ALDEN F. ABBOTT
General Counsel

RONNIE SOLOMON, Cal. Bar No. 284923
SARAH SCHROEDER, Cal. Bar No. 221528
Federal Trade Commission
901 Market Street, Suite 570
San Francisco, CA 94103
rsolomon@ftc.gov, sschroeder@ftc.gov
Tel: (415) 848-5100; Fax: (415) 848-5184

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF CALIFORNIA**

**FEDERAL TRADE COMMISSION**,

Plaintiff,

vs.

**NTS IT CARE, INC.**, a California corporation, and

**JAGMEET SINGH VIRK**, individually, and as an owner and officer of NTS IT Care, Inc.,

Defendants.

**Case No.** 4:20-cv-3388-PJH

**COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF**

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Sections 5(a), 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a), 53(b), and 57b, the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101–6108, as amended, and the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, as amended, to obtain temporary, preliminary, and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and the TSR, 16 C.F.R. Part 310, as amended.

## JURISDICTION, VENUE, AND INTRADISTRICT ASSIGNMENT

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

3. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(1), (c)(2), and (d), and 15 U.S.C. §§ 53(b).

4. Assignment to the San Francisco Division is proper pursuant to Local Rule 3–2(d) because Defendants have provided their services in San Francisco County.

## PLAINTIFF

5. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101–6108, as amended. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

6. The FTC is authorized to initiate federal district court proceedings by its own attorneys, to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 56(a)(2)(A)–(B), 57b, 6102(c), 6105(b), and 8404.

## DEFENDANTS

7. Defendant **NTS IT Care, Inc.** ("NTS") is a California corporation with its principal place of business at 1605 South Main Street, Suite 125, Milpitas, CA 95035. NTS transacts or has transacted business in this District and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, NTS has advertised, marketed, distributed, or sold its purported computer security or technical support services to consumers throughout the United States.

8. Defendant **Jagmeet Singh Virk** ("Virk") is the owner, Chief Executive Officer, Chief Financial Officer, and Secretary of NTS. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of NTS, including the acts and practices set forth in this Complaint. Defendant Virk resides in this District and, in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

## COMMERCE

9. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

## DEFENDANTS' DECEPTIVE BUSINESS PRACTICES

### Overview

10. Since at least August 2014, Defendants have operated a scheme that deceives consumers into buying unnecessary computer technical support services. Defendants carry out their scheme through Internet browser pop-up windows disguised as urgent security alerts from a computer's operating system (the "pop-up warning"). Consumers receive these pop-up warnings when browsing the Internet. Defendants' pop-up warnings falsely claim to detect computer viruses or other intrusions, warn of the complete disabling of the computer, and instruct consumers to immediately call a telephone number to fix the purported computer problem.

11. When consumers call the telephone number on the pop-up warning, they are routed to Defendants' call center in India. Defendants' sales representatives located there (the "sales representatives") use high-pressure sales tactics to deceive consumers out of money. They remotely access the computer, conduct fake security diagnostics, and mislead consumers by falsely claiming to detect malicious software (such as viruses, spyware, and other malicious files), system compromises (such as infections or breaches), and other security vulnerabilities (such as claiming that the system has no security or is unprotected). They also claim, falsely, that consumer's computers are unprotected by antivirus and security software. Defendants and their sales representatives also falsely claim to be part of or affiliated with well-known technology companies, such as Microsoft or Apple, or claim that they are authorized by those companies to service computers.

12. In reality, Defendants have no basis or substantiation for their claims about computer security threats and issues. Nor are Defendants affiliated with or authorized by Microsoft, Apple, or other well-known technology companies to service consumers' computers. Underscoring the deceptive nature of their claims, Defendants have diagnosed clean, secure, and uninfected computers with non-existent computer security threats and issues.

13. Through these deceptive sales tactics, sales representatives convince consumers to purchase expensive, multi-year "technical support" service packages. Defendants charge each consumer hundreds of dollars, typically ranging from $99 to $499, to remedy the purported security issues. Since 2016, Defendants have taken approximately $5 million from consumers through these activities. Since NTS has been in operation since 2014, total consumer harm is likely to be even greater. Defendants' conduct has resulted in hundreds of consumer complaints to the FTC, the Better Business Bureau, and other entities.

14. Defendants' conduct especially targets vulnerable populations, such as older adults who may be unfamiliar with computer security. Defendants use intimidation and scare tactics to take advantage of inexperience with computer security.

**Defendants Lure Consumers through a Pop-Up Warning Disguised as a Security Alert**

15. Defendants' pop-up warnings typically appear when consumers are browsing the Internet. The pop-up warnings are designed to appear as if they originated from the operating system of a consumer's computer, to create a sense of urgency, and to mislead consumers into believing that the pop-up warning is from Microsoft, Apple, or a similar company. They tell consumers that their computers have been compromised by malicious software, such as a virus, spyware, or other security threat, that their computer has been "blocked," and that the consumer's personal information is being stolen.

16. The pop-up warnings impart a sense of urgency and need for quick action. They urge consumers to immediately call a toll-free number to resolve the problem and to prevent their computer from becoming disabled or experiencing further damage. For instance, they instruct consumers to call "within the next 5 minutes" or "immediately so that our engineers can walk you through the removal process over the phone." Some pop-up warnings also cause alarming sounds to play when they appear.

17. Further, some of Defendants' pop-up warnings explicitly claim to be a warning from Microsoft. They prominently display the Microsoft or Microsoft Windows logo, claim to be a "Windows Support Alert," or claim that "Windows" has detected a security vulnerability. They urge consumers to contact a toll-free number that purports to be "Microsoft Security Tollfree," the "Microsoft Helpline," or "Certified Windows Technicians."

18. The pop-up warnings are designed so that consumers are unable to easily close or navigate around them, rendering the Internet browser difficult to use. This practice is known as "browser hijacking." In some instances, the pop-up warning instructs consumers not to close the window to avoid further computer problems.

//

//

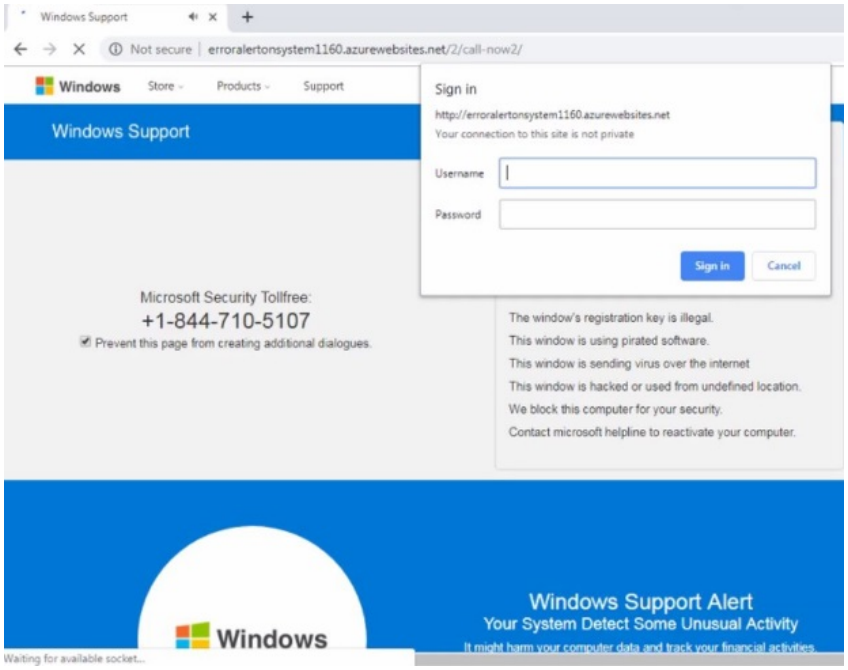
//

//

19. Examples of Defendants' pop-up warnings are below:

**Figure A**

(screen image of an NTS pop-up warning captured by a consumer)




(Text in **Figure A**):

Microsoft Security Tollfree:

+1-844-710-5107

. . . .

The window's registration key is illegal.

This window is using pirated software.

This window is sending virus over the internet.

This window is hacked or used from undefined location.

We block this computer for your security.

Contact microsoft helpline to reactivate your computer.

. . . .

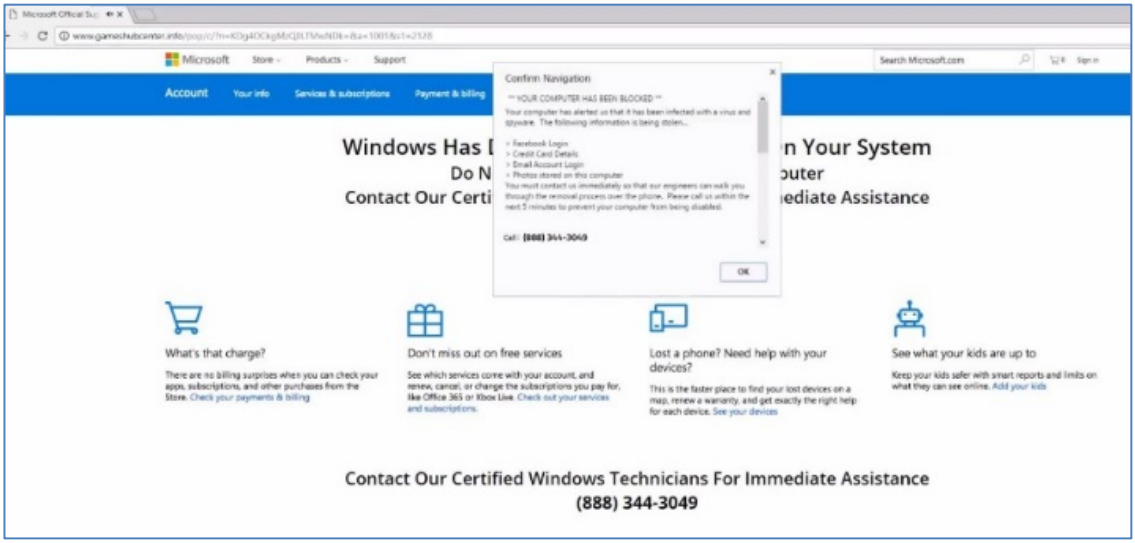
Windows Support Alert

Your System Detect Some Unusual Activity

It might harm your computer data and track your financial activities.

**Figure B**

(screen image of an NTS pop-up warning captured by a consumer)




(Text in **Figure B**):

**YOUR COMPUTER HAS BEEN BLOCKED**

Your computer has alerted us that it has been infected with a virus and spyware.

The following information is being stolen…

> Facebook Login

> Credit Card Details

> Email Account Login

> Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Call: (888) 344-3049

. . . .

Windows Has D[illegible] Your System

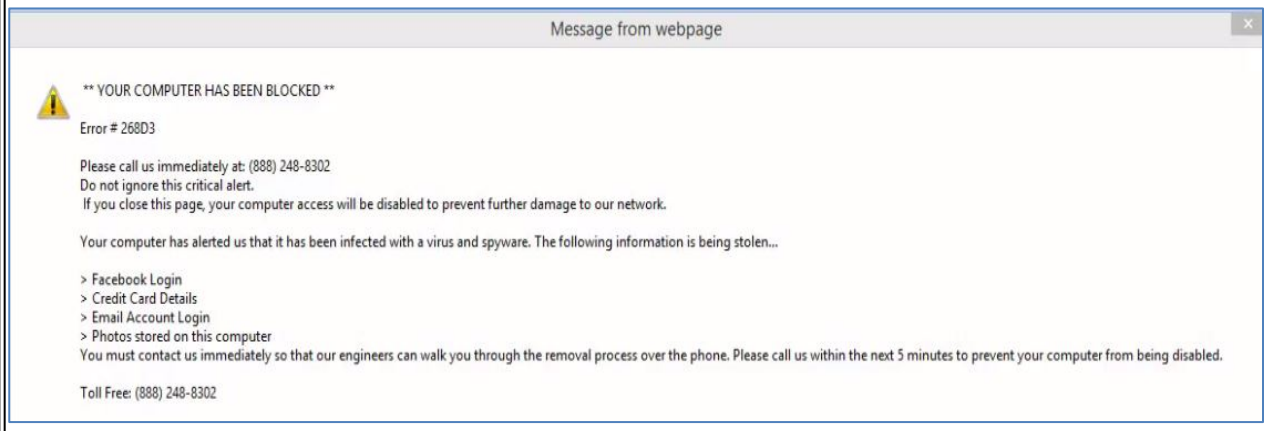
. . . .

Contact Our Certified Windows Technicians For Immediate Assistance

(888) 344-3049

**Figure C**

(screen image of an NTS pop-up warning captured by a consumer)




(Text in **Figure C**):

**YOUR COMPUTER HAS BEEN BLOCKED**

Error# 268D3

Please call us immediately at: (888) 248-8302

Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware.

The following information is being stolen…

> Facebook Login

> Credit Card Details

> Email Account Login

> Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: (888) 248-8302

**Defendants Gain Remote Access to Consumers' Computers**

20. Calling the toll-free number in the pop-up warning connects consumers with Defendants' sales representatives. The sales representatives lead consumers through a sales pitch designed to convince them that their computer is in urgent need of repair. Regardless of the actual state of the consumer's computer, Defendants' sales representatives are trained to tell consumers that there is a problem stemming from computer security threats and issues.

21. Defendants' sales representatives begin by asking the consumer about the security issue identified in the pop-up warning. Although Defendants' sales representatives at that point in the call have no way of verifying whether consumers' computers actually have a security threat or issue present, they nonetheless purport to confirm the problem and assure consumers that they can fix it.

22. In some instances, Defendants' sales representatives state or imply, either directly, indirectly, or by failing to correct consumers' obvious misimpressions, that they are part of or affiliated with companies like Microsoft or Apple, or that such companies have certified Defendants to service their products or to provide computer and technical support services. This causes consumers to believe that Defendants' sales representatives are trustworthy.

23. After convincing consumers that the pop-up warnings indicate serious security problems and that they are qualified to fix those problems, the sales representatives claim that they must remotely access the computer. Defendants' sales representatives typically direct consumers to go to a website and enter a code to begin the remote access session. Once the sales representatives gain remote access, they are able to control the consumers' computers. Among other things, the sales representatives can view the computer screen, move the mouse or cursor, enter commands, and run applications. The sales representatives also see the pop-up warnings that triggered the consumers' calls. At the same time, consumers can see what the sales representatives are doing on their computers.

**Defendants Run Fake Diagnostics**

24. Once in control of the computer, Defendants' sales representatives run a series

of purported diagnostic tests that are meant to look like "security scans" testing the security and performance of the machine. Defendants' purported diagnostics are a high-pressured sales pitch designed to scare consumers into believing that their computers have serious security threats or issues present. In reality, these fake "diagnostics" consist of the sales representative running simple, routine commands and benign inquiries, as described below, and claiming that the outputs indicate computer security threats or issues. Defendants' sales representatives falsely claim to detect malicious software, system compromises, or other security vulnerabilities without any proper analysis or substantiation.

25. Defendants' sales representatives use a series of different fake diagnostic tactics to convince consumers that there are critical computer security threats and issues that require immediate repair and remediation.

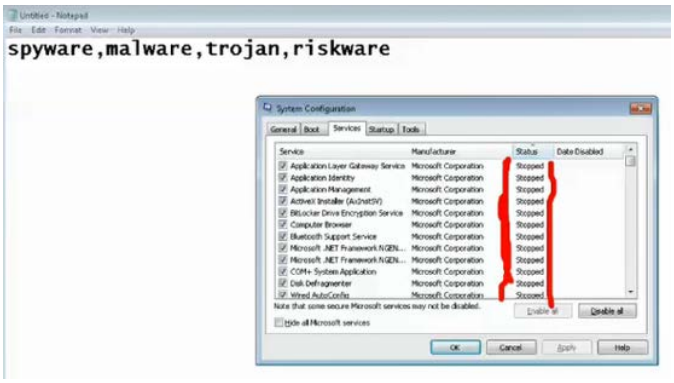
**Msconfig Tactic**

26. For example, Defendants' sales representatives run the "msconfig" command on Windows computers, which opens the System Configuration utility in the computer. *See* Figure D. Defendants' sales representatives falsely claim that all Windows services listed should be in the "Running" state, and that those services listed in the "Stopped" state are evidence of malicious software, system compromises, or other security vulnerabilities.

27. For example, Figure D below is a screen image (captured by an FTC investigator on December 5, 2019) of the System Configuration utility that Defendants' sales representative prompted on the investigator's computer during an undercover phone call. Defendants' sales representative falsely claimed that the "Stopped" services were a sign of "critical" problems on the computer. He stated that the problems were "worse than the virus," and typed the words "spyware, malware, trojan, riskware" onto the investigator's computer screen. Defendants' sales representative used a similar tactic in a recording captured by a consumer, and falsely claimed "here are some errors on this computer. That's why the services are not running." The sales representative further claimed that the consumer's computer had a "hidden virus" and "errors" that needed to be "clean[ed]."

**Figure D**

(screen image captured by an FTC investigator in December 2019)




28. In fact, it is normal for Windows services listed in System Configuration utility to be in the "Stopped" state when they are not running or being used. "Stopped" applications do not prove that a computer has malicious software, system compromises, or other security vulnerabilities present. The sales representative did not do any further or proper analysis necessary to determine the presence of malicious software, system compromises, or other security vulnerabilities.

**Windows Event Viewer Tactic**

29. Another tactic Defendants' sales representatives use involves prompting the Windows Event Viewer tool and highlighting the number of "Error" and "Warning" messages listed. Defendants' sales representatives falsely claim that the presence of these messages indicate a security threat or issue.

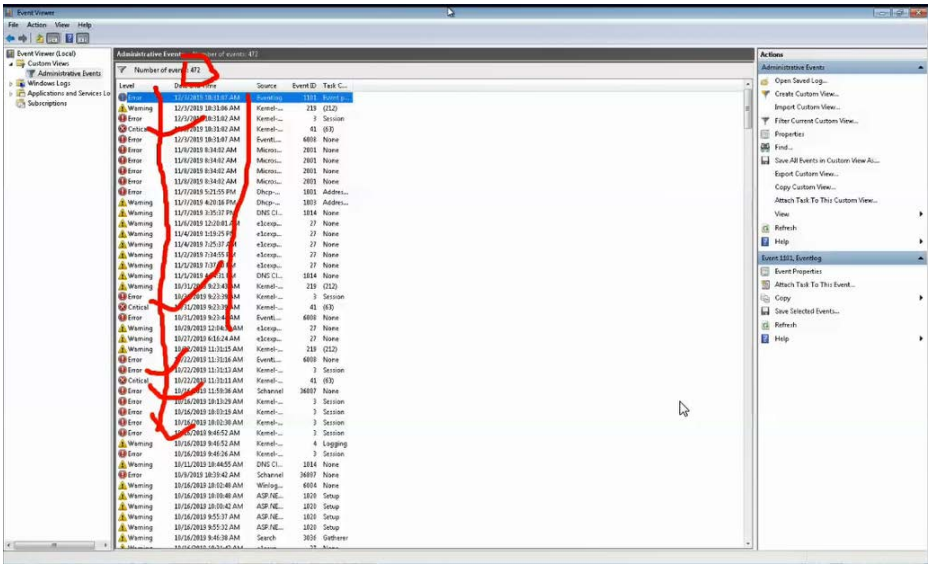
30. For example, in a recording captured by a consumer, Defendants' sales representative opened the Windows Event Viewer tool while remotely connected to a consumer's computer and circled the number of events in red, which he diagnosed as "infections" that "can transfer into your other internet devices" and as "a really bad sign." On December 4, 2019, Defendants' sales representative used the same tactic with an FTC investigator and claimed her computer had 472 errors. *See* Figure E. The sales representative described these 472 errors and warnings as "critical" and capable of causing "damage" to the investigator's files, and told the investigator "so we need to go ahead and remove all of this."

The sales representative also claimed that the computer had "bad files" and "some kind of unwanted application" and "that's why you are getting all these warning things . . . the bad files." The sales representative further claimed that these "warnings" had "disable[d] all the security." The sales representative claimed that these "bad files" needed to be removed, were "more critical" than a virus, and referred to them as "some kind of Trojan" infection. In addition, the sales representative warned that if the "unwanted software" was not removed, that "you will have lots of infection problem [sic] coming more again and again."

31. In truth, it is normal for a Windows system to collect hundreds or thousands of "Error" or "Warning" messages in the course of routine operations over time. Messages such as these are part of the normal functioning of a Windows operating system. These messages do not by themselves indicate that a computer has any malicious software, system compromises, or other security vulnerabilities present. The sales representative did not do any further or proper analysis necessary to determine the presence of malicious software, system compromises, or other security vulnerabilities.

**Figure E**

(screen image captured by FTC investigator in December 2019)



**Other Fake Diagnostic Tactics**

32. Defendants' sales representatives also manipulate the Windows Command Prompt application to run fake "scans" that produce equally fake error and warning messages.

33. For example, Figure F below is a screen image captured by a consumer during an interaction with Defendants' sales representative. Figure F shows the Command Prompt screen prompted by Defendants' sales representative, who typed the "dir/s" Windows command, causing lines of text to scroll down the screen for several seconds. The sales representative claimed that this was a security scan. In fact, the "dir/s" Windows command simply displays a listing of all files and directories on the computer. It does not scan for performance or security problems. Although not a security scan, the sales representative claimed that this "scan" returned results indicating "errors," "unwanted connections," and "security expired" on the consumer's computer, and that these were "a really major issue."

34. In reality, the "errors," "unwanted connections," and "security expired" messages were not the results of a scan. Rather, they appeared after the sales representative manually typed or pasted these fabricated messages into the command prompt window to make it appear as if the "scan" returned worrisome results. Since these fabricated outputs are not valid or recognized Windows commands, each line generated an error message when the sales representative typed them into the command prompt window. The sales representative did not do any further or proper analysis necessary to determine the presence of malicious software, system compromises, or other security vulnerabilities.

//

//

//

//

//

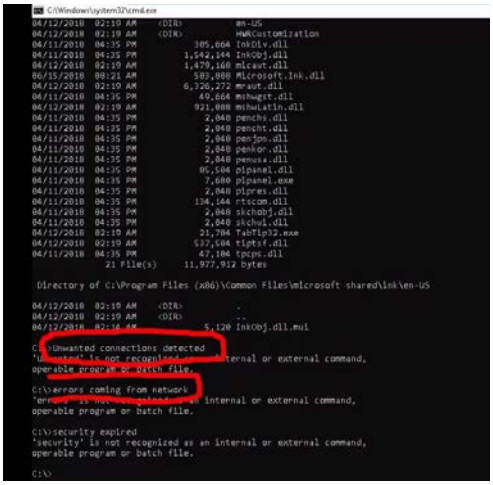
//

//

//

**Figure F**

(screen image captured by a consumer)




35. Defendants' sales representatives also run the "netstat" Windows command, which displays information about all networks to which the consumer's computer is connected, in a table format. The output appears in a format that looks like a listing of results. The sales representatives claim that the output "results" represent malicious activity on the system, such as evidence that hackers have accessed or are attempting to access the computer.

36. For example, Figure G below is a screen image of the "netstat" command output captured by a consumer during an interaction with one of Defendants' sales representatives. Defendants' sales representative claimed, without any analysis or substantiation, that the results were evidence of a "really major threat going on right now," and that there were foreign connections that might steal the consumer's personal information: "There are a lot of foreign addresses which are connected right now . . . the worst part is that whenever these might get established, these can misuse information." To emphasize this claim and scare the consumer, the sales representative circled and highlighted the connections and wrote the word "misuse" next to them on the consumer's screen. The sales representative claimed and that "[t]hese might get all of your personal information. So it's crunch time. We need to go ahead and install the security as soon as possible."

37. In reality, the "netstat" command is a tool used to view information about network connections. The "foreign address" column in the "netstat" command output indicates the host

address at the other end of the connection from the computer. It does not, by itself, indicate that a computer has any malicious software, system compromises, or other security vulnerabilities present. The "foreign address" could belong to hosts providing legitimate services—such as the remote control LogMeIn application that the sales representative is using. The results show normal network traffic and connections, and the sales representative did not do any proper analysis to substantiate the claim that these connections indicate a computer intrusion or a threat.

**Figure G**

(screen image captured by a consumer)


38. Defendants' sales representatives also open and display the computer's "security settings," and point out that certain types of content have been "disabled." Defendants' sales representatives claim that this represents the presence of malicious files. In reality, the security settings show that different types of potentially dangerous content are "disabled." They also falsely claim that consumers' computers are vulnerable and unprotected by any antivirus or computer security software.

39. Defendants' sales representatives run these and other fake diagnostics on consumers' computers. After running the purported diagnostics, Defendants' sales representatives tell consumers that their computers have malicious software, system compromises, or other security vulnerabilities present. Defendants have no basis or substantiation for these claims. Through these fake diagnostics, Defendants have diagnosed otherwise "clean," uninfected or uncompromised computers with non-existent security issues.

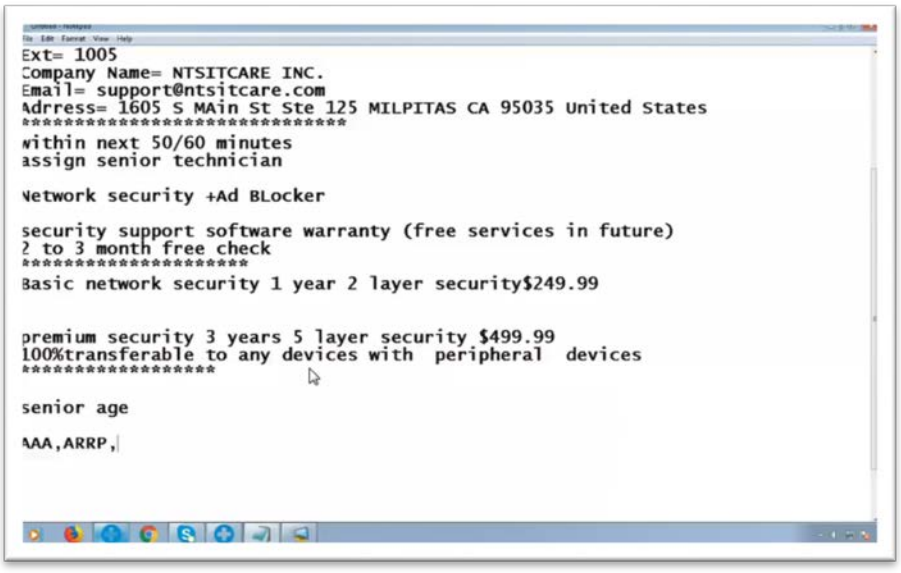
**Defendants Deceive Consumers into Buying Unnecessary Computer Technical Support Services**

40. By exploiting consumers' concerns about Internet threats like malicious software, system compromises, or other security vulnerabilities, and misrepresenting affiliations with companies like Microsoft, Defendants scare consumers into believing that their computers and personal information are in imminent danger.

41. Defendants' sales representatives tell consumers that they can remedy non-existent security issues for a fee. They launch the Notepad application and type Defendants' contact information and the cost of Defendants' computer security and technical support services. For example, Figure H below is a screen image captured by an FTC investigator on December 5, 2019 during an undercover call.

**Figure H**

(screen image captured by FTC investigator in December 2019)




42. In another instance, Defendants' sales representative opened the Notepad application and pasted Defendants' prices and contact information, along with the header "NTS SOFTWARE SUPPORT (Microsoft Product Support)." For example, Exhibit I is a screen image captured by a consumer during an interaction with Defendants' sales representative.

**Figure I**

(screen image captured by a consumer)


43. Defendants typically charge consumers between $99.99 and $499.99 for their purported technical support services. Defendants typically collect payment by credit card. Once a consumer agrees to purchase Defendants' technical support services, sales representatives ask for personal and credit card information, and they input the payment credentials into and scroll through a payment page on the NTS website while the consumer looks on. Since 2016, Defendants have taken approximately $5 million from consumers through these deceptive activities.

44. After consumers pay, Defendants' sales representatives perform services that are in many instances unnecessary, because Defendants' sales representatives have done no proper analysis to determine whether there are any computer security threats or issues present. Defendants' sales representatives indiscriminately diagnose computers with security threats and issues regardless of the actual state of the computer.

**Role of Individual Defendant Jagmeet Virk Singh**

45. At all times material to this Complaint, acting alone or in concert with others, Jagmeet Virk Singh has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Defendant NTS, including the acts and practices set forth in this Complaint.

46. Virk founded Defendant NTS in 2014 and has served as the company's CEO, CFO, and Secretary, as well as its agent for service of process. Virk has repeatedly identified

himself as NTS's "President" or "Chairperson" to financial institutions. In 2019, Virk attested that he is the NTS "manager" and "officer" in a sworn declaration filed on behalf of NTS in a pending San Bernardino County Superior Court lawsuit. As owner and sole officer of NTS, Virk has the authority to control the acts and practices of the company.

47. Virk controls the finances of Defendant NTS. At all times material to this Complaint, Virk has been the sole signatory and control person on NTS depository bank accounts. Virk has written checks from NTS's bank accounts, and deposited checks from consumers. Virk has wired millions of dollars from NTS bank accounts to accounts in India. Virk also opened and controls NTS's accounts with payment processing companies, including PayPal, Inc., Authorize.Net., and Network Merchants, Inc. Virk signed a W-9 Request for Taxpayer Number and Certification for NTS. Additionally, Virk identified himself as the only individual who is a "controlling person" and "authorized signer" for NTS in a "Beneficial Ownership Declaration" provided to Citibank N.A.

48. Virk oversees the other business activities of Defendant NTS. He rents office space for NTS in Milpitas, California, and conducts business from there. Virk also is the signatory, account holder and/or payer for numerous accounts and vendors that NTS uses to conduct the scam. Virk opened and controls the corporation's accounts with LogMeIn, a company that offers software to remotely connect to computers, as well as NTS's electronic payment gateway accounts. Virk has paid entities and individuals for NTS business expenses, including for "leads and marketing." Virk also registered and controls NTS's domain name, www.ntsitcare.com.

49. Several consumers report having direct contact with Virk. One consumer reported that an NTS sales representative referred to Virk as his "manager," and transferred the consumer to Virk to approve a special payment plan. The consumer spoke with an individual who identified himself as Jagmeet Virk. Virk told the consumer how to pay NTS and sent the consumer an email with a "Reply-To" line that indicated it was from "Jagmeet Virk."

50. Virk has been aware of consumer complaints about NTS and its fraudulent conduct. Virk received and responded to fraud complaints that the Better Business Bureau

("BBB") and criminal authorities have brought directly to him. The BBB office serving Los Angeles, San Jose, and Silicon Valley contacted NTS with concerns about the amount and pattern of consumer complaints it had received about NTS, including complaints about deceptive sales tactics and claiming affiliation with Microsoft. Virk sent the BBB a response on behalf of NTS. The BBB thereafter denied NTS's business accreditation when Virk failed to respond to or address the BBB's concerns and requests for more information. Furthermore, the BBB has sent NTS dozens of consumer complaints and refund requests.

51. Virk also was aware that law enforcement officers were investigating consumer complaints about NTS. In January 2018, a police officer from the Milpitas Police Department contacted and interviewed Virk about consumer complaints. The Milpitas police officer informed Virk about a complaint from an older adult who received a pop-up warning on her computer claiming it had a virus. The woman called the phone number on the pop-up warning and reached NTS, which charged her to remove the purported virus. Virk told the Milpitas police officer that he owns NTS, provides Internet security services, and that he has a call center in India. The Milpitas Police advised Virk that they were referring the report to the BBB.

52. In May 2018, MasterCard flagged NTS's merchant account with a "High Fraud Alert" due to a high percentage of transactions being flagged as fraudulent.

53. As the owner, high-ranking corporate officer, and active participant in the daily activities of Defendant NTS, Virk knew that representations by NTS to consumers were false or deceptive, was recklessly indifferent to the truth or falsity of such representations, or was aware of a high probability that the representations were fraudulent and intentionally avoided the truth.

54. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission.

## VIOLATIONS OF THE FTC ACT

55. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

## Count I

## Deceptive Misrepresentations about Affiliations

56. In numerous instances, in connection with the advertising, marketing, promotion, offering for sale, or sale of computer technical support services and security software, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including Internet communications and telephone calls, that they are part of or affiliated with well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service products or to provide computer and technical support services.

57. In truth and in fact, Defendants are not part of or affiliated with such companies, nor have such companies certified or authorized Defendants to service their products or to provide computer and technical support services.

58. Therefore, Defendants' representations as set forth in Paragraph 56 above are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

## Count II

## Deceptive Misrepresentations about Viruses and Computer Security Issues

59. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of computer technical support services and security software, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including Internet communications and telephone calls, that they have detected security or performance issues on consumers' computers, including malicious software (such as viruses, spyware, and other malicious files), system compromises (such as infections or breaches), and other security vulnerabilities (such as claiming that the system has no security or is unprotected).

60. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 59 above, Defendants have not detected security or performance issues on consumers' computers.

61. Therefore, Defendants' representations as set forth in Paragraph 59 above are false, misleading, or were not substantiated at the time they were made and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

## VIOLATIONS OF THE TELEMARKETING SALES RULE

62. In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101–6108. The FTC adopted the original Telemarketing Sales Rule ("TSR") in 1995, extensively amended it in 2003, and amended certain sections thereafter.

63. Defendants are "seller[s]" or "telemarketer[s]" engaged in "telemarketing as defined by the TSR, 16 C.F.R. § 310.2(dd), (ff), and (gg).

64. Section 310.3(a)(2) of the TSR prohibits sellers or telemarketers from "misrepresenting, directly or by implication, in the sale of goods or services . . . affiliation with, or endorsement or sponsorship by, any person or government entity."

65. Section 310.3(a)(4) of the TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services.

66. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

### Count III

### Deceptive Telemarketing Calls in Violation of the TSR

### (Affiliations)

67. In numerous instances, in connection with telemarketing their goods and services, Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that Defendants are part of or affiliated with well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service products or to provide computer and technical support services.

68. Defendants' acts or practices, as described in Paragraph 67 above are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. §§ Section 310.3(a)(2) and 310.3(a)(4).

**Count IV**

**Deceptive Telemarketing Calls in Violation of the TSR**

**(Viruses and Computer Security Issues)**

69. In numerous instances, in connection with telemarketing their goods and services, Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that Defendants have detected security or performance issues on consumers' computers, including malicious software, such as viruses, spyware, and other malicious files, system compromises, such as infections or breaches, and other security vulnerabilities (such as claiming that the system has no security or is unprotected).

70. Defendants' acts or practices, as described in Paragraph 69 above are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. §§ 310.3(a)(2) and 310.3(a)(4).

**CONSUMER INJURY**

71. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the TSR. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust gains and enrichment, and harm the public interest.

72. Since 2016, Defendants have taken approximately $5 million from consumers through their deceptive and unlawful activities.

**THIS COURT'S POWER TO GRANT RELIEF**

73. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts,

restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

74. Section 19 of the FTC Act, 15 U.S.C. § 57b, and Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of TSR, including the rescission or reformation of contracts, and the refund of money.

**PRAYER FOR RELIEF**

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), Section 19(b) of the FTC Act, 15 U.S.C § 57b, the TSR, and the Court's own equitable powers, requests that the Court:

A. Award Plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief, including temporary and preliminary injunctions and an order freezing assets;

B. Enter a permanent injunction to prevent future violations of the FTC Act and the TSR by Defendants;

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act and the TSR, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

D. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

//

//

//

//

//

//

Dated: May 18, 2020

Respectfully submitted,
ALDEN F. ABBOTT
General Counsel

/s/ ***Ronnie Solomon***

Ronnie Solomon
Sarah Schroeder
Federal Trade Commission
901 Market Street, Suite 570
San Francisco, CA 94103
Phone: (415) 848-5100

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION