTC Act through the unfair sales of surreptitious monitoring devices, illegal harvesting and sharing of private information, and failure to secure user data of Support King, LLC., formerly doing business as SpyFone.com. Under the order the Respondent is banned from offering, promoting, selling, or advertising any surveillance app, services, or business. The Respondents must delete any information illegally collected from their apps and notify owners of devices on which SpyFone’s apps were installed that their devices might have been monitored and the devices might not be secure.

Participants

For the *Commission*: *Jacqueline Connor Ford*

For the *Respondent*: *Alexandra Megaris and Leonard Gordon [Venable LLP]*.

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:

I. RESPONDENTS

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,

Complaint

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.

II. 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,

Complaint

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.

III. 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[.]"

Complaint

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.

IV. 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:

Complaint

- 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.

V. 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.

Complaint

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.

VI. 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.

Complaint

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.

Decision and Order

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

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 issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested Persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes 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.

Decision and Order

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 (*i.e.*, 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.

Decision and Order

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;

Decision and Order

(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:

- A. Within five (5) days after the date of entry of this order post a Clear and Conspicuous notice on all of Corporate Respondent’s consumer-facing websites, which will remain posted for two years after entry of this Order, and which states:

The Federal Trade Commission (FTC) [hyperlink to www.ftc.gov], the nation’s consumer protection agency, recently alleged that Support King sold illegal monitoring products and services. To settle the lawsuit, Support King agreed to disable its monitoring products and services and tell people that it is against the law to monitor other adults without their permission. A previous notice of June 2020 inaccurately suggested the settlement pertained only to subscribers in the United States. The settlement relates to Support King’s services worldwide.

Decision and Order

If you think someone is illegally monitoring your phone or your phone was compromised by this software, please call 1-877-382-4357 or visit the Federal Trade Commission [hyperlink to FTC consumer blog post announcing settlement] for more information.

For help, please use a different, secure phone to call the National Domestic Violence Hotline at 1-800-799-7233. If you're in danger right now, call 911.

- B. Send an email with the subject line “Notice of FTC Settlement: Illegal Monitoring Products Disabled” to Purchasers of a Monitoring Product or Service prior to entry of this Order, which Clearly and Conspicuously states:

The Federal Trade Commission (FTC) [hyperlink to www.ftc.gov], the nation's consumer protection agency, recently alleged that Support King sold illegal monitoring products and services. To settle the lawsuit Support King agreed to disable its software and let you know that it is against the law to monitor other adults without their permission. A previous notice of June 2020 inaccurately suggested the settlement pertained only to subscribers in the United States. The settlement relates to Support King's services worldwide.

- C. Send a Clear and Conspicuous notice via on-screen notification to Mobile Device users with a Monitoring Product or Service installed on their Mobile Device prior to the entry of this Order, which shall Clearly and Conspicuously state:

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 800-799-7233 using a secure phone. If you're in danger, call 911.

Decision and Order

IV. BAN ON MONITORING PRODUCTS AND SERVICES

IT IS FURTHER ORDERED that Respondents are permanently restrained and enjoined from licensing, advertising, marketing, promoting, distributing, or offering for sale, or assisting in the licensing, advertising, marketing, promoting, distributing, or offering for sale, any Monitoring Products or Services to consumers.

V. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Respondents, 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, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Respondents work with privacy or security firms, and the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of Personal Information.

VI. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Corporate Respondent, and any Covered Business, must not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, each Respondent must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;
- 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;

Decision and Order

- 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 Respondents through risk assessments and/or penetration testing;
 4. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) requiring authentication to access them, and (b) limiting employee or service provider access to what is needed to perform that employee's job function;
 5. Encryption of (a) Personal Information collected through Monitoring Products and Services and (b) financial account information; and
 6. Policies and procedures to ensure that all service providers with access to Respondents' network or access to Personal Information are adhering to Respondents' Information Security Program.
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results. 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.
- G. 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

Decision and Order

- H. 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-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Security Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and

Decision and Order

explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by a Covered Business's management. The Assessment must be signed by the Assessor and must state that the Assessor conducted an independent review of the Information Security Program and did not rely solely on assertions or attestations by a Covered Business's management. To the extent that Respondents revise, update, or add one or more safeguards required under Provision VII of this Order in the middle of an Assessment period, the Assessment shall assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed 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." All subsequent biennial Assessments must be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VIII. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Assessment required by Provision VII of this Order titled Information Security Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control, that is relevant to the Assessment for which there is no reasonable claim of privilege.
- B. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondents have implemented and maintained the Information Security Program required by Provision VI of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub- Provisions VI.A-I; or (3) identification of any gaps or weaknesses in the Information Security Program.

Decision and Order

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;

Decision and Order

- 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
- F. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent 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."

XI. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

- A. Each Respondent, within seven (7) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after entry of this Order, the Individual Respondent for any business that such Respondent, individually or collectively with any the other Respondent, is the majority owner or controls directly or indirectly, and the Corporate Respondent, must deliver a copy a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order, and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

Decision and Order

- A. One year after entry of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:
1. Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondents; (b) identify all of the Respondents' businesses by all of their names, telephone 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 any ownership interest in or control directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
 2. Additionally, Individual Respondent must report any change in: (a) name, including aliases or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Individual Respondent performs services whether as an employee or otherwise and (ii) any entity in which Individual Respondent has any ownership interest and over which Individual Respondent has direct or indirect control. For each

Decision and Order

such business activity, also identify its name, physical address, and any Internet address.

- C. Each Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: “_____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent 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.”

XIII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondents must create certain records for ten (10) years after the issuance date of this Order and retain each such record for five (5) years. Specifically, Corporate Respondent and Individual Respondent, for any business that such Respondent, individually or collectively with any other Respondents, is a majority owner or controls directly or indirectly, must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each Person providing services, whether as an employee or otherwise, that Person’s: name; address; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission and all attestations; and
- D. A copy of each unique advertisement or other marketing material.

XIV. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents’ compliance with this Order:

Decision and Order

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview any employee or other Person affiliated with any Respondent who has agreed to such an interview. The Person interviewed may have counsel present.
- C. The Commission may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of 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 on December 20, 2041, 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; *provided, however*, 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. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Concurring and Dissenting Statement

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

STATEMENT OF COMMISSIONER ROHIT CHOPRA

Today, the Commission has proposed banning Support King, the operator of SpyFone, and its top executive, Scott Zuckerman, from marketing surveillance software to address severe misconduct related to their spying software scheme.

As alleged in the Commission's complaint, Support King licensed and marketed products where stalkers¹ and other users were given instructions on how to install an app on another person's mobile device, allowing users to have unfettered access to their target's location, text messages, and more. The company also employed shoddy security protocols that led to unauthorized access of sensitive personal records. To top it off, the company lied to its users about how it was handling the intrusion.

Surveillance Ban

The Commission is seeking public comment on banning Support King and Scott Zuckerman from licensing, marketing, or offering for sale surveillance products. This is a significant change from the agency's past approach. For example, in a 2019 stalkerware settlement, the Commission allowed the violators to continue developing and marketing monitoring products.²

¹ See Press Release, Electronic Frontier Foundation, Watch EFF Cybersecurity Director Eva Galperin's TED Talk about Stalkerware (May 28, 2020) <https://www.eff.org/deeplinks/2020/05/watch-eff-cybersecurity-director-evagalperins-ted-talk-about-stalkerware>.

² The Commission's settlement in Retina-X Studios allowed the bad actors to continue to develop and market surveillance products, subject to certain requirements that the product would be used "legitimately." Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Settlement with Stalking Apps Developer (Mar. 27, 2020), <https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-stalking-appsdeveloper>. I reluctantly supported the resolution, despite my concerns about the leniency of the sanctions for illegal stalkerware behavior. The proposed ban in this matter will be easier to enforce, rather than making determinations about "legitimate" surveillance.

Concurring and Dissenting Statement

In addition to the surveillance ban, affected individuals will receive notifications that someone may have been surreptitiously monitoring their mobile device, as well as information to seek help if they may be in danger.³ The Commission welcomes public comment on these provisions.

Criminal Law Enforcement

The FTC's proposed order in no way releases or absolves Support King or Scott Zuckerman of any potential criminal liability. While this action was worthwhile, I am concerned that the FTC will be unable to meaningfully crack down on the underworld of stalking apps using our civil enforcement authorities.⁴ I hope that federal and state enforcers examine the applicability of criminal laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and other criminal laws, to combat illegal surveillance, including the use of stalkerware.⁵

While certain applications of these laws have been concerning,⁶ I believe it would be appropriate for enforcers to use these laws to seek criminal sanctions against individuals and firms that facilitate human endangerment through surveillance and stalkerware.

³ Notice to affected individuals promotes greater accountability for bad actors and better functioning markets. Past Commissions routinely deprived these individuals of direct notice from bad actors, but we have changed course.

⁴ Ideally, the Commission can also secure redress and damages for affected individuals in these matters. But monetary relief may not be sufficient to deter wrongdoing, given the structure of the market.

⁵ The Computer Fraud and Abuse Act prohibits, among other things, "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" and obtaining information. 18 U.S.C. § 1030 (a)(2)(C). The Act also prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value" 18 U.S.C. § 1030 (a)(4).

⁶ The indictment of Aaron Swartz for violations of the Computer Fraud and Abuse Act raised serious concerns about the application of the Act. *See e.g.* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), <https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computerhacking-cases/>.

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

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

Analysis to Aid Public Comment

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 Programming 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.

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

BOARD OF DENTAL EXAMINERS OF ALABAMACONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT.*Docket No. C-4757; File No. 191 0153**Complaint, September 28, 2021 – Decision, December 20, 2021*

This consent order addresses the Board of Dental Examiners of Alabama's violation of the FTC Act through the exclusion of new competition in the relevant market. The complaint alleges that the Board of Dental Examiners of Alabama prohibited dental assistants and other non-dentist practitioners from performing scans inside a patient's mouth without on-site dentist supervision thereby limiting new and innovative teledentistry platforms and the dentists who partner with these platforms. Under the order the Respondent must no longer impede clear aligner platforms or dental professionals affiliated with them from providing clear aligner therapy through remote treatment.

Participants

For the *Commission*: Philip Kehl, Elizabeth Gillen, and Melissa Westman-Cherry.

For the *Respondent*: Ashby Pate, Jackson Sharman, and Logan Matthews [*Lightfoot Law*].

COMPLAINT

Pursuant to the provisions of the Federal Trade Commission Act, and by virtue of the authority vested in it by said Act, the Federal Trade Commission ("Commission"), having reason to believe that the Respondent, Board of Dental Examiners of Alabama, has violated the provisions of said Act, and it appearing to the Commission that a proceeding in respect thereof would be in the public interest, hereby issues this Complaint stating its charges as follows:

NATURE OF THE CASE

1. This case challenges actions of the Board of Dental Examiners of Alabama ("Dental Board") that unreasonably exclude emerging competition from certain new and innovative teledentistry platforms, and the dentists who partner with these platforms. The Dental Board is comprised of seven members, six of whom are practicing dentists.

2. In recent years, dentists working with several new firms have started to offer teeth alignment treatment that differs from the traditional treatments offered through dental offices, such as braces or clear aligners prescribed following an in-office appointment with a dentist. In this new treatment model, patients are fitted for clear aligners following a visit to a storefront location, where a digital scan is performed by a dental assistant. The scan is then reviewed by a dentist working remotely. Patient interactions with dental professionals also take place on a remote basis. This mode of treatment often is substantially less expensive than traditional treatments.