IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

UNIVERSAL NETWORK SOLUTIONS, LLC, a Colorado limited liability company, and RAJINDER SINGH, individually, and as a member and manager of Universal Network Solutions, LLC,

Defendants.

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 Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain 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).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

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

PLAINTIFFS

4. 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.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act 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).

DEFENDANTS

6. Defendant Universal Network Solutions, LLC ("Universal") is a limited liability company with its principal place of business at 4750 Uravan Street, Denver, CO 80249. Universal 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, Universal has advertised, marketed, distributed, or sold purported computer technical support services and security software to consumers throughout the United States.

7. Defendant Rajinder Singh formed Universal Network Solutions, LLC, listed his Denver, Colorado address as Universal's principal office and mailing address, and registered Universal's website, unsllc.us. At 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 Universal, including the acts and practices set forth in this Complaint. Defendant Singh 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

8. 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' BUSINESS ACTIVITIES

Overview

9. Since at least May 2016, Defendants have operated a scheme to deceive consumers into purchasing Defendants' purported technical support or computer security services in order to address alleged computer problems regardless of whether any problems actually exist. Defendants carry out their scheme by misrepresenting to consumers that their computers are infected with viruses or are otherwise compromised, and that the consumers' computer files are vulnerable to being stolen or lost. Defendants also falsely claim to be authorized by well-known technology companies, such as Microsoft or Norton, to service those companies' products and provide the needed technical support. Based on these misrepresentations, Defendants trick consumers into paying hundreds of dollars for technical support services they do not need.

Defendants' Computer Pop-Up Security Warnings

10. Consumers of Universal's services report that while on the Internet, a pop-up appears on their computers that they cannot close. The pop-ups are designed to appear as if they originated from the computer's operating system and often mislead consumers into believing that they are receiving a message from Microsoft or another well-known company.

11. The pop-up warns these consumers that their computers have been infected with

viruses or other malware and have serious security issues that put the consumer's information at risk of being lost or stolen. Sometimes the pop-up is accompanied by a voice recording warning of the security risk and adding to the urgency of the message. The pop-up instructs them to call a toll-free number listed in the message immediately to obtain assistance and prevent further harm. Exhibit A is an example of a pop-up that appeared during 2016 and directs the viewer to call a phone number that Defendants used. When the mouse is hovered over the Internet Explorer icon on the bottom left corner of the screen, sometimes the pop-up claims to be from "Microsoft Official Support." Exhibit B is an enlargement of this image.

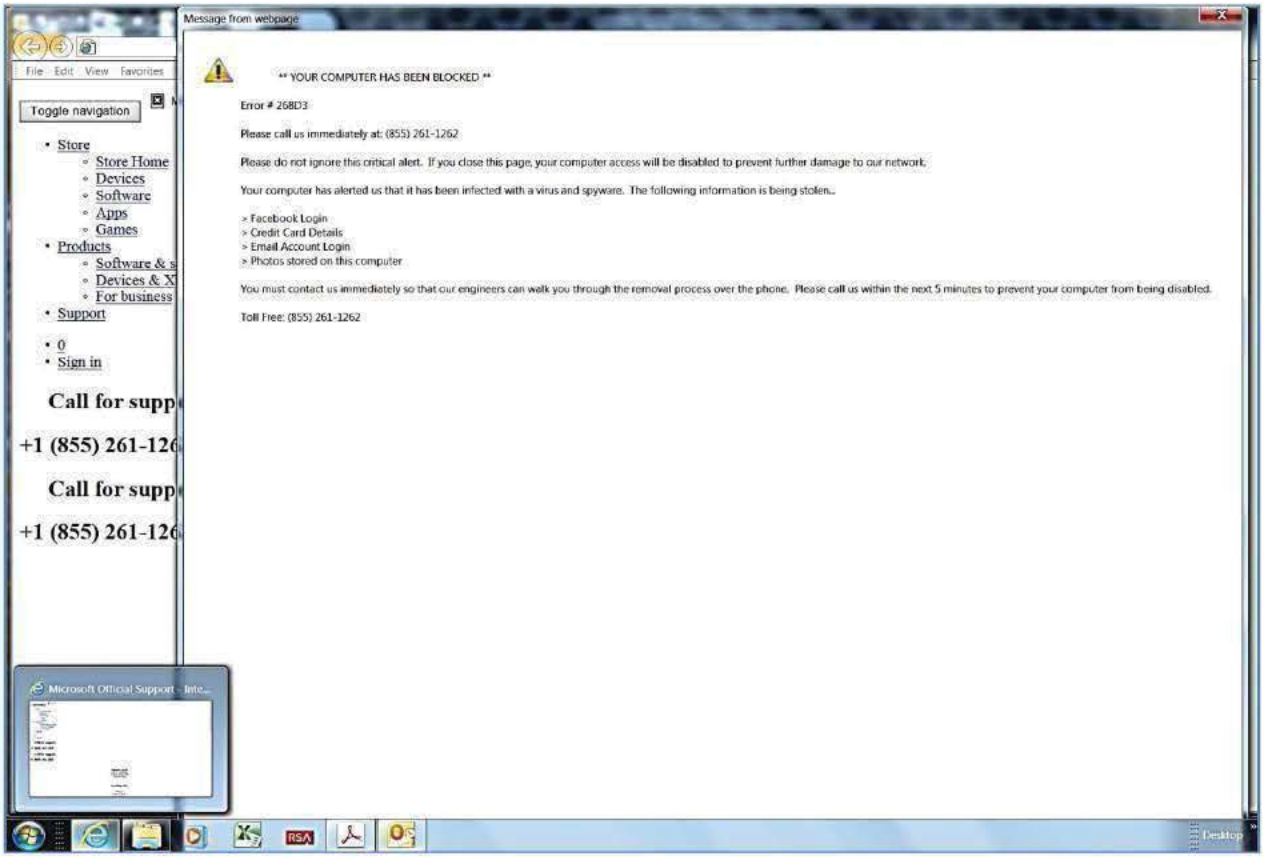

Exhibit A

Exhibit B

12. Defendants' pop-ups are typically designed so that consumers cannot close them by clicking on the "X" in the upper right hand corner, or navigate around them. The consumers' web browsers become unusable as a result of the pop-up.

Defendants Deceive Consumers into Buying Unnecessary Computer Technical Support Services and Security Software

13. When consumers call the phone number in the pop-up, Defendants' telemarketers answer and lead consumers through a deceptive sales pitch designed to convince them that their computers are in urgent need of repair.

14. To gain consumers' trust, Defendants claim that they are affiliated with Microsoft, Norton, or other well-known technology companies. One telemarketer told an FTC investigator that he was with Microsoft. Later, the telemarketer claimed service would be performed by a "Microsoft certified network support team." In fact, Defendants and their telemarketers are not affiliated with, or certified or authorized by, Microsoft.

15. After convincing consumers that the pop-ups indicate that there are problems with their computers and that Defendants are qualified to diagnose those problems and fix them, Defendants' telemarketers tell consumers that Defendants need to remotely access the consumers' computers to identify and resolve the specific problems. The telemarketers typically tell the consumer to go to a website, enter a remote access key, and follow the prompts to begin the remote access session. Once Defendants gain remote access, they are able to control the consumers' computers. During the remote access session, Defendants can view the consumer's computer screen, move the cursor, enter commands, run applications, and access stored information. Consumers can also see what Defendants are seeing and doing on their computers while Defendants have remote access.

16. Once in control of consumers' computers, Defendants run a series of purported diagnostic tests, which in reality, are nothing more than a high-pressured sales pitch designed to scare consumers into believing that their computers are corrupted, hacked, or otherwise compromised, or generally performing badly. For computers running versions of Microsoft Windows, these diagnostic tests often include displaying the computer's Event Viewer and the Microsoft System Configuration Utility ("msconfig") services tab.

17. To convince consumers that there is a problem that needs to be repaired, Defendants often show consumers numerous "Error" and "Warning" messages in the computer's Event Viewer. For example, Exhibit C is an image of an FTC computer during a January 6, 2017 undercover transaction, showing Defendants' use of the Event Viewer.

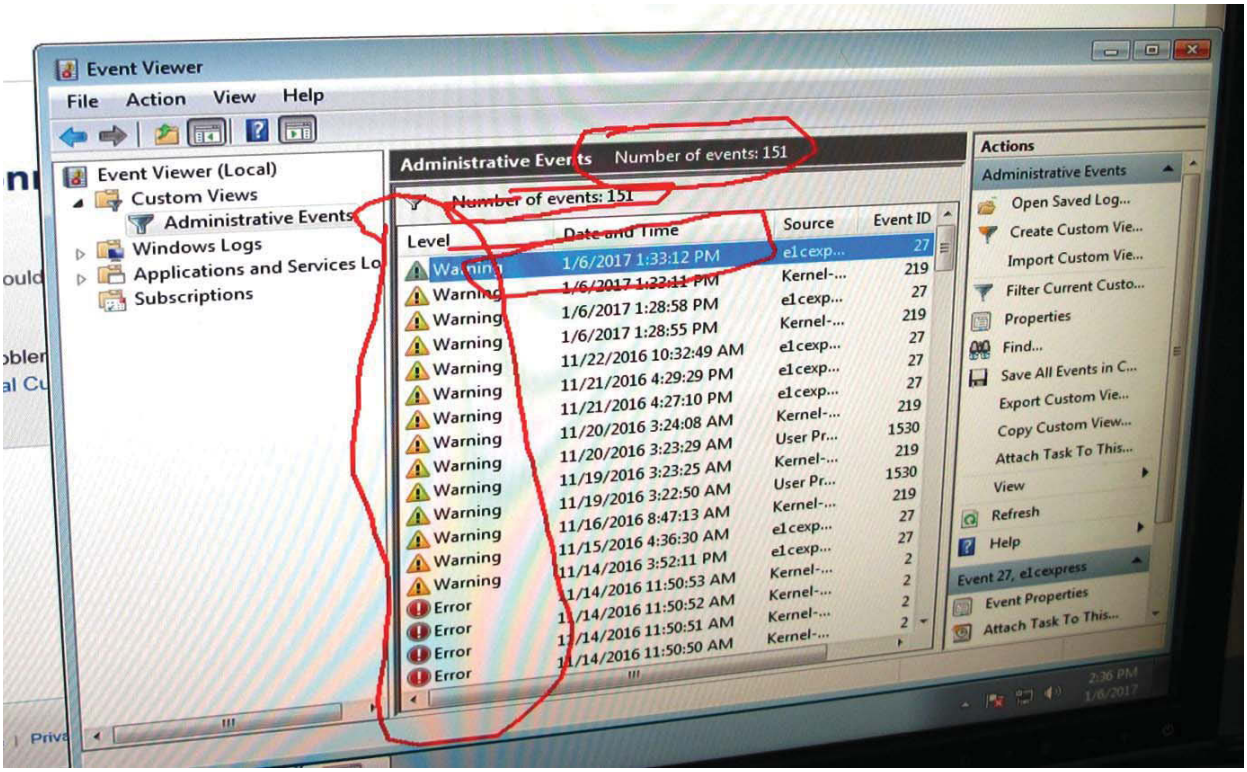

Exhibit C

18. While displaying this screen, Defendants' telemarketer remotely drew red circles around a number of error and warning messages displayed on the FTC computer's Event Viewer. He claimed that these messages were evidence that the FTC computer was riddled with computer problems, including 151 viruses. But these "errors" were simply normal computer operations. The FTC computer used during the undercover transaction was free of viruses, spyware, malware, or other security issues at the time.

19. Defendants also use the computer's System Configuration to show consumers that the computer problems purportedly have caused a number of Windows services to stop working. For example, during the same January 6, 2017 undercover transaction, the telemarketer prompted the System Configuration window on the FTC computer to show a number of "Stopped"

services." Exhibit D is an image of the same FTC computer showing Defendants' use of the System Configuration.

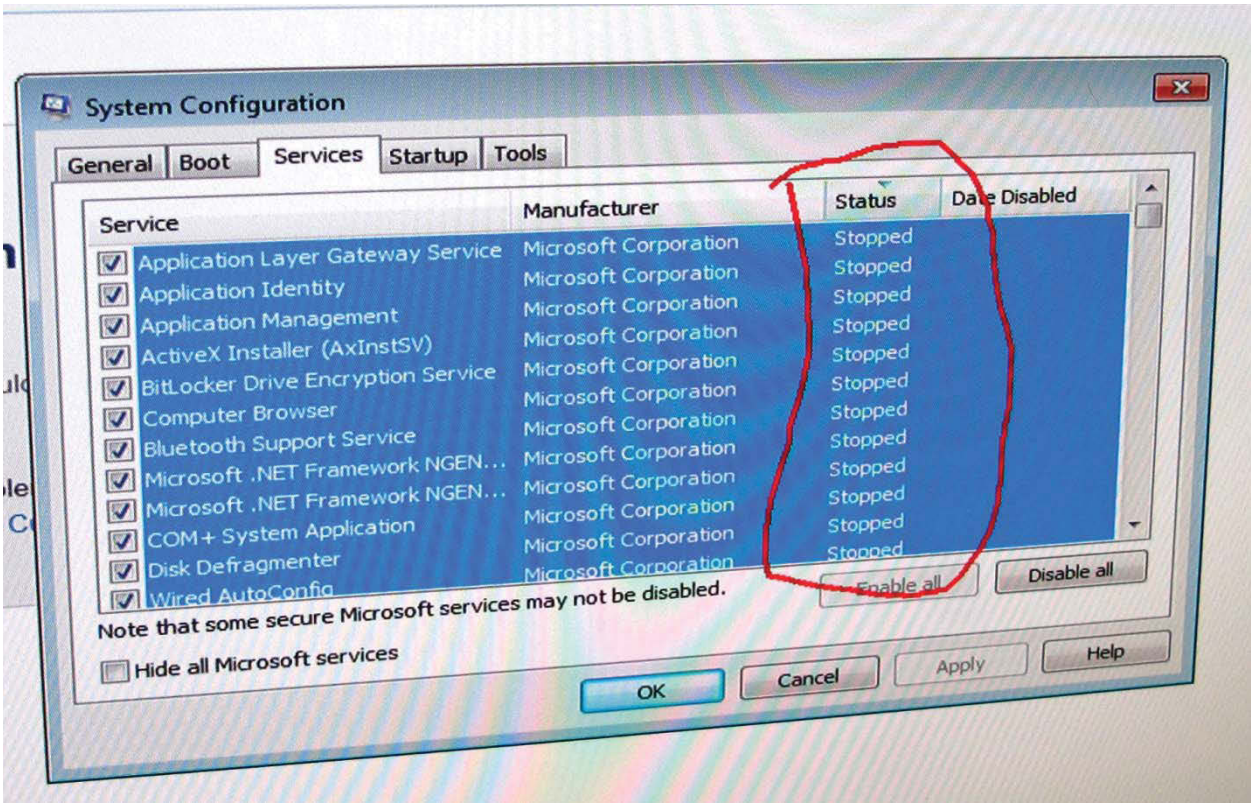

Exhibit D

20. Once again, the telemarketer remotely circled in red the FTC computer's screen, highlighting where services in the FTC computer's System Configuration were shown as "Stopped." The telemarketer then told the FTC investigator that the System Configuration showed that the "heart of the computer" had stopped. The telemarketer further claimed that the FTC computer was in immediate danger because viruses were entering the computer, and someone was trying to hack into the computer and steal information such as banking usernames and passwords.

21. In fact, it is impossible to know whether a computer is infected with malware, is being hacked, or is otherwise compromised based solely on the fact that the computer's Event Viewer contains "Error" and "Warning" messages, or the fact that the System Configuration lists a number of "Stopped" services. In the course of normal operations over time, a Windows system collects hundreds or thousands of "Error" or "Warning" messages. Similarly in the course of normal operations, Windows services that are not needed are designated as "Stopped," and such a designation in no way indicates a problem with the computer's system.

22. Defendants nevertheless use these innocuous "Error," "Warning," and "Stopped" messages to scare consumers into believing that their computers are not operating properly and are in urgent need of repair.

23. Defendants charge consumers from $99 to $199.99 to cleanup and fix the purported problems and a one-year service contract that covers two devices, $349.99 for a three-year service contract that also covers two devices, $499.99 for a five-year service contract that covers three devices, and $599.99 for a "lifetime" 15-year service contract that covers six devices.

24. Defendants pressure consumers to purchase the longer-term contracts, claiming that those contracts are already discounted because the services are "from Microsoft," and that the higher-priced plans cover more devices, even devices purchased in the future.

25. If a consumer agrees to pay, Defendants' telemarketers ask the consumer to pay by credit card or PayPal.

26. After charging consumers for technical support services, Defendants then spend one to three hours logged onto consumers' computers to perform the purported "repairs." In

numerous instances, these "repairs" are unnecessary or may even be harmful because Defendants have unfettered access to consumers' computers, allowing them to disable or install whatever software Defendants want onto the computers, or access sensitive personal information stored on a consumer's computer.

VIOLATIONS OF THE FTC ACT

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

28. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

Count I

Defendants' Deceptive Misrepresentations About Affiliations

29. In numerous instances, in connection with the marketing, offering for sale, or selling 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 telephone calls and internet communications, that they are part of or affiliated with well-known U.S. technology companies, such as Microsoft or Norton, or are certified or authorized by these companies to service their products.

30. In truth and in fact, Defendants are not part of or affiliated with these U.S. technology companies, nor are Defendants certified or authorized to service their products.

31. Therefore, Defendants' representations as set forth in Paragraph 29 of this Complaint 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

Defendants' Deceptive Misrepresentations About Security or Performance Issues

32. In numerous instances, in connection with the marketing, offering for sale, or selling 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 telephone calls and internet communications, that they have detected security or performance issues on consumers' computers, including system errors, viruses, spyware, malware, or the presence of hackers.

33. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 32, Defendants have not detected security or performance issues on consumers' computers.

34. Therefore, Defendants' representations as set forth in Paragraph 32 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).

CONSUMER INJURY

35. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act. 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 enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

36. 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.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and as authorized by 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 but not limited to, a preliminary injunction;

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

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

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

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel

Date: May 3, 2017

s/ Barbara Chun

Barbara Chun
Thomas Syta
FEDERAL TRADE COMMISSION
10877 Wilshire Blvd. Suite 700
Los Angeles, CA 90024
Telephone: (310) 824-4343
Email: bchun@ftc.gov; tsyta@ftc.gov
Attorneys for Plaintiff Federal Trade Commission