ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 23-005

Investigation by LETITIA JAMES, Attorney General of the State of New York, of

Powerline Group Inc., Powerline Media LLC, Powerline Data LLC, Powerline Digital LLC, Powerline Commerce LLC, ILF Mobile Apps Corp., Auto Forward Data Services LLC, DDI Utilities Inc., DDI Data Solutions Inc., Highster Mobile Inc., Highster Data Services LLC, PhoneSpector LLC, Safeguarde LLC, BFG Marketing LLC, Digital Security World LLC, CTS Technologies Corp., and Patrick T. Hinchy,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") §§ 349 and 350 into the promotion and sale of mobile phone monitoring services by Powerline Group Inc., Powerline Media LLC, Powerline Data LLC, Powerline Digital LLC, Powerline Commerce LLC, ILF Mobile Apps Corp., Auto Forward Data Services LLC, DDI Utilities Inc., DDI Data Solutions Inc., Highster Mobile Inc., Highster Data Services LLC, PhoneSpector LLC, Safeguarde LLC, BFG Marketing LLC, Digital Security World LLC, and CTS Technologies Corp. (collectively, the "Corporate Respondents"), as well as Patrick T. Hinchy (the "Individual Respondent"), who serves as an officer of, and has a controlling interest in, each of the Corporate Respondents, in his individual capacity (collectively, the "Respondents"). This Assurance of

Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and the Respondents (collectively, the "Parties").

OAG's FINDINGS

1. Respondent Powerline Group Inc. is a Florida corporation with its principal place of business at 1660 Route 112, Suite F, Port Jefferson Station, New York.

2. Respondent Powerline Media LLC is a Florida limited liability company with its principal place of business at 10 Fairway Drive, Deerfield Beach, Florida.

3. Respondent Powerline Data LLC is a Florida limited liability company with its principal place of business at 980 North Federal Highway, Boca Raton, Florida.

4. Respondent Powerline Digital LLC is a Florida limited liability company with its principal place of business at 9025 Marina Boulevard, Boca Raton, Florida.

5. Respondent Powerline Commerce LLC is a Florida limited liability company with its principal place of business at 10 Fairway Drive, Deerfield Beach, Florida.

6. Respondent ILF Mobile Apps Corp. is a New York corporation with its principal place of business at 154 Horizon View Drive, Farmingville, New York.

7. Respondent Auto Forward Data Services LLC is a New York limited liability company with its principal place of business at 1660 Route 112, Suite F, Port Jefferson Station, New York.

8. Respondent DDI Utilities Inc. is a New York corporation with its principal place of business at 154 Horizon View Drive, Farmingville, New York.

9. Respondent DDI Data Solutions Inc. is a New York corporation with its principal place of business at 1201 Route 112, Suite 800, Port Jefferson Station, New York.

10. Respondent Highster Mobile Inc. is a New York corporation with its principal place of business at 407 East Main Street, Suite 1, Port Jefferson, New York.

11. Respondent Highster Data Services LLC is a New York limited liability company with its principal place of business at 1660 Route 112, Suite F, Port Jefferson Station, New York.

12. Respondent PhoneSpector LLC is a Delaware limited liability company with its principal place of business at 1201 Route 112, Suite 800, Port Jefferson Station, New York

13. Respondent Safeguarde LLC is a Delaware limited liability company with its principal place of business at 433 Plaza Real, Boca Raton, Florida.

14. Respondent BFG Marketing LLC is a Florida limited liability company with its principal place of business at 1615 South Congress Avenue, Suite 101, Delray Beach, Florida.

15. Respondent Digital Security World LLC is a Delaware limited liability company with its principal place of business at 2255 Glades Road, Suite 324A, Boca Raton, Florida.

16. Respondent CTS Technologies Corp. was a New York corporation with its principal place of business at 1 Field Lane, Miller Place, New York.

17. Respondent Patrick T. Hinchy is the owner and an officer of each of the Corporate Respondents. Individually or in concert with others, he formulates directs, or controls the policies, acts, or practices of the Corporate Respondents. His principal place of business is 8406 Hawks Gully Avenue, Delray Beach, Florida.

Respondents' Spyware Products

18. Since at least 2011, Respondent Hinchy, has owned and operated numerous entities, including the Corporate Respondents, that have promoted and sold software products designed to enable a purchaser to monitor the activity on another person's Android or iOS Mobile Device[1] (the "Target Device"). The products have been sold under the following brand names: Auto Forward, Easy Spy, DDI Utilities, Highster Mobile, PhoneSpector, Surepoint, and

[1] Defined below in Paragraph 75.b.

TurboSpy (collectively, "Respondents' Spyware Apps" and, individually, each a "Spyware App").

19. Once installed on a Target Device, the Spyware App will copy information from the Target Device and transmit it to Respondents' servers, where the information is made available for viewing by the purchaser of the Spyware App. Information copied and transmitted by Respondents' Spyware Apps includes: call logs (including phone number, date, and call duration); text messages (including message content, date, and recipient); camera images and videos (including the image or video itself and date taken); location (including current latitude and longitude of the device); Gmail data (including an excerpt/snippet of the email message content, email subject, sender and recipient email address, and date); WhatsApp messages (including message text, sender, and date); Skype data (including message content, sender, and date); Facebook, Instagram, and Twitter data (including direct message content, date, and sender); and Google Chrome data (including browser history with URL and dates visited).

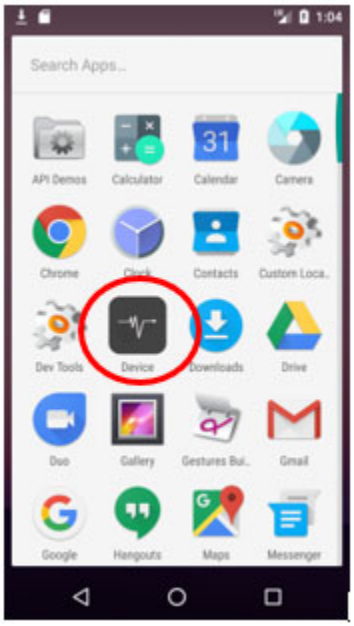
20. To access certain categories of information, such as social media logs, the user must modify the Target Device by bypassing protections put in place by phone manufacturers for the Spyware App to be able to access the phone's operating system. This process is known as "rooting" on Android devices and "jailbreaking" on iOS devices. Rooting an Android device or jailbreaking an iOS device generally invalidates any manufacturer's warranty for the device.

21. Some of the Respondents' Spyware Apps also enabled a user to remotely activate the camera or microphone of the Target Device to enable spying or eavesdropping on the owner of the device.

22. While installation of Respondents' Spyware Apps requires temporary access to the Target Device, the Spyware Apps provide no subsequent notifications to alert the owner of

the Target Device that information from the Target Device is being collected and exfiltrated by a Spyware App.

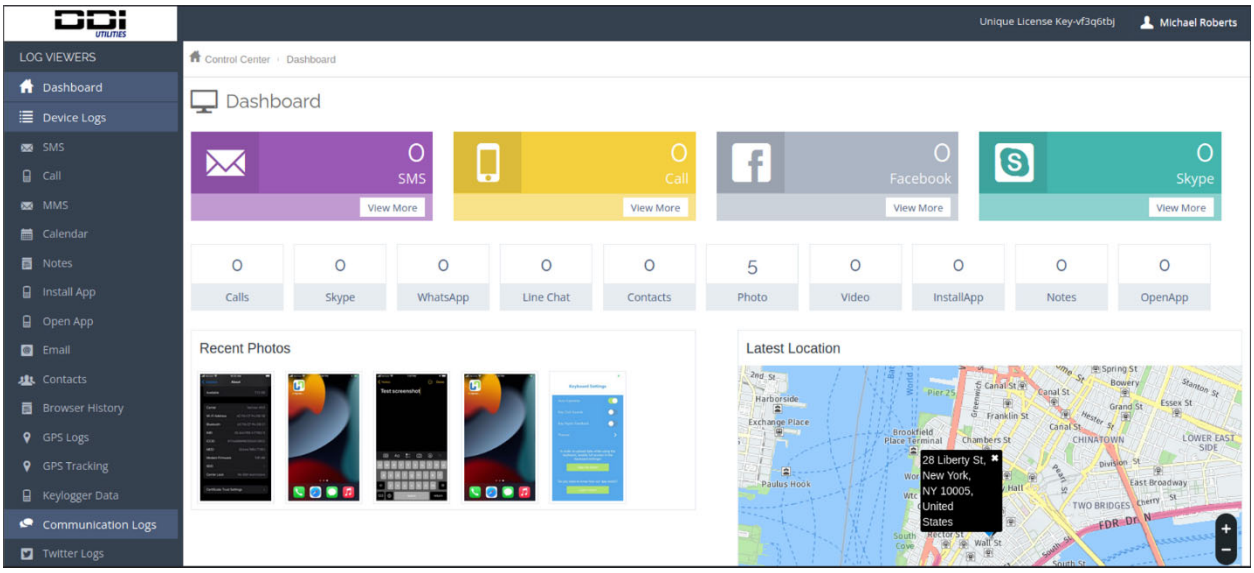
23. Once installed on a Target Device, the Spyware App will cause an icon to appear on the Target Device's home screen. Prior to changes to the iOS and Android operating systems, however, the icon could be hidden by the person controlling the Spyware App. In addition, up until October 2021, the icons for Respondents' Spyware Apps were generic and provided no indication that a Spyware App had been installed and was running on the Target Device.



[Icon for 2019 version of Highster Mobile for Android]

24. Customers[2] can view data that has been copied from the Target Device by Respondents' Spyware Apps and uploaded to Respondents' servers by logging into a web dashboard. As seen below, the main dashboard page shows a map with the Target Device's location and indicates the number of various types of communications that have been captured as well as recent photos and videos, social media activity, and newly installed apps.

[2] Defined below in Paragraph 75.f.



25. Some of Respondents' Spyware Apps also allowed the user to remotely execute a series of "stealth commands" from the web dashboard. Some of these commands, as seen below, included activating the camera, removing any traces of the installation of the Spyware App, unlocking the Target Device, and hiding the Spyware App icon.

Settings

We have recently published a revised version of our privacy policy. Please read through these revisions and take some time to fully understand them and how they might affect you. Your use of evt17.com is subject to these revisions. OK

Send a stealth command to target device. If device is not connected to Internet, you can alternatively send comands via sms. Note that on Android 4.4 and higher sms will drop in inbox and user will see it. You can see stealth commands delivery reports here (/iphone/users/stealth_commands_listing)

STEALTH COMMANDS		
Command	**Send Stealth Command**	**Send SMS Command***
Stealth Camera	Send	#$#pic#$#
Remove Installation Traceability	Send	#$#trace#$#
Lock Target Phone (to unlock the device please input the license key)	Send	#$#lock#$#
Unlock Target Phone	Send	#$#unlock#$#
Get Location	Send	#$#gps#$#
Restart Services	Send	#$#restart#$#
Show Application Icon on Device	Send	#$#showicon#$#
Hide Application Icon on Device	Send	#$#hideicon#$#

*on Android 4.4 and higher sms will drop in inbox and user will see it.

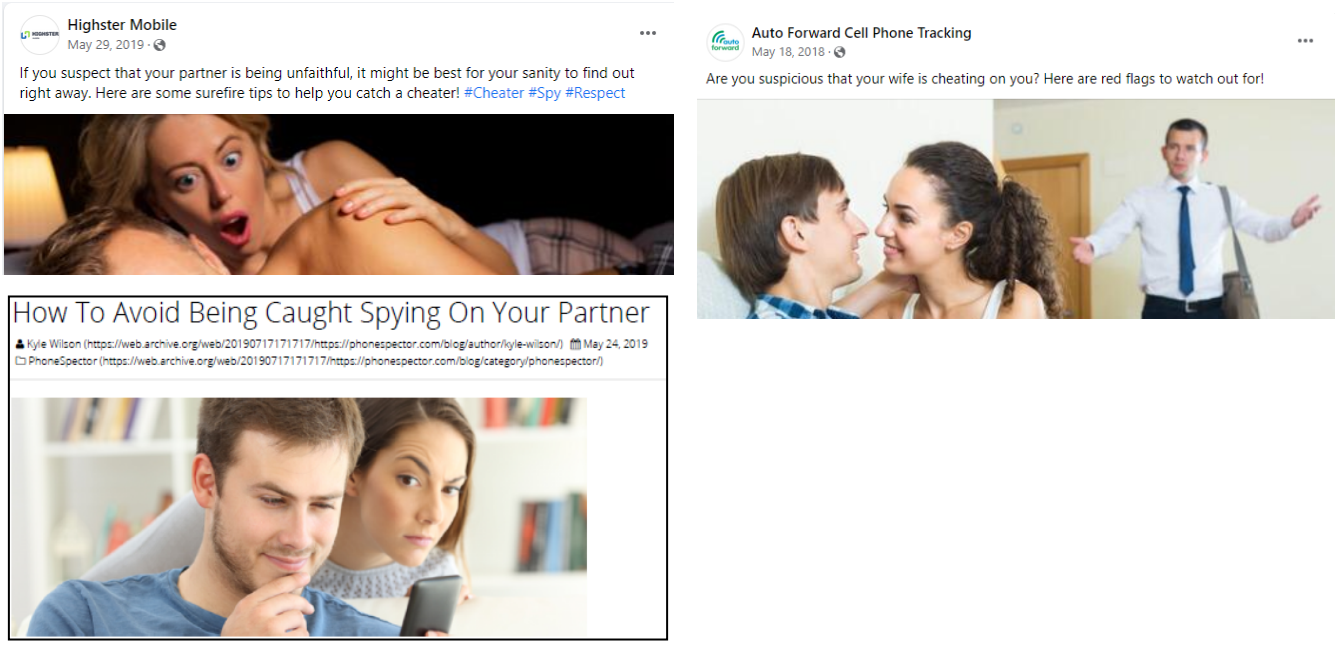
[Stealth Command Menu from dashboard for 2019 version of Highster Mobile for Android]

26. In addition to Respondents' Spyware Apps, Respondents offered products for monitoring iOS devices that did not require accessing or installing any software on the Target Device (together with Respondents' Spyware Apps, "Respondents' Spyware Products"). Instead,

these products worked by exfiltrating information from the iCloud account associated with the Target Device. A Customer wishing to use this type of Spyware Product sold by Respondents thus had to obtain the login credentials for the iCloud account associated with the iOS device they intended to monitor. The Customer would provide those credentials to Respondents whose software, in turn, would use the credentials to access the iCloud account and copy the same type of information as described above in Paragraph 19. The Customer would then be able to view the information through a web dashboard as described above.

Respondents Misrepresented the Legal Risks of Using the Spyware Products for Covert Spying

27. Respondents' marketing focused heavily on promoting the Spyware Products for covert spying on adults without the consent of the device owner and misleadingly implied that such use was legally permissible.



[Screenshots from Highster Mobile Facebook Page (at upper left), phonespector.com/blog (at lower left), Auto Forward Facebook page (right)]

28. Respondents' promotional materials targeted individuals hoping to catch a cheating spouse or intimate partner by stating that the Respondents' Spyware Apps could be installed on the Target Device without the knowledge or consent of the device owner. For example, a May 2019 blog post on the PhoneSpector website, titled "How To Avoid Being Caught Spying On Your Partner" made the following claims about the PhoneSpector Spyware App:

> While your partner's phone likely contains the answers you're looking for, accessing that information is a lot easier said than done. It's difficult enough to find the right moment to look through your partner's phone. Especially if they're having an affair, as they'll likely be doing everything they can to keep it a secret. Even worse, if they catch you snooping through their device (and they're not cheating on you) they may never trust you again. This is where PhoneSpector comes in. It allows you to monitor all their phone activity, without the risk to be caught spying.[3]

The post went on to describe the PhoneSpector Spyware App as "completely undetectable."[4]

29. Articles posted on the blogs linked to the websites of Highster Mobile and Auto Forward, under the heading of "relationship advice," encouraged consumers to use the Spyware Products to spy on a partner suspected of cheating. For example, a blog post on the Highster Mobile website, published in June 2019, advised consumers, "If you are suspicious of your partner, trust your gut. It's telling you something for a reason. Download Highster Mobile and hack into their phone and uncover the truth."[5] A November 2018 blog post on the Auto Forward website, titled "How to Spy on Husband's Cell Phone with Convenience," stated that for "wives, the best thing about this monitoring software is the fact that they can easily spy on their husband's cell phone device without the latter knowing about it," and that using the Auto

[3] www.phonespector.com/blog/how-to-avoid-being-caught-spying-on-your-partner/index.html, captured on August 16, 2019.
[4] *Id.*
[5] www.highstermobile.com/blog/hack-someones-phone-with-just-their-number/index.html, captured on August 16, 2019.

Forward Spyware App for such covert monitoring can "can help placate or affirm issues encountered during marriage."[6]

30. In addition to product websites, Respondents promoted the use of Respondents' Spyware Products as tools for catching a suspected cheater through a number of purported independent review sites owned and operated by Respondents.

31. For example, Safeguarde.com published an article in May 2022, titled "Best Apps to Spy on a Cell Phone," stating that "[w]hile there are many reasons someone would need to spy on texts (if you are an employer or a parent for instance,) catching a cheating spouse is the most popular."[7] The article, which recommended Respondents' Spyware Apps Auto Forward Spy, Highster Mobile, DDI Utilities, and PhoneSpector as the "best spy apps for the average person," stressed the importance the undetectability of the Spyware Apps:

> Stealth is one of the most important aspects of a cell phone spy and text message tracker. Being able to track another person's cell phone or tablet usage undetected is of utmost importance to the purchaser. The hard truth is that if you want to spy on SMS texts, listen in on phone calls, and take pictures remotely without being detected, you're going to need a good spyware app. One that is *invisible and untraceable at all times*. [emphasis added][8]

32. Content published by Respondents even went so far as to state that unauthorized installation of a Spyware App on and the subsequent monitoring of another adult's Mobile Device was legal. For example, a promotional article, titled "Five Best Cell Phone Spy Apps for Android and iPhone You Can Use to Spy On Your Partner," which was reviewed by Respondent Hinchy prior to publication in early 2019, stated that "no special clearances" are required to "use

[6] www.auto-forward.com/blog/spy-husbands-cell-phone-convenience.html, captured on August 16, 2019
[7] https://safeguarde.com/best-spy-apps-for-iphone/, captured on October 18, 2022.
[8] *Id.*

spy applications to track and view someone's text messages, emails, call log, social media activity, photos, videos, real-time GPS location, and more."[9]

33. In some instances, Respondents' customer support staff reinforced the impression that use of the Respondents' Spyware Products for covert spying on adults was legally permissible by assisting Customers who made clear that they were indeed using Respondents' Spyware Products to covertly monitor intimate partners.

34. For example, a Customer who contacted customer support regarding one of Respondents' Spyware Apps in 2017, asked "how can I hide the app from him seeing it?", noting that "if he sees it then it's over so please explain." Without asking any questions about whose phone the Customer was attempting to monitor, Respondents' customer support representative responded by stating that the "app name is visible on the homescreen but it can be hidden" and went on to provide instructions for hiding the app icon.

35. In some cases, Respondents' customer support staff even assisted Customers with hacking into accounts of their intimate partners in order to activate a Spyware Product. For instance, a customer support ticket from November 2017 noted that the Customer requesting assistance "said that she wants to get data from his husband's iPhone and was informed that she needs to get his iCloud username and password" but that "she doesn't know what his iCloud username and password is." In response, support staff suggested that the problem might be addressed by "guessing his iCloud account" and provided guidance to the Customer on trying to guess the password. The instructions noted that the credentials "might or might not be the same with the person's normal email account" and warned that the Customer would only be allowed 3-

[9] www.bestcellphonespyapps.com/BestCellPhonespyapps.com/bestcellphonespyapps.com/best-cell-phone-spy-apps-for-android-and-iphone/index.html, captured on August 19, 2019.

5 attempts. Respondents' customer support also advised the Customer not to use a feature that would cause an email to be sent to her husband.

36. By openly promoting Respondents' Spyware Products for spying on adults without consent of the device owner and actively assisting Customers in such use, Respondents created the false impression that such use was permissible. However, as described below, Respondents' own disclaimers and terms and conditions acknowledged that Customers who use Respondents' Spyware Products to spy on another adult without consent risk violating numerous state and federal laws, as well as the Spyware Products' terms and conditions.

Respondents Disclaimers Were Hidden and Legally Insufficient

37. Despite promoting the Respondents' Spyware Products as tools for covertly monitoring the device of another adult, the terms and conditions page on most of the Respondents' Spyware Products websites acknowledged that such use violates state and federal criminal statutes as well as the Spyware Products' terms and conditions, and several included relevant portions of the Computer Fraud and Abuse Act, which prohibits intentionally accessing a computer, including a smartphone, without authorization.[10]

38. Respondents included similar disclaimers in the terms and conditions pages of the purported independent review sites that they owned and controlled, one of which included an admission that "it's illegal in most countries to install monitoring / surveillance software onto a cell phone which you do not own or have proper authorization to install."[11]

39. Such advisories and disclaimers, however, were not prominently displayed and were unlikely to be discovered by the average consumer purchasing Spyware Products in

[10] *See, e.g.*, www.highstermobile.co/terms/index.html; www.auto-forward.com/terms/index.html; www.surepointspy.com/terms-and-conditions/index.html, all captured on August 16, 2019.
[11] www.Safeguarde.com, captured on August 16, 2019.

response to Respondents' express recommendations to use Respondents' Spyware Products for covert surveillance of a suspected cheater.

40. In instances where Respondents did address the legality of covert monitoring with Respondents' Spyware Products in FAQ pages, Respondents provided no information on criminal laws prohibiting unauthorized monitoring of Mobile Devices and only described the use of Respondents' Spyware Products for potentially legal uses, such as monitoring custodial minor children and employees with notification.[12]

Respondents Did Not Disclose Affiliation with Purported Third-Party Review Sites

41. As mentioned above, Respondents owned and operated several websites that misleadingly identified themselves as purveyors of independent, unbiased product reviews designed to assist Customers in choosing the best spyware products. In reality, these sites were owned and controlled by Respondents for the express purpose of promoting and endorsing Respondents' Spyware Products.

42. For example, Respondents' sites bestcellphonespyapps.com and safeguarde.com both contained identical "affiliate disclosure" disclaimers that falsely claimed that the sites were "independently owned" and that the site operators "always post honest opinions, findings, beliefs, or experiences based on our research and/or experience with the product or service."[13]

43. Similarly, Respondents' site, top5powerguide.com, expressly misrepresented the independence of its published content:

> We want to make it clear that we do not get paid to write our reviews. We do what we do because we have a passion for all things digital and we fully stand behind everything we test, research, and review. To keep our website alive, we ultimately need to monetize our efforts which occurs through advertising, sponsors, and affiliate relationships. These ways of generating revenue do not

[12] www.highstermobile.co/faq/index.html, captured on August 16, 2019.
[13] www.bestcellphonespyapps.com/disclaimer/index.html; www.safeguarde.com/disclaimer/index.html, both captured on August 16, 2019.

> affect how we review our products, define our rankings, or create our content — we promise![14]

44. In addition, the only products recommended and promoted in the articles on these sites were Respondents' Spyware Products. For example, a January 18, 2018, blog post on Digitaladdicts.com, titled "Best Spy Apps: How To Spy on a Cell Phone," claimed that the use of spyware to "spy on a girlfriend, boyfriend, husband, or wife" was the reason that "so many cell phone spy apps have been hitting the market over the last decade."[15] The article went on to state its intent to show the reader which particular "cell phone spy apps are worth your time, trust and money" and encouraged readers to purchase Highster Mobile, DDI Utilities, and PhoneSpector.[16] Respondents published a similar article on safeguarde.com that listed Auto Forward, Highster Mobile, and PhoneSpector as "the top 3 apps for spying on text messages."[17]

45. Another blog post published by Respondents, titled "PhoneSpector Review – 2019's Best Cell Phone Spy App," boldly claimed that the "PhoneSpector phone spy app is the best cell phone spy app for all Androids and iPhones."[18] The site also included purported reviews of other of Respondents' Spyware Apps, Auto Forward, Highster Mobile, Surepoint Spy, Easy Spy, and DDI Utilities, all of which recommended the products for purchase.[19] In contrast, reviews for two products offered by competitors of Respondents concluded that the products were overpriced and readers would be better served purchasing one of Respondents' Spyware Products.[20]

---

[14] www.top5powerguide.com/about/index.html, captured on August 16, 2019.
[15] www.digitaladdictsblog.com/superior-apps-spying-superior-spy-apps/index.html, captured on August 16, 2019.
[16] *Id.*
[17] www.safeguarde.com/index.html, captured on August 16, 2019.
[18] www.bestcellphonespyapps.com/best-cell-phone-spy-app-available/index.html, captured on August 16, 2019.
[19] www.bestcellphonespyapps.com, captured on August 16, 2019.
[20] *Id.*

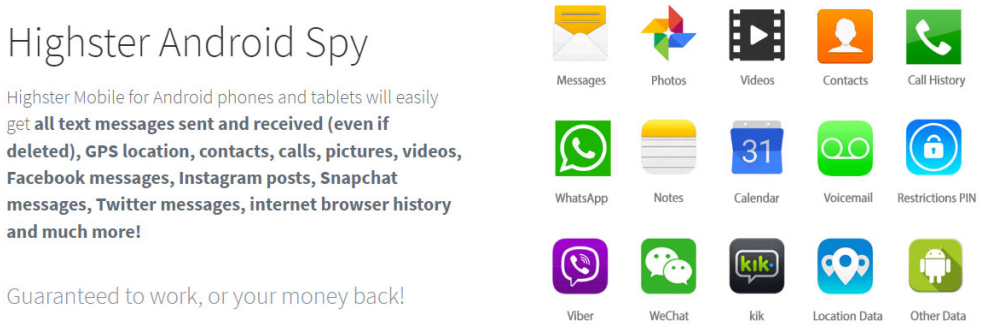
46. Adding to the deceptive nature of these sites, Respondents published content under the names of fictitious authors, who were identified as being purported experts committed to providing readers the most accurate information about different spyware products on the market. One such pseudonym that appeared frequently in articles on the review sites described above was "Pat Stanley", who was described as a spyware "expert" who had "researched and used pretty much all the cell phone spyware currently available on the internet," and wanted to "help make the best choice for you, so your investment will return the 'dividends' you're after."[21]

47. The claims that the authors of these reviews were independent and unbiased experts were false. In fact, the purported reviews, including articles by fictious authors like Pat Stanley, were written by employees of the Corporate Respondents who reported directly to Respondent Hinchy, who was responsible for approving all such content and worked with a vendor in connection with updating information about Pat Stanley on bestcellphonespyapps.com and other sites where promotional content was published.

Respondents Misrepresented Product Features

48. Respondents' promotional and marketing materials stressed the ability of the Respondents' Spyware Apps to allow their Customers to view messages and other content from third-party apps like Gmail, Facebook, and Instagram.

[21] www.bestcellphonespyapps.com/best-cell-phone-spy-app-available/index.html, captured on August 16, 2019.



[Screen shot from August 2019 site copy of www.highstermobile.co]

49. Access to social media logs and other incoming messages on third-party apps like WhatsApp, however, required performing the invasive process of rooting or jailbreaking the Target Device to allow the Spyware App to access the device operating system.

50. The OAG's examination of one of Respondents' Spyware Apps, Highster Mobile, confirmed that rooting an Android device was a requirement for the Spyware App to access Facebook, Gmail, Instagram, Line, Skype, Snapchat, Twitter, and WhatsApp. Once installed, the Highster Mobile Spyware App checks to see if the device has been rooted and, if so, modifies the filesystem-level permissions so that it can monitor communications that are sent and received by those apps.[22]

51. Respondents failed to provide adequate disclosures of the rooting or jailbreaking requirement and the risks associated with performing such procedures, risks which could include damaging the Target Device, voiding the device warranty, and disabling security protections on the device.

52. For example, while the FAQs for Highster Mobile promoted the Android version's ability to "get . . . Facebook messages, Instagram posts and Snapchat messages," they

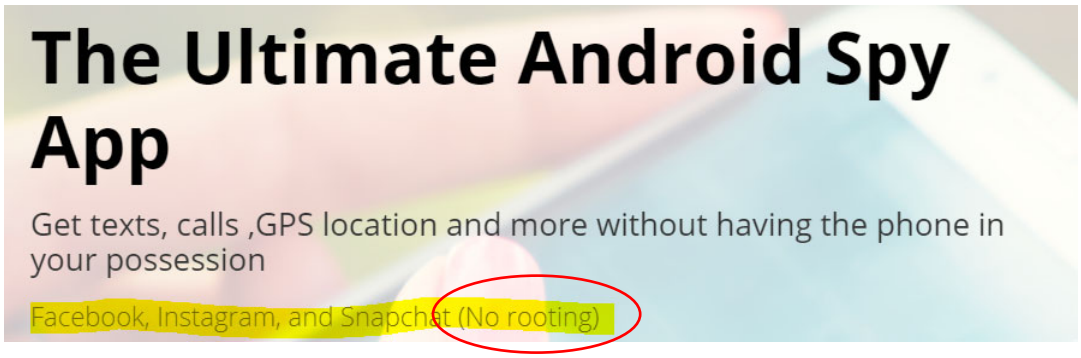
[22] The OAG confirmed this operation on the 2019 and 2022 versions of Highster Mobile.

made no mention of the need to root Android devices to enable the Highster Mobile to access such information.[23]

53. Respondents also repeatedly made false claims on product websites and review sites that rooting was not required for access to third-party messaging and social media apps. Respondent Hinchy personally reviewed and approved the publication of such content.

54. For instance, a purported "review" of the Spyware App, PhoneSpector, posted on BestCellPhonespyapps.com in December 2017, and still available in August 2019, touted PhoneSpector as the "best cell phone spy app for all Androids and iPhones."[24] The cited author, Pat Stanley, claimed to have tested the product and claimed that it was "undetectable," worked on "all Androids and iPhones," and that "[n]o physical phone possession or access" was needed. The review also stated that PhoneSpector was able to access "Facebook messages without having to root the Android device."[25]

55. The article contained a link to the PhoneSpector website, which also included false claims that social media content could be accessed without rooting the device.



[23] *See, e.g.*, www.highstermobile.co/faq/index.html, captured on August 16, 2019. The FAQs did note that "Apple devices will need to be jailbroken before the application can be installed."
[24] www.bestcellphonespyapps.com/best-cell-phone-spy-app-available/index.html, captured on August 16, 2019.
[25] *Id.*

56. A careful review of the PhoneSpector website in 2019, however, reveals that physical access is, in fact, required to install PhoneSpector on an Android device and that the device must be rooted in order to gain access to social media apps, such as Facebook. At the bottom of the PhoneSpector homepage, a disclaimer notes that "[p]hysical access to the Android phone for approximately 45 seconds is required."[26]

57. The terms and conditions page on the PhoneSpector website also contained the following vague statement, acknowledging the need to root Android devices in order to enable any features that are not part of the "basic package".[27]

> You may use basic features package on a device without it jailbreaking (iOS) or rooting (Android). In case you require more features in any other premium or phone and computer packages you will need to make a jailbreak (iOS) or root (Android), which is a legal procedure according to the final rule of the Copyright Law of the United States.

58. Customer support communications confirm that, like all of Respondents' Spyware Apps for Android devices, rooting was indeed required for PhoneSpector to gain access to social media content and messages on the Target Device. The requirement was also acknowledged in some of Respondents' promotional content, including a January 2019 blog article for bestcellphonespyapps.com by fictitious author Pat Stanley, which stated that "[r]ooting an Android device isn't necessary *unless you want to see certain information such as; Facebook, Twitter, Instagram, Emails, WhatsApp, and other app related data*."

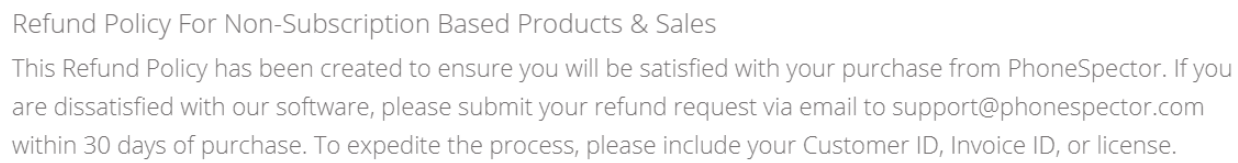
Respondents Misled Customers Regarding their Refund Policy

[26] www.phonespector.com, captured on August 16, 2019.
[27] www.phonespector.com/terms-of-use/index.html, captured on August 16, 2019. The PhoneSpector website was subsequently updated to include an FAQ page, that contained the following statement under the question "which features require rooting?", "On the Android device, rooting of the monitored phone is required to retrieve emails and Incoming messages from Facebook, Instagram, Snapchat, WhatsApp and Skype."

59. Respondents misled Customers with respect to the applicable refund policies by falsely claiming that the Spyware Products came with a "money back guarantee," hiding a condition in the refund policy that made it impossible to obtain a refund after any use of the product and confusingly including separate refund policies for different purchase models.

60. For example, the PhoneSpector website claimed that both the Android and iPhone versions of the product came with a "30-day money back guarantee."[28]

61. Similarly, the posted refund policies for DDI Utilities, Highster Mobile, and PhoneSpector instructed purchasers to submit refund requests within 30 days of purchase and goes on to state that the product refund policy was "designed" to "ensure" that the Customer will be "satisfied"[29] or "happy"[30] with their purchase.



[DDI Utilities Refund Policy – August 2019].

62. The refund policies for Easy Spy and SurePoint advised Customers that if they were not "fully satisfied" with their purchase, they "can be eligible for a full refund according to Refund Conditions outlined below."[31]

---

[28] www.phonespector.com/refund-policy/index.html, captured on August 16, 2019.
[29] *Id.*
[30] www.ddiutilities.com/refund-policy/index.html, captured on August 16, 2019.
[31] *See* www.surepointspy.com/refund-policy/index.html; www.buyeasyspy.com/refund_policy.html, captured on August 16, 2019.

63. Respondents reinforced the perception that Customers who were dissatisfied with the performance of Respondents' Spyware Products could obtain a refund in promotional materials that promoted Respondents' Spyware Products and claimed they came with a "money-back guarantee."

64. Towards the end of Respondents' Spyware Products' refund policies, however, was a "condition" that stipulated that no refunds would be issued if the license key had been activated (which was necessary to download or otherwise test the functionality of the app) or if the "software had been used in any capacity whatsoever."[32] Customers were thus provided no ability to evaluate the product and no opportunity for a refund if they were unsatisfied with the App's performance.

65. Respondents added to the likelihood that Customers would fail to understand the strict refund policies for the Spyware Products by including refund policies for "subscription" and "non-subscription based products and sales" when there was only one purchase mode available, either subscription or one-time purchase, for each of Respondents' Spyware Products.[33]

66. Respondents have since revised the text of the refund policies, but Customers are still unlikely to understand that refunds are unavailable if there has been any use of the product. The revised policies state that Customers may be eligible to receive a "full refund within 14 days following the day of your purchase as long as the refund reasons do not contradict the Refund Policy conditions below."[34]

---

[32] *See* notes 27-29.

[33] In August 2019, Highster Mobile and PhoneSpector were subscription based, with recurring payments of $29.99 (basic) or $39.99 (pro). DDI Utilities, by contrast, was available for a one-time payment of $69.99.

[34] https://highstermobile.co/refund, captured on October 29, 2022.

67. As seen below, the policy initially lists six reasons, generally related to user or device issues, for which a refund will be refused.

> **Subject to the applicable law and to this Refund Policy conditions, you may be eligible to receive a full refund within 14 days following the day of your purchase as long as refund reasons do not contradict the Refund Policy conditions outlined below.**
>
> - No refund will be issued after 14 days have passed since the purchase date.
> - The claim for refund may apply only to the primary Highster Mobile license (No refund will be issued for Premium Support or Extended Download Warranty).
> - If you purchased additional services and/or products or subscription/s in another order, you must specify which account you are requesting to be refunded.
> - No refund will be issued if a user refuses to re-install or re-link Highster Mobile Software in the event of the performed upgrade of the operating system on the target device.
> - No refund will be issued if a user's target device is not in compliance with the Highster Mobile Compatibility Policy.
> - No refund will be issued if the target device has lost connection due to the absence of internet access, factory reset or update to the latest operating system version.

[Highster Mobile Refund Policy – October 2022].

68. Notably, none of the initial six conditions would prevent a Customer who had successfully installed one of Respondents' Spyware Apps from receiving a refund within 14 days of his or her purchase based on dissatisfaction with the product.

69. Only if a reader continues to the bottom of the next section, which lists 20 *additional* reasons for which a refund will be refused and that are purportedly "completely beyond [the Respondent entity's] control" would the reader find number 19, which states, "No refund will be due if the purchased product's license key is activated by clicking the YOUR DOWNLOAD LINK field in the Activation email or if any data from a device is uploaded to an online account."[35]

[35] *Id.*

Respondents Misrepresented the Security of the Spyware Apps

70. Respondents published statements that would lead a reasonable consumer to assume that any information copied from a Target Device by one of Respondents' Spyware Apps would be transmitted and stored in a secure environment. For example, a 2016 article published by Respondent described the Auto Forward Spyware App as a "safe and secure cell phone surveillance app." Another article published by Respondents in 2019 expressly stated that information copied from a Target device was transmitted to the "cell phone spy server" through a "secure connection."

71. These representations were misleading. Prior to October 2021, all of Respondents' Spyware Apps transmitted data copied from Target Devices to Respondents' servers through an unsecure, unencrypted connection. As noted in one of Respondents' published articles discussing the benefits of using a virtual private network, unencrypted data is vulnerable to being intercepted and viewed by "your ISP, the government, hackers and other third parties." The article goes on to explain that encrypted data, by contrast, "looks like gibberish to anyone who intercepts it" and is thus "impossible to read."[36] Despite having a clear understanding of the importance of encrypting sensitive data before transmitting sensitive data over public or private networks, Respondents supplied customers with Spyware Apps that failed to provide this basic security measure for over six years.

72. The OAG finds that Respondents' conduct violated Executive Law § 63(12), which authorizes the OAG to pursue repeated fraudulent or illegal acts, and GBL §§ 349 and 350, which prohibit deceptive acts and practices and false advertising.

73. Respondents neither admit nor deny the OAG's Findings, paragraphs 1-72 above.

[36] https://bestcellphonespyapps.com/whats-the-best-vpn-for-android/, captured on August 19, 2019.

74. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), GBL §§ 349 and 350.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

75. For the purposes of this Assurance, the following definitions apply:

a. "Clear(ly) and Conspicuous(ly)" mean 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:

i. 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 or streaming video, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("Triggering Representation") is made through only one means.

ii. 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.

iii. 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.

iv. In any communication using an interactive electronic medium, such as the internet or software, the disclosure must be unavoidable.

v. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the Triggering Representation appears.

vi. The disclosure must not be contradicted or mitigated by, or inconsistent with, any other representation(s).

vii. The disclosure must not be combined with other marketing or promotional text or information that is unrelated or immaterial to the subject matter of the disclosure or not legally required.

viii. The disclosure must be in close proximity to the Triggering Representation.

b. "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.

c. "Spyware" or "Spyware Products" means any software, product, or service that enables users to track or monitor another person's activities on a Mobile Device, including but not limited to, text messages, web browser history, geolocation, photos, and social media activity.

d. "Spyware App" means a Spyware Product that is installed and run on an iOS or Android Mobile Device and transmits information copied from the device for viewing on another platform or device.

e. "Covered Business" means (a) Corporate Respondents; and (b) any business that Respondents control, directly or indirectly, that promotes, markets, offers, sells, or distributes Spyware Products or any other Mobile Device monitoring services. Covered Business does not include any business that offers only services unrelated to Mobile Device monitoring (e.g., people search services).

f. "Customer" means the consumer who has attempted to or completed the purchase of or subscription to one or more of the Spyware Products offered by Respondents, or a user of such Spyware Products.

g. "Target Device" means the Mobile Device on which the Customer has downloaded or installed or intends to download or install one or more of the Spyware Apps offered by Respondents in order to review the data associated with that device.

h. "Target Device Holder" means the person who uses and/or possesses the Target Device and whose data is being accessed by the installed Spyware Products.

i. "Target Account" means the online account or service used to store Mobile Device data (e.g., an iCloud account) to which the Customer has connected one or intends to connect or more of the Spyware Products offered by Respondents in order to review the data stored in that online account or service.

j. "Target Account Holder" means the person who uses and/or possesses the Target Account and whose data is being accessed by the connected Spyware Products.

k. "Promotional Material" means any documents, communications, or other media created by, solicited by, or otherwise approved of by Respondents for the purpose of promoting, marketing, or publicizing Spyware Products, including but not limited to advertisements, web pages, streaming videos, advertorials, blog posts, and sponsored product reviews.

l. "Refund Policy" means any contract term, agreement, or other policy adopted by Respondents regarding when, if, and under what circumstances Customers can receive a full or partial refund of moneys paid for Spyware Products, including but not limited to any purported guarantees Respondents may provide that a consumer will be satisfied with their purchase of or subscription to a Spyware Product.

m. "Transition Date" means the date by which all Covered Businesses must comply with the terms of this Assurance and shall be one hundred twenty (120) days from the date this Assurance is executed in full (the "Effective Date").

76. Respondents shall comply with Executive Law § 63(12) and GBL §§ 349 and 350 in the advertising and sale of software and related services and agree to adhere to the following terms with respect to the operation of all Covered Businesses.

Misrepresentations in the Marketplace and/or to Customers

77. Respondents shall not misrepresent, expressly or by implication, the legality of using of Spyware Products to monitor Mobile Devices, including but not limited to by:

a. Representing that Spyware Products can be legally used to surreptitiously monitor the Mobile Device of a spouse or intimate partner;

b. Representing that data derived from Spyware Products may be admissible as evidence in a court proceeding; and,

c. Representing that Spyware is intended to be used to covertly monitor the activities of adults who have not consented its use.

78. Respondents shall not make misrepresentations, expressly or by implication, regarding whether Respondents' Spyware Products have been reviewed by, approved of, or otherwise tested by independent third parties.

79. Respondents shall Clearly and Conspicuously disclose any financial relationship between Respondents and the authors and/or publishers of any articles, blog posts, and product reviews.

80. Respondents shall Clearly and Conspicuously disclose that any Promotional Material is a sponsored advertisement paid for by Respondents, including but not limited to on all third-party websites where Respondents have paid to have Promotional Material placed.

81. Respondents shall not misrepresent, expressly or by implication, the security measures used to protect the data collected by Respondents' Spyware Products.

Suspension of Access to and/or Deletion of Data Collected Prior to Transition Date

82. On or before the Transition Date, for any Customers who have not complied with the Affirmation and Notice requirements set forth in Paragraphs 86-88 below, Respondents shall (a) suspend all Customer access to data collected by use of Respondents' Spyware Products, including but not limited to suspending Customers' access to the dashboards through which they

typically access data collected by Respondents' Spyware Products, and (b) prevent Customers from accessing data collected by Respondents' Spyware Products on a going forward basis.

83. Respondents shall not provide any services in connection with, support for, or any further use of its Spyware Products for Customers who have not complied with the Affirmation and Notice requirements set forth in Paragraphs 86-88 below by the Transition Date.

84. If a Customer objects to any suspension provided in Paragraphs 82-83 above, and/or makes any other related inquiry, Respondents shall explain the relevant terms of this Assurance and the Affirmation and Notice requirements in a clear and concise manner.

85. Within 60 days of the Transition Date, Respondents must identify all data associated with accounts for which either the Customer or Respondents have not yet completed the steps set forth in Paragraphs 86-88 (the "Non-Compliant Data"). On or by the 60th day after the Transition Date, Respondents must delete or quarantine all Non-Compliant Data such that all Non-Compliant Data is inaccessible by all Customers and that access to the Non-Compliant Data cannot be restored to any Customer for any reason. If Respondents choose to quarantine the Non-Compliant Data rather than delete it, Respondents must quarantine the data in a manner that ensures it cannot be accessed by any third parties unless required by law. Nothing in this Assurance requires Respondents to delete or destroy data and/or withhold data from production to the extent that data is subject to a litigation hold, preservation notice, or other request by a government agency and/or preservation or production thereof is otherwise required by law, regulation, or Court order.

Affirmations Required for Ongoing and/or Future Use of Spyware Products

86. On or before the Transition Date, Respondents shall require each Customer that purchases or subscribes to Respondents' Spyware Products, or otherwise requests access to the data collected by one of Respondents' Spyware Products, to provide an express electronic

acknowledgment regarding the lawfulness of the Customer's use of the Spyware Product(s), including, at least (a) that the Customer will use Spyware Product(s) for legitimate and lawful purposes, and (b) that the Customer is authorized to install and/or otherwise connect the Spyware Product(s) to the Target Device and/or Target Account (the "Affirmation"). The Affirmation shall also comply with the requirements set forth below in Paragraphs 87-88 (the "Affirmation Requirements").

87. The Affirmation shall:

a. Be presented to the Customer of the Spyware Product(s) in a distinct, standalone screen or box during the purchase process and/or in a separate flow established for existing Customers.

b. Require the Customer of the Spyware Product(s) to affirmatively acknowledge that the Spyware Product(s) may only be used for legitimate and lawful purposes.

c. Disclose, in a Clear and Conspicuous manner, that using Spyware Product(s) to monitor the Mobile Devices and/or other activities of adults who have not consented to the installation and/or use Spyware Product(s) on their Mobile Devices and/or related accounts is not permitted and that it's illegal in most countries to install monitoring / surveillance software onto a cell phone which you do not own or have proper authorization to install software on.

d. Include a Clear and Conspicuous link to the terms and conditions page of the relevant product website.

e. Include a Clear and Conspicuous option that allows the Customer and/or user of the Spyware Product(s) to refuse to provide the Affirmation. If the

Customer and/or user of the Spyware Product(s) selects this option, Respondents must immediately discontinue that Customer's purchase of the Spyware Product(s) and/or terminate that Customer's access to any data collected by the Spyware Product(s).

f. Require the Customer and/or user of the Spyware Product(s) being purchased or accessed to provide the following information regarding the intended monitoring use of the Spyware Product(s) by selecting one of the following options:

   i. The Mobile Device to be monitored is used by an adult over the age of 18 who is aware of and consented to both (a) the installation of the Spyware Product(s) on the device and (b) all monitoring performed on the device using the Spyware Product(s).

   ii. The Mobile Device to be monitored is used by an adult employee of the Customer of the Spyware Product(s), and the employee has been notified that the device will be monitored using the Spyware Product(s).

   iii. The Mobile Device to be monitored is used by a minor child who is in the custody of the Customer of the Spyware Product(s). Any Customer that selects this option must be required to follow the further steps set forth in Paragraph 103.

   iv. The Mobile Device to be monitored is used by the Customer and all data to be monitored by use of the Spyware Product(s) belongs to the Customer.

88. The Affirmation flow shall conclude with an advisory that, unless the Customer selected that they intend to use the Spyware Product(s) to monitor a minor dependent child (as set forth in Paragraph 87.f.iii above) and completed the additional necessary steps regarding the monitoring of a minor child (as set forth in Paragraph 103 below), the Spyware Product(s) will notify the Target Device Holder and/or Target Account Holder that (a) the Spyware Products have been installed on their Mobile Device and/or connected to their Target Accounts and (b) the Spyware Product(s) may be used to monitor their Mobile Device activity (the "Notification").

89. On or before the Transition Date, Respondents shall require all existing Customers who purchased and/or subscribed to the Spyware Products to complete the Affirmation described in Paragraphs 86-88 during the dashboard login process. After the Customer is presented with the Affirmation flow, the Customer shall not be permitted to access their account dashboard and/or any other data collected by the Spyware Products unless and until the Customer has completed the Affirmation.

90. On or before the Transition Date, Respondent shall require all Customers who purchase or renew a Spyware Product to complete the Affirmation described in Paragraphs 86-88 prior to completing the transaction. After completing the Affirmation, Customers shall be advised of the Notifications to the Target Device Holders and/or Target Account Holders unless the Customer has affirmed that they intend to use the Spyware Products to monitor a minor custodial child and has completed the additional necessary steps regarding the monitoring of a minor child (as set forth in Paragraph 103 below). The advisory shall be presented in accordance with the following conditions:

a. The advisory regarding the Notification shall be presented to the Customer only after the Customer has made the selection of the intended monitoring use set forth in Paragraph 87.f above.

b. Once the advisory has appeared to the Customer, the Customer shall not be permitted to return to an earlier point in the Affirmation flow to make any changes to their selections, including but not limited to their selection of the intended monitoring use set forth in Paragraph 87.f above.

91. Respondents may not, directly or indirectly, assist any Customer with the creation of a fraudulent Affirmation or other related documentation, including by providing guidance or otherwise advising Customers on how to avoid having the Notification appear on the Target Device or to the Target Account Holder.

92. Respondents may not, directly or indirectly, assist or otherwise allow a Customer to avoid having the Notification appear on the Target Device or to the Target Account Holder, including by preventing the same email account from being used for subsequent purchase attempts with changes to the Affirmation selection, including where the purchaser had not previously completed a purchase or created an account (i.e., where the purchaser had abandoned the purchase attempt after being presented with the Affirmation and attempts to start over and make a new selection during the Affirmation flow).

Notifications Related to Prior Use of Spyware Products

93. Within sixty (60) days of the Effective Date, Respondents must post on all websites Respondents host, operate, and/or control relating to the Spyware Products Clear and Conspicuous instructions for how a Target Device Holder or a Target Account Holder who suspects their Mobile Device is being monitored without consent can remove the Spyware Apps and change their iCloud credentials, as well as links to resources for domestic violence victims, including the National Domestic Violence Hotline.

94. Within sixty (60) days of the Effective Date, Respondents must send an email notification to all current and past Customers of Respondents' Spyware Products at the email

address associated with the initial purchase of the Spyware Products. This email notification shall include (a) notice of Respondents' settlement with the OAG, and (b) a link to this Assurance on the OAG's website.

95. On or before the Transition Date, Respondents must send an email notification to the email addresses associated with all Target Account Holders that have been or are being monitored through use of Respondents' Spyware Products (i.e., the email addresses used to log in to the monitored iCloud or other online account to be monitored by use of the Spyware Products) (the "Email Notification") by a Customer that has not affirmed that they intend to use the Spyware Products to monitor a minor custodial child (as set forth in Paragraph 87.f.iii above) and completed the additional necessary steps regarding the monitoring of a minor child (as set forth in Paragraph 103 below).

96. The Email Notification shall notify the Target Account Holder that (a) the Spyware Product(s) have been connected with their associated iCloud or other online accounts and (b) the Spyware Product(s) may be used to monitor the activities of their Mobile Devices and/or any other information that is stored on the Target Account, as well as provide (c) notice of Respondents' settlement with the OAG, (d) a description of Respondents' settlement with the OAG, and (e) notice that this Assurance is available on the OAG's website.

Ongoing Notifications Related to Use of and Visibility of Spyware Products

97. On or before the Transition Date, Respondents shall ensure that the installed Spyware App on all Target Devices displays as an icon that is identified with the name of the product or service purchased (i.e., the name displayed must be that of the actual Spyware App purchased by the Customer and not an alternative name or pseudonym). When opened, the Spyware App must (a) Clearly and Conspicuously state the material functions of the Spyware App, (b) Clearly and Conspicuously state that Mobile Device activity is being monitored by the

Spyware App, (c) Clearly and Conspicuously identify how the user of the Mobile Device can contact Respondents for additional information regarding Spyware Products and/or if they have questions about the Spyware App, and (d) Clearly and Conspicuously post links to the information posted on the Spyware Product website set forth above in Paragraph 93.

98. On or before the Transition Date, Respondents shall ensure that the installed Spyware Apps on all Target Devices, except in cases where the Customer has affirmed that they intend to use the Spyware Products to monitor a minor custodial child (as set forth in Paragraph 87.f.iii above) and has completed the additional necessary steps regarding the monitoring of a minor child (as set forth in Paragraph 103, below), display a Notification to the users of all Target Devices at the time the Customer first logs on to the dashboard and within 72 hours of every subsequent dashboard session in which the Customer has accessed data obtained from the Target Device. This message shall Clearly and Conspicuously state the types of data that the Spyware App collects from the Target Device and provide instructions, with accompanying links, directing individuals who suspect their Mobile Device is being illegally monitored to the notices and information required under Paragraph 93.

99. By the Transition Date, Respondents shall require that every Spyware App associated with any product license that is newly purchased or renewed complies with the Notification requirements set forth in Paragraphs 97-98 and that, following a license renewal, existing Customers are unable to use previously downloaded versions of Respondents' Spyware Apps that are not compliant with the Notification requirements set forth in Paragraph 97-98.

100. Except in circumstances where the Customer has affirmed that they intend to use the Spyware Products to monitor a minor custodial child (as set forth in Paragraph 87.f.iii above) and has completed the additional necessary steps regarding the monitoring of a minor child (as set forth in Paragraph 103 below), on or before the Transition Date, Respondents shall send a

Notification to the email address for the Target Account Holder that is used to sign in to any iCloud or other online accounts being monitored through use of the Spyware Products at the time the Customer first logs on to the dashboard and within 72 hours of each occasion on which the data obtained from the Target Account is accessed through the product dashboard made available to the Customer by Respondents. This message shall Clearly and Conspicuously state the types of data that the Spyware Product collects from the Target Account and provide instructions, with accompanying links, directing individuals that suspect their Mobile Device is being monitored without their consent to the notices and information required under Paragraph 93.

101. Within sixty (60) days of the Effective Date, Respondents must post on all websites Respondents host, operate, and/or control relating to the Spyware Products, including on both the home page and the page where any Spyware Product is made available for purchase, a Clear and Conspicuous statement that Spyware Products can only be used for legal purposes and that it's illegal in most countries to install monitoring / surveillance software onto a cell phone which you do not own or have proper authorization to install.

102. Respondents may not, directly or indirectly, provide any information, direction, functionality, or other assistance to Customers seeking to avoid having the Notification appear on the Target Device and shall ensure that the purchase flow does not present the customer with information about device notifications until after the Affirmation has been completed. Respondent shall include on any FAQ page related to Respondents' Spyware Products that Respondents will not assist Customers attempting to circumvent or avoid the Notifications.

Affirmation for the Monitoring of a Custodial Minor Child

103. Where the Customer has affirmed that they intend to use the Spyware Products to monitor a custodial minor child (as set forth in Paragraph 87.f.iii above), Respondents are not required to provide the Notifications set forth in Paragraphs 97-98 and 100 above to the Target

Device and/or Target Account Holders where the Customer seeking to monitor their custodial minor child (the "Monitoring Guardian") has completed an additional affirmation (together with the Affirmation, the "Affirmations") that includes at least the following:

a. The Monitoring Guardian must affirm that the Spyware Product is being purchased to monitor the Mobile Device of a child under the age of 18 who is in the legal custody or guardianship of the Monitoring Guardian;

b. The Monitoring Guardian must provide the birthdate and state of residence of the child being monitored;

c. The Monitoring Guardian must affirm that they believe that monitoring the minor child's Mobile Device by use of the Spyware Product is in the best interest of the child;

d. The Monitoring Guardian must acknowledge that the Spyware Product will cease operating or begin providing Notifications on the date that the child turns 18; and,

e. The Monitoring Guardian must affirmatively select a check box stating that, "I certify that the information provided above regarding the minor child I intend to monitor with the purchased product is true and correct."

104. Respondents shall either discontinue the operation of any Spyware Product used to monitor a minor child on the date the child turns 18 or begin providing the Notifications set forth in Paragraphs 97-98 and 100 on that date.

Advertisements Regarding Spying on Adults Prohibited

105. Respondents shall not engage in any advertising, marketing, or otherwise create any Promotional Material for their Spyware Products that suggests, represents, or otherwise indicates, explicitly or implicitly, that Spyware or any monitoring products or services should or may be installed or used on a Mobile Device or in connection with any online account that is

owned or used by another adult without that adult's knowledge and consent. Prohibited advertising, marketing, or Promotional Materials include, but are not limited to:

a. Making representations concerning the ability to use Spyware Products to monitor other adults, including intimate partners, without such adult's knowledge; and,

b. Purchasing any form of advertising, including but not limited to Google or Bing keyword advertising, that displays Respondents' Spyware Products to consumers searching for terms involving adults monitoring other adults without the monitored adult's knowledge or consent, including but not limited to tracking their movements, reviewing their private documents or messages, and listening in on their phone calls, without the monitored adult's knowledge or consent.

Misrepresentations Regarding Testimonials and Endorsements Prohibited

106. Respondents shall not make any explicit or implicit misrepresentations concerning testimonials by or endorsements of third parties, including but not limited to representations that misrepresent or omit material details concerning (a) the author of any testimonial or review or (b) Respondents' material connections to such author or any website or other media where such testimonial or review appears.

Misrepresentations Regarding Refund Policy Prohibited

107. Respondents shall Clearly and Conspicuously disclose all terms and conditions related to its Refund Policy on all websites Respondents host, operate, and/or control relating to the Spyware Products, including on the page where any Spyware Product is made available for purchase.

108. Respondents shall not make any representations regarding satisfaction guarantees in connection with Respondents' Spyware Products unless Respondents provide a trial period where Customers can receive a refund for the full amount paid for the Spyware Products after a

trial period during which the Customer can evaluate the performance of the Spyware Product purchased after having installed or used it.

Adequate Disclosures Related to Rooting/Jailbreaking Requirements

109. Respondents shall Clearly and Conspicuously disclose that rooting or jailbreaking a Mobile Device on any product page or Promotional Material discussing any feature that requires that the Target Device be rooted or jailbroken. Respondents shall not make any express or implied representations that jailbreaking or rooting is not required for Spyware Products that do require such procedures for some features without Clearly and Conspicuously disclosing the particular features that require jailbreaking or rooting. Respondents shall Clearly and Conspicuously disclose that jailbreaking or rooting can void the warranty of the Mobile Device in any promotional or product information related to a feature that requires jailbreaking or rooting.

Data Security

110. Respondents shall comply with Executive Law § 63(12) and GBL § 899-bb in connection with its collection, use, and maintenance of personal information.

111. By the Transition Date, Respondents shall develop and maintain a comprehensive, written data and information security program that is consistent with the requirements of GBL § 899-bb (the "Data Security Program").

112. The Data Security Program shall, at minimum, include reasonable technological, administrative, and physical safeguards designed to secure the private information of Customers and information obtained from Target Devices, through Respondents' Spyware Products. These measures shall include, at least:

a. Respondents shall encrypt the personal information that it collects, uses, stores, transmits and/or maintains, whether stored within Respondents' network, or

transmitted electronically within or outside Respondents' network, using a reasonable encryption algorithm where technically feasible. Information collected from the Target Devices shall be encrypted both in transit and at rest.

b. Respondents shall disclose in their public-facing privacy policies a description of Respondents' Data Security Program, including the safeguards put in place to protect the personal information of both Respondents' Customers and information collected form Target Devices.

Record-Keeping

113. Respondents shall create and maintain records for three (3) years that are sufficient to show compliance with this Assurance, including Notification requirements and Affirmations by Customers. During the period of record keeping, Respondent will provide the OAG a yearly summary chart which indicates the total number of Spyware Product purchases made for the year and, for each of use cases set forth in Paragraph 87.f, the percentage of those purchases in which the Customer selected the respective use case.

Compliance Certification

114. Each year for three (3) years on the anniversary date of the Effective Date of this assurance or until such time as companies are no longer doing business in New York State, Respondents shall provide non-public, one sentence annual certifications of compliance with this Assurance to the OAG.

Monetary Relief

115. Respondents shall pay to the State of New York four hundred ten thousand dollars ($410,000.00) in penalties, disgorgement, and costs (the "Monetary Relief Amount"). Payment of the Monetary Relief Amount shall be made in installments in accordance with Schedule A, attached hereto. All payments shall reference AOD No. 23-005

116. Payments shall be made by wire transfer in accordance with instructions provided by an OAG representative.

MISCELLANEOUS

117. Within thirty (30) days of the Effective Date, Respondents shall provide notice of the requirements of this Assurance to each of its current officers and managers that have supervisory authority with respect to the subject matter of this Assurance. Further, Respondents shall provide notice of the requirements of this Assurance to each new officer and manager that has supervisory authority with respect to the subject matter of this Assurance within thirty (30) days from which such person assumes his/her position at an entity owned, operated, and/or controlled by Respondents.

118. In the event the OAG receives a FOIL request for information and/or documents obtained as part of this investigation and for which confidential treatment has been requested, the OAG shall provide notice to Respondents. Respondents shall have 14 days from receipt of such notice (the "Disclosure Notice Period") to provide a written response to explain to OAG why the information and/or documents should be exempt from disclosure and, if necessary, to seek judicial intervention to prevent disclosure.

119. If the OAG believes Respondents have failed to comply with a provision of the Assurance, and if in the OAG's sole discretion the failure to comply does not threaten the health or safety of the citizens of New York or create an emergency requiring immediate action, prior to taking legal action for any alleged failure to comply with the Assurance, the OAG shall provide written notice to Respondents. Respondents shall have 14 days from receipt of such written notice (the "Notice Period") to provide a written response, including either a statement that Respondents believe they are in full compliance with the relevant provision or a statement explaining why they did not comply with the relevant provision, and how Respondents have

come into compliance or when they will come into compliance. Respondents shall not seek a declaratory judgment concerning any alleged failure to comply with the Assurance during the Notice Period.

120. Respondents expressly agrees and acknowledges that the OAG may, upon written notice to Respondents, initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for alleged violations of the Assurance, or if the Assurance is voided pursuant to Paragraph 126, and agrees and acknowledges that in such event:

a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance, subject to any applicable work product or attorney-client privilege or other evidentiary challenges or objections;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondents irrevocably and unconditionally waive any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

121. If a court of competent jurisdiction determines that the Respondents have or any individual Respondent has violated the Assurance, the OAG may seek a court order requiring Respondents to pay reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

122. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondents. Respondents shall include in any

such successor, assignment, or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG, except where such assignment, delegation, or transfer is part of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of all of the Respondents' assets or a part thereof.

123. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

124. Any failure by the OAG to insist upon the strict performance by Respondents of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

125. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-005, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; and electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to the Respondents, to:

Patrick Hinchy
101 East Camino Real
Boca Raton, Florida 33432
Patrick.hinchy@thepowerlinegroup.com

Michael Weinstein, Esq.
Cole Schotz P.C.
25 Main Street
Hackensack, New Jersey 07601
mweinstein@coleschotz.com

If to the OAG, to:

Marc Montgomery, Assistant Attorney General, or in his absence, to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

126. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondents and their counsel and the OAG's own factual investigation as set forth in Findings, Paragraphs 1-72 above. The Respondents represent and warrant that neither they nor, to Respondents' knowledge, their counsel have made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondents are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

127. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

128. The Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondents further represent and warrant that Patrick Hinchy, as the signatory to this Assurance, is a duly authorized officer acting at the direction of the Respondents.

129. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondents' obligations under this Assurance are enduring. Nothing in this Assurance shall relieve Respondents of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

130. Respondents shall not make or permit to be made any public statement denying, directly or indirectly, the propriety of this Assurance or the OAG investigation. Nothing in this

paragraph affects Respondents' (i) testimonial or other legal obligations or (ii) right to take positions in defense of litigation or other legal proceedings to which the OAG is not a party. This Assurance is not intended for use by any third party in any other proceeding.

Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondents violate the Assurance after its Effective Date.

131. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

132. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

133. Respondents acknowledge that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

134. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

135. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

136. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for

purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

137. The Effective Date of this Assurance shall be February 1, 2023.

LETITIA JAMES
ATTORNEY GENERAL OF THE STATE OF NEW YORK

By: Marc Montgomery
Assistant Attorney General
Bureau of Internet and Technology
Office of the New York State Attorney General
28 Liberty St.
New York, NY 10005
Phone: (212) 416-8433
Fax: (212) 416-8369

1/27/2023
Date

Powerline Group Inc., Powerline Media LLC, Powerline Data LLC, Powerline Digital LLC, Powerline Commerce LLC, ILF Mobile Apps Corp., Auto Forward Data Services LLC, DDI Utilities Inc., DDI Data Solutions Inc., Highster Mobile Inc., Highster Data Services LLC, PhoneSpector LLC, Safeguarde LLC, BFG Marketing LLC, Digital Security World LLC, CTS Technologies Corp., and Patrick T. Hinchy

By: Patrick Hinchy
101 East Camino Real
Boca Raton, Florida 33432
1/27/23
Date