

FILED

2017 APR 24 AM 9:15

U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO
CLEVELAND

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

FEDERAL TRADE COMMISSION, and the

STATE OF OHIO,
OFFICE OF THE ATTORNEY GENERAL,

Plaintiffs,

v.

REPAIR ALL PC, LLC, an Ohio limited liability
company,

PRO PC REPAIR LLC, an Ohio limited liability
company,

I FIX PC LLC, an Ohio limited liability company,

WEBTECH WORLD LLC, a New Jersey limited
liability company,

ONLINE ASSIST LLC, a New Jersey limited
liability company,

DATADECK LLC, a Delaware limited liability
company,

I FIX PC, also d/b/a TECHERS247, I FIX PC,
and I FIX PC 247, a Canadian partnership,

JESSICA MARIE SERRANO, individually, as
owner of Repair All PC, LLC, and as owner and
officer of Pro PC Repair LLC and I Fix PC LLC,

FILE UNDER SEAL

1 Case No. 17 CV 0869

COMPLAINT FOR PERMANENT
INJUNCTION AND OTHER
EQUITABLE RELIEF

DISHANT KHANNA, individually and as
assistant director of Repair All PC, LLC,

MOHIT MALIK, individually and as an owner,
officer, and director of WebTech World LLC and
Online Assist LLC,

ROMIL BHATIA, individually and as director of
Datadeck LLC,

LALIT CHADHA, individually and as a partner
of I Fix PC, also d/b/a Techers247, I Fix PC,
and I Fix PC 247, and

ROOPKALA CHADHA, individually and as a
partner of I Fix PC, also d/b/a Techers247,
I Fix PC, and I Fix PC 247,

Defendants.

Plaintiffs, the Federal Trade Commission ("FTC") and the State of Ohio, Office of the
Attorney General, for their Complaint allege:

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 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).

2. The State of Ohio, by and through its Attorney General, Michael DeWine,
brings this action under the Ohio Revised Code ("R.C.") and the Consumer Sales Practices Act
("CSPA"), 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
R.C. 1345.01 *et seq.*, and its Substantive Rules, O.A.C. 109:4-3-01 *et seq.*

JURISDICTION AND VENUE

3. 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).

4. This Court has supplemental jurisdiction over the State of Ohio's claims pursuant to 28 U.S.C. § 1367.

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

PLAINTIFFS

6. 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.

7. 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).

8. The State of Ohio, Office of Attorney General, is the enforcing authority under the CSPA pursuant to R.C. 1345.01 *et seq.* and is authorized to pursue this action to enjoin violations of the CSPA and to obtain legal, equitable or other appropriate relief, including rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, or other relief as may be appropriate.

DEFENDANTS

Corporate Defendants

9. Defendant Repair All PC, LLC ("Repair All") is an Ohio limited liability company with its principal place of business at 3100 East 45th Street, Suite 408, Cleveland,

Ohio. Repair All 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, Repair All has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

10. Defendant Pro PC Repair LLC (“Pro PC”) is an Ohio limited liability company with its principal place of business at 3100 East 45th Street, Suite 320, Cleveland, Ohio. Pro PC 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, Pro PC has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

11. Defendant I Fix PC LLC (“I Fix-US”) is an Ohio limited liability company with its principal place of business at 4305 Bush Avenue, Cleveland, Ohio. I Fix-US 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, I Fix-US has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

12. Defendant WebTech World LLC (“WebTech”) is a New Jersey limited liability company with its principal place of business at 255 Lucas Lane, Apartment 7, Voorhees, New Jersey. WebTech 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, WebTech has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

13. Defendant Online Assist LLC (“Online Assist”) is a New Jersey limited liability company with its principal place of business at 255 Lucas Lane, Apartment 7, Voorhees, New

Jersey. Online Assist 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, Online Assist has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

14. Defendant Datadeck LLC (“DataDeck”) is a Delaware limited liability company with its principal place of business at 122 Delaware Street, Suite 11, 2nd Floor, New Castle, Delaware. DataDeck 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, DataDeck has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

15. Defendant I Fix PC, also doing business as Techers247, I Fix PC, and I Fix PC 247 (“Techers247”) is an Ontario, Canada partnership with its principal place of business at 39 O’Shea Crescent, Ajax, Ontario, Canada. Techers247 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, Techers247 has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

Individual Defendants

16. Defendant Jessica Marie Serrano (“Serrano”) is the owner and registered agent of Repair All, the owner and officer of Pro PC, and the owner, officer, and registered agent of I Fix-US. At all times material to this Complaint, acting alone or in concert with others, Defendant Serrano has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Serrano, in connection with the matters alleged herein, transacts or has transacted business in this district

and throughout the United States. Defendant Serrano manages the finances of Repair All, including opening at least one bank account, depositing consumer payments, issuing consumer refunds, and paying for business expenses. She also opened at least one merchant account for Repair All that was used to process credit card payments from consumers. She owns, pays for, and manages Repair All's website. She also manages the finances of Pro PC and I Fix-US, including opening at least two bank accounts for Pro PC and at least one bank account for I Fix-US, depositing consumer payments, issuing consumer refunds, and paying for business expenses, including advertising, telephone and web hosting services, computer remote access service, and a virtual office used by Pro PC.

17. Defendant Dishant Khanna ("Khanna") is the assistant director of Repair All. At all times material to this Complaint, acting alone or in concert with others, Defendant Khanna has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Khanna, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States. Defendant Khanna helped manage Repair All's merchant account used to process consumers' credit card payments, including the account's chargebacks and reserve funds. He has also communicated directly with an investigator at the Cuyahoga County Department of Consumer Affairs, including discussing a consumer complaint and Repair All's advertising and refund policies. He has also worked with Defendant Serrano to secure a virtual office used by Pro PC.

18. Defendant Mohit Malik ("Malik") is the owner, officer, director, and registered agent of WebTech and Online Assist. At all times material to this Complaint, acting alone or in concert with others, Defendant Malik has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Malik, in connection with the matters alleged herein, transacts or has transacted business in this district

and throughout the United States. Defendant Malik owns, pays for, and manages WebTech's and Online Assist's websites, for which he also secured domain privacy services.

19. Defendant Romil Bhatia ("Bhatia") is the director of DataDeck. At all times material to this Complaint, acting alone or in concert with others, Defendant Bhatia has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Bhatia, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States. Defendant Bhatia manages the finances of DataDeck, including opening at least two bank accounts, depositing consumer payments, wiring significant funds to Repair All, and paying for business expenses, including advertising, telephone service, computer remote access service, and a physical office used by DataDeck. He also owns, pays for, and manages Techers247's website, for which he also secured domain privacy services.

20. Defendant Lalit Chadha ("L. Chadha") is a partner of Techers247. At all times material to this Complaint, acting alone or in concert with others, Defendant L. Chadha has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant L. Chadha, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States. Defendant L. Chadha owned, paid for, and managed Techers247's website before recently transferring it to Defendant Bhatia.

21. Defendant Roopkala Chadha ("R. Chadha") is a partner of Techers247. At all times material to this Complaint, acting alone or in concert with others, R. Chadha has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant R. Chadha, in connection with the matters

alleged herein, transacts or has transacted business in this district and throughout the United States.

Common Enterprise

22. Defendants Repair All, Pro PC, I Fix-US, WebTech, Online Assist, DataDeck, and Techers247 (collectively, “Corporate Defendants”) have operated as a common enterprise while engaging in the deceptive acts and practices and other violations of law alleged below. Corporate Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, business functions, and office locations, and that commingled funds. For example, they share some of the same telephone numbers and customer support email addresses, demonstrating that they employ and control the same telemarketers who solicit and sell to consumers. They also employ some of the same managerial or supervisory personnel who interact with consumers and other third parties. Further, they share some business addresses where consumers have sent check payments or other mail. Moreover, they transfer substantial funds to each other, by electronic transfers and checks. Because these Corporate Defendants have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Defendants Serrano, Khanna, Malik, Bhatia, L. Chadha, and R. Chadha have formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Corporate Defendants that constitute the common enterprise.

COMMERCE

23. 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

24. Defendants operate a scheme that deceives consumers into buying unnecessary computer technical support services and security software to address purported problems with consumers' computers that Defendants do not actually know exist. In carrying out their scheme, Defendants use computer pop-up security warnings ("pop-up warnings") that appear on consumers' computer screens and advise consumers that their computers are infected with viruses, are being hacked, or are otherwise compromised. The pop-up warnings instruct consumers to call a toll-free number to fix the purported computer problems. When consumers call, Defendants misrepresent to consumers that their computers are indeed infected with viruses, are being hacked, or are otherwise compromised. Defendants falsely claim to be affiliated with well-known technology companies, such as Microsoft or Apple, or authorized by those companies to service consumers' computers. Since at least 2013, Defendants have caused substantial harm to consumers through their scheme.

Defendants' Computer Pop-Up Security Warnings Lure Consumers

25. 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 computer's operating system and often mislead consumers into believing that they are receiving a message from Microsoft, Apple, or their Internet service provider. The pop-up warnings advise consumers that their computers have been compromised by viruses, hackers, or other threats and urge consumers to immediately call the toll-free number listed in the message to resolve the computer problems. The pop-up warnings are designed so that consumers are unable to close or navigate around them, rendering the Internet browser unusable. This practice is known as "browser hijacking." In some instances, the pop-up warnings instruct consumers not to close the

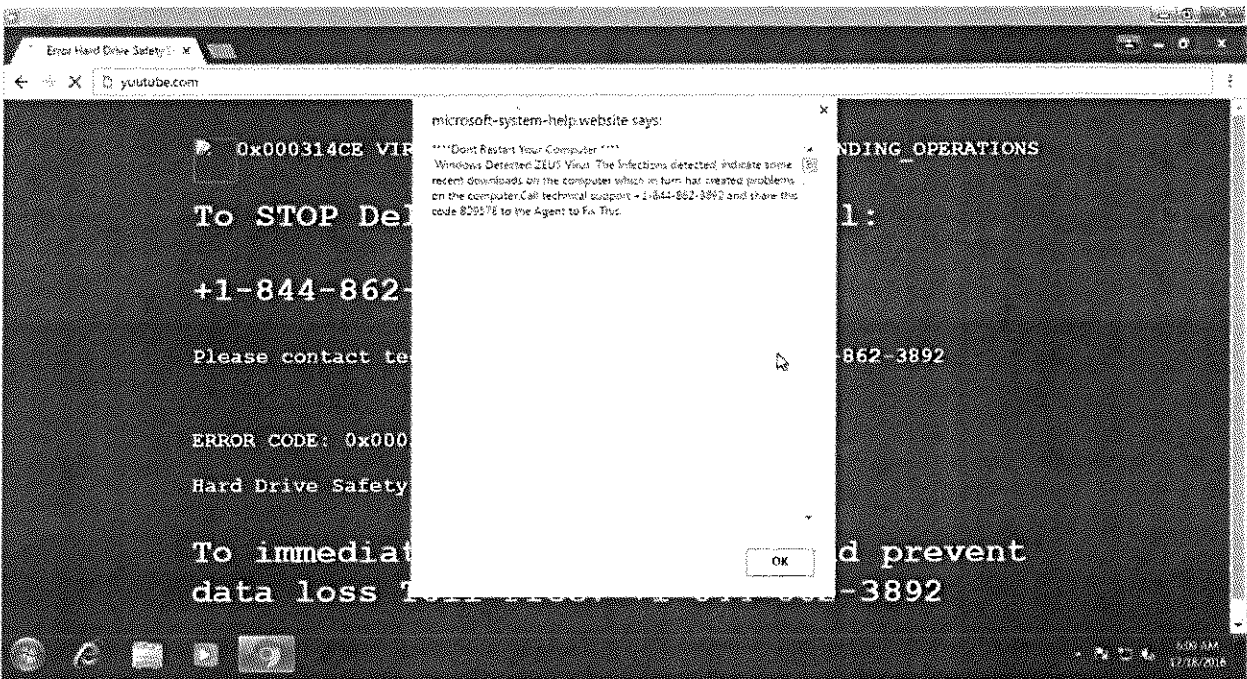
message to avoid further problems in the computer. For example, Image A below is a screenshot of a pop-up warning captured from an undercover call to Defendant WebTech conducted on December 18, 2016. The pop-warning states:

micorsoft-system-help.website says:

******Dont Restart Your Computer******

Windows Detected ZEUS Virus, The Infections detected, indicate some recent downloads on the computer which in turn has created problems on the computer.Call technical support +1-844-862-3892 and share this code B2957E to the Agent to Fix This.

Image A



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

26. Consumers who call the toll-free numbers contained in the pop-up warnings are connected to Defendants' telemarketers. The telemarketers then lead consumers through a sales pitch designed to convince consumers that their computers are in urgent need of repair, even though the telemarketers do not know that an actual problem in the computer exists.

27. Defendants' telemarketers begin by asking consumers what the computer problem is, according to the pop-up warnings. After consumers explain the message in the pop-up warnings, the telemarketers purport to confirm the computer problem and then assure consumers that they can fix it.

28. To gain consumers' trust, Defendants' telemarketers claim that they are affiliated with Microsoft or Apple or are otherwise certified or authorized by those companies to service consumers' computers. In fact, Defendants and their telemarketers are not affiliated with or certified or authorized by Microsoft or Apple.

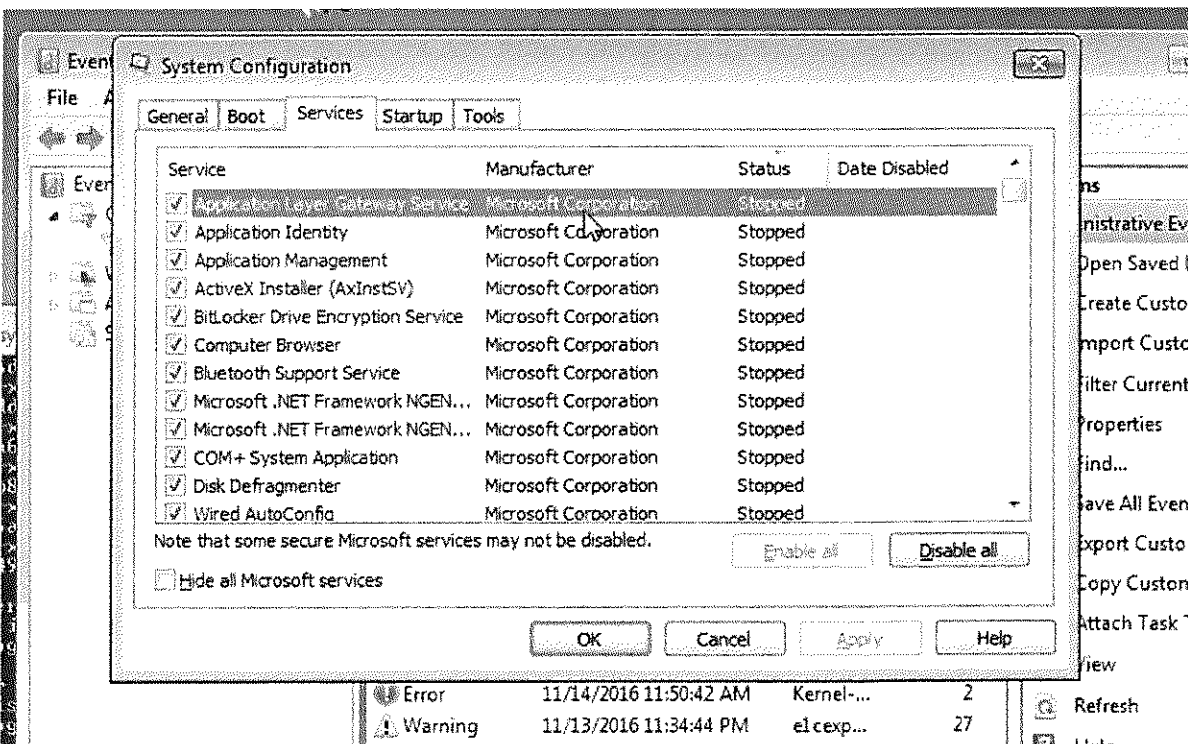
29. After convincing consumers that the pop-up warnings indicate that there are problems with their computers and that Defendants' telemarketers are qualified to diagnose and fix those problems, the telemarketers tell consumers that they need to remotely access the consumers' computers to diagnose and resolve the specific problems. The telemarketers typically direct consumers to go to a website, enter a code, and follow the prompts to begin the remote access session. Once the telemarketers gain remote access, they are able to control the consumers' computers. Among other things, the telemarketers can view the computer screen, move the mouse or cursor, enter commands, and run applications. At the same time, consumers can see what the telemarketers are seeing and doing on their computers.

30. Once in control of consumers' computers, Defendants' telemarketers run a series

of purported diagnostic tests, which, in reality, is nothing more than a high-pressured sales pitch designed to scare consumers into believing that their computers are infected with viruses, are being hacked, or are otherwise compromised.

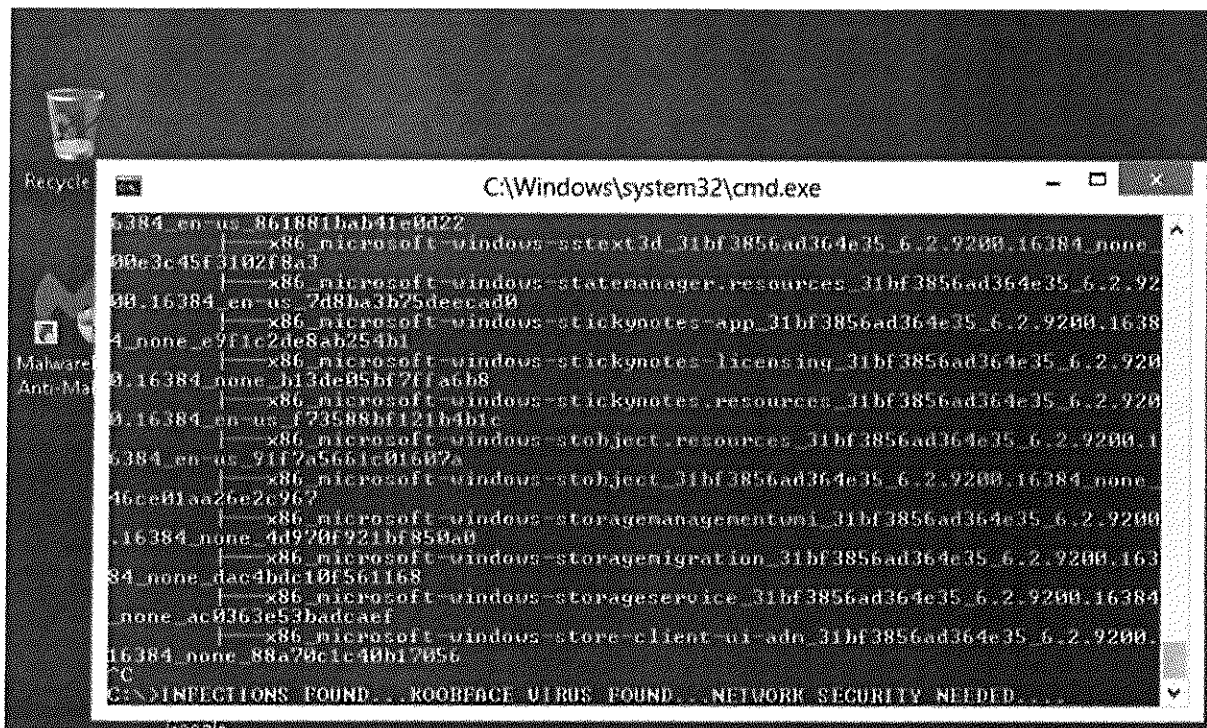
31. For example, to convince consumers that there is a problem that needs to be repaired, Defendants' telemarketers run the "msconfig" command, which opens the System Configuration utility in the computer. The telemarketers then wrongly claim that all Windows services listed in System Configuration should be in the "Running" state and that the Windows services listed in the "Stopped" state are evidence of viruses or serious problems in the computer. For example, Image B below is a screenshot of System Configuration, which was prompted by the telemarketer and lists a number of "Stopped" Windows services, captured from an undercover call to Defendant Online Assist on February 1, 2017.

Image B



32. Defendants' telemarketers also run the "dir/s" command, which displays a list of files in the computer and a total file count at the end. The telemarketers then claim that the file count represents all the files that had been infected with a virus. Similarly, the telemarketers also run the "tree" command, which displays a list of files and directories in the computer. The telemarketers then manipulate the "tree" command output by adding an alarming message at the end of the listing. For example, Image C below is a screenshot of the "tree" command output captured from an undercover call to Defendant Repair All conducted on April 28, 2016. The telemarketer added the following alarming yet false text at the end of the "tree" command output: "INFECTIONS FOUND...KOOBFACE VIRUS FOUND...NETWORK SECURITY NEEDED..." In some instances, the telemarketers tell consumers the name of a virus, such as "Zeus" or "Koobface," and then search the definition of the virus on the Internet and instruct consumers to read about the virus.

Image C



```
C:\Windows\system32\cmd.exe

6384_en-us_861881bab41e8d22
|x86_microsoft-windows-estext13d_31bf3856ad364e35_6.2.9200.16384_none_
00e3c45f3102f8a3
|x86_microsoft-windows-statemanager.resources_31bf3856ad364e35_6.2.92
00.16384_en-us_7d8ba3b25deecad0
|x86_microsoft-windows-stickynotes-app_31bf3856ad364e35_6.2.9200.1638
4_none_e9ffc2de8ab254b1
|x86_microsoft-windows-stickynotes-licensing_31bf3856ad364e35_6.2.920
0.16384_none_b13de85bf2ffa6b8
|x86_microsoft-windows-stickynotes.resources_31bf3856ad364e35_6.2.920
0.16384_en-us_f73588bf121b4b1c
|x86_microsoft-windows-stobject.resources_31bf3856ad364e35_6.2.9200.1
6384_en-us_91f7a5661c01607a
|x86_microsoft-windows-stobject_31bf3856ad364e35_6.2.9200.16384_none_
46ce01aa26e2c967
|x86_microsoft-windows-storagemanagementui_31bf3856ad364e35_6.2.9200
.16384_none_4d970f921bf850a0
|x86_microsoft-windows-storagemigration_31bf3856ad364e35_6.2.9200.163
84_none_dac4bdc10f561168
|x86_microsoft-windows-storageservice_31bf3856ad364e35_6.2.9200.16384
_none_ac0363e53badcaef
|x86_microsoft-windows-store-client-ui-adm_31bf3856ad364e35_6.2.9200.
16384_none_88a79c1c40b17056
C:\>INFECTIONS FOUND...KOOBFACE VIRUS FOUND...NETWORK SECURITY NEEDED...
```

33. Defendants' telemarketers also run the "netstat" command, which displays information about the network to which the consumer's computer is connected, in a table format. The telemarketers then claim that the information displayed on the "netstat" command output is proof that hackers have accessed or are attempting to access the computer. For example, Image D below is a screenshot of the "netstat" command output captured from the undercover call to Defendant Repair All on April 28, 2016. The telemarketer falsely claimed that the entries stating "ESTABLISHED" was evidence of current or imminent hacking of the computer.

Image D

```
Microsoft Windows [Version 6.0.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Anyone>NETSTAT

Active Connections

Proto Local Address           Foreign Address         State
TCP    192.168.163.128:50116    cnc:https               CLOSE_WAIT
TCP    192.168.163.128:50120    cnc:https               CLOSE_WAIT
TCP    192.168.163.128:50287    a184-85-215-67:http     CLOSE_WAIT
TCP    192.168.163.128:50288    a184-85-215-67:http     CLOSE_WAIT
TCP    192.168.163.128:50289    a184-85-215-67:http     CLOSE_WAIT
TCP    192.168.163.128:50290    a184-85-215-67:http     CLOSE_WAIT
TCP    192.168.163.128:50347    64.74.103.145:https     ESTABLISHED
TCP    192.168.163.128:50353    64.74.103.145:https     CLOSE_WAIT
TCP    192.168.163.128:50388    64.74.103.145:https     ESTABLISHED
TCP    192.168.163.128:50389    64.74.103.145:https     CLOSE_WAIT
TCP    192.168.163.128:50390    64.74.103.145:https     ESTABLISHED
TCP    192.168.163.128:50394    ord31s22-in-f3:https    ESTABLISHED
TCP    192.168.163.128:50401    ord36s02-in-f3:https    ESTABLISHED
TCP    192.168.163.128:50406    at114s38-in-f4:https    ESTABLISHED
TCP    192.168.163.128:50408    ig-in-f239:https        ESTABLISHED
TCP    192.168.163.128:50409    ord30s26-in-f14:https   ESTABLISHED
TCP    192.168.163.128:50410    at114s38-in-f4:https    ESTABLISHED
TCP    192.168.163.128:50412    ord36s02-in-f3:https    ESTABLISHED
TCP    192.168.163.128:50413    text-1b:https           ESTABLISHED
TCP    192.168.163.128:50415    upload-1b:https         ESTABLISHED
TCP    192.168.163.128:50421    ord30s26-in-f14:https   ESTABLISHED

C:\Users\Anyone>
```

34. In truth, it is impossible to know whether a computer is infected with viruses, is being hacked, or is otherwise compromised based solely on the fact that the System Configuration lists a number of “Stopped” Windows services, that the “dir/s” and “tree” commands displays a list of computer files and directories, or that the “netstat” command displays entries stating “ESTABLISHED.” In fact, it is normal for Windows services that are not needed to be designated as “Stopped,” and this in no way indicates a computer problem. Further, the “dir/s” and “tree” command outputs merely show the files and directories in the computer; they do not indicate a computer problem, unless manipulated for malicious reasons. Moreover, the information displayed on the “netstat” command output shows only the connections in the same network as the computer, and it does not indicate the presence of hackers accessing or attempting to access the computer.

35. Defendants’ telemarketers nevertheless use these kinds of tactics to scare consumers into believing that their computers are not operating properly and are in urgent need of repair. The telemarketers then sell their services, which could include a one-time “fix” or long-term service plans that cost hundreds of dollars.

36. Consumers who do not agree, or hesitate, to pay for the computer technical support services and security software that Defendants’ telemarketers recommend are subjected to intense pressure. In at least some instances, when the telemarketers sensed that the victim was becoming uncooperative, the telemarketers executed the “syskey” application, which allows the telemarketer to set a secret password that would make the computer unusable until the password is entered. This is a common tactic to hold computers for ransom, and there is no legitimate reason for the telemarketers to set such a password.

37. If consumers agree to pay, Defendants’ telemarketers ask for their credit card information. More recently, however, the telemarketers ask consumers to pay by electronic

check or by mailing a physical check to an address in the United States provided by the telemarketers. After consumers pay, Defendants' telemarketers perform services that, in many instances, consumers do not need.

VIOLATIONS OF THE FTC ACT

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

39. 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 (By Plaintiff FTC)

40. 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 Apple, or are certified or authorized by these companies to service their products.

41. 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.

42. Therefore, Defendants' representations as set forth in Paragraph 40 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
(By Plaintiff FTC)

43. 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.

44. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 43, Defendants have not detected security or performance issues on consumers' computers.

45. Therefore, Defendants' representations as set forth in Paragraph 43 of this Complaint 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 OHIO CONSUMER SALES PRACTICES ACT

46. R.C. 1345.02(A) prohibits suppliers from committing "an unfair or deceptive act or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during or after the transaction."

47. R.C. 1345.03(A) prohibits suppliers from committing "an unconscionable act or practice in connection with a consumer transaction. Such an unconscionable act or practice by a supplier violates this section whether it occurs before, during, or after the transaction."

48. Defendants are “suppliers” under the CSPA, as that term is defined in R.C. 1345.01(C) to mean “a seller, lessor, assignor, franchisor, or other person engaged in the business of effecting or soliciting consumer transactions, whether or not the person deals directly with the consumer.”

49. Defendants’ transactions described herein constitute “consumer transactions” under the CSPA, as that term is defined in R.C. 1345.01(A) to mean “a sale, lease, assignment, award by chance, or other transfer of an item of goods, a service, a franchise, or an intangible, to be an individual for purposes that are primarily person, family, or household, or solicitation to supply any of these things.”

Count III
Ohio Consumer Sales Practices Act Violation
(By Plaintiff State of Ohio)

50. 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 through telephone calls and internet communications, that Defendants are part of well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service their products.

51. 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.

52. Defendants’ representations as set forth in Paragraph 50 are false and misleading and likely to mislead consumers acting reasonably, and/or consumers within the State of Ohio were actually misled by Defendants’ misrepresentations in violation of R.C. 1345.02.

Count IV
Ohio Consumer Sales Practices Act Violation
(By Plaintiff State of Ohio)

53. 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 through 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.

54. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 53, Defendants have not detected security or performance issues on consumers' computers.

55. Defendants' representations as set forth in Paragraph 53 are false and misleading and likely to mislead consumers acting reasonably, and/or consumers within the State of Ohio were actually misled by Defendants' misrepresentations in violation of R.C. 1345.03(6).

CONSUMER INJURY

56. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the CSPA. 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

57. 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.

58. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow Plaintiff State of Ohio, Office of Attorney General, to enforce its state law claims against Defendants in this Court for violations of the CSPA, including injunctive relief, rescission or reformation of contracts, the refund of monies paid, and the disgorgement of ill-gotten monies.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and Plaintiff State of Ohio, pursuant to R.C. 1345.07(A), and as authorized by the Court's own equitable powers, request that the Court:

A. Award Plaintiffs 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, temporary and preliminary injunctions, and an order providing for immediate access, the turnover of business records, an asset freeze, the appointment of a receiver, and the disruption of domain and telephone services;

B. Enter a permanent injunction to prevent future violations of the FTC Act and the CSPA by Defendants under these or any other names, their agents, servants, representatives, salespersons, employees, successors, and assigns and all persons acting in concert or participation with Defendants, directly or indirectly;

C. Issue a declaratory judgment declaring that each act or practice complained of herein violates the CSPA in the manner set forth in the Complaint;

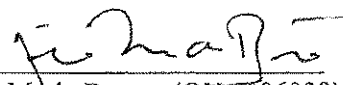
D. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act and the CSPA, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies;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

E. Award Plaintiffs 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

Dated: 4/24/2017

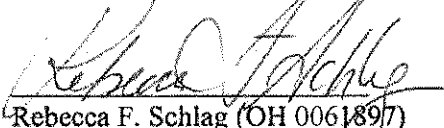

Fil-M de Banate (OH 0086039)
Amy C. Hocevar (OH 0075510)
Adrienne M. Watson (OH 0089568)
Federal Trade Commission
1111 Superior Avenue East, Suite 200
Cleveland, Ohio 44114
Telephone: (216) 263-3413 (de Banate)
Telephone: (216) 263-3409 (Hocevar)
Telephone: (216) 263-3411 (Watson)
Facsimile: (216) 263-3426
fdebanate@ftc.gov
ahocevar@ftc.gov
awatson@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

Dated:

April 24, 2017

MICHAEL DeWINE
OHIO ATTORNEY GENERAL


Rebecca F. Schlag (OH 0061897)
Senior Assistant Attorney General
Consumer Protection Section
Cleveland Regional Office
615 West Superior Avenue, Floor 11
Cleveland, Ohio 44113
Telephone: (216) 787-3030
Rebecca.Schlag@OhioAttorneyGeneral.gov

Attorneys for Plaintiff
STATE OF OHIO