UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JUDGE ENGELMAYER

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

Pecon Software Ltd., a corporation, also d/b/a Pecon Services LLC, Pecon Services, Inc.,

Pecon Infotech Ltd., a corporation,

Pecon Software UK Ltd., a corporation,

Mahesh Kumar Shah, a/k/a MK Shah, individually and as an officer of Pecon Software Ltd and Pecon Infotech Ltd.,

Prateek Shah, individually and as an officer of Pecon Software Ltd and Pecon Infotech Ltd.,

Sujoy Roy, individually and as an officer of Pecon Software Ltd and Pecon Infotech Ltd.,

Zulfiquar Ali, individually and as an officer of Pecon Software Ltd and Pecon Infotech Ltd., and

Vikas Kumar Gupta, individually and as an officer of Pecon Software Ltd and Pecon Infotech Ltd., also d/b/a Arya Global Services,

Defendants.

Case No. 12 CV 7186

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

FILED
12 SEP 24 PM 2:52
S.D. OF N.Y.

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

1. The FTC brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b) and 57b, and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108, 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 the Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, as amended.

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), 53(b), 57b, 6102(c), and 6105(b).

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

PLAINTIFF

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. 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.

5. 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), and 6105(b).

DEFENDANTS

6. Defendant Pecon Software Ltd., d/b/a Pecon Services LLC, Pecon Services, Inc., is an Indian corporation with its principal place of business at EN 27 Advantage Tower, 2nd Floor, Sector V, Salt Lake, Kolkata, West Bengal, India 700091 in India. Pecon Software Ltd. 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, Pecon Software Ltd. has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

7. Defendant Pecon Infotech Ltd. is an Indian corporation with its principal place of business at EN 27 Advantage Tower, 2nd Floor, Sector V, Salt Lake, Kolkata, West Bengal, India 700091 in India. Pecon Infotech Ltd. 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, Pecon Infotech Ltd. has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

8. Pecon Software UK Ltd is a United Kingdom corporation with its principal place of business at Suite 250, 162-168 Regent Street, London UK W1B 5TD. Pecon Software UK Ltd. 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, Pecon Software UK Ltd. has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

9. Defendant Mahesh Kumar Shah, a/k/a MK Shah, is the CEO and Managing Director of Pecon Software Ltd. and Pecon Infotech Ltd. 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 Pecon Software Ltd. and Pecon Infotech Ltd. set forth in this Complaint. Defendant Mahesh Kumar Shah resides in West Bengal, India and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

10. Defendant Prateek Shah is a Director of Pecon Software Ltd. 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 Pecon Software Ltd. set forth in this Complaint. Defendant Prateek Shah resides in West Bengal, India and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

11. Defendant Sujoy Roy is a Director and Chief Operating Officer of Pecon Software Ltd. 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 Pecon Software Ltd. set forth in this Complaint. Defendant Sujoy Roy resides in West Bengal, India and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

12. Defendant Zulfiquar Ali is a Director of Pecon Software Ltd. 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 Pecon Software Ltd. set forth in this Complaint. Defendant Zulfiquar Ali resides in West Bengal, India and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

13. Defendant Vikas Kumar Gupta is Vice President of Business Development and Customer

Service Manager of Pecon Software Ltd. 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 Pecon Software Ltd. set forth in this Complaint. Defendant Vikas Kumar Gupta resides in India and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

14. Defendants Pecon Software Ltd., d/b/a Pecon Services LLC, Pecon Services, Inc., Pecon Infotech Ltd., and Pecon Software UK Ltd. (collectively "Corporate Defendants") have operated as a common enterprise while engaging in the illegal acts and practices alleged below. The Corporate Defendants have conducted the business practices described below through interrelated companies that have common ownership, officers, managers, business functions, employees, and office locations. For example, Mahesh Kumar Shah is the CEO of Pecon Software Ltd. and Pecon Infotech Ltd. Pecon Infotech Ltd. registered the Corporate Defendants' home domain, *pecon.co.in*. On this website, Pecon Infotech Ltd. and Pecon Software Ltd. are both listed, and they share the same corporate address as well as the same corporate phone number. In addition, this domain shares the same IP address with other domains registered by Pecon Software Ltd. Pecon Software UK Ltd. is used as the contact and billing address for credit card sales made by consumers for the Corporate Defendants' services.

15. Because the Corporate Defendants have operated as a common enterprise, each individual entity is jointly and severally liable for the acts and practices alleged below. The Defendants Mahesh Kumar Shah, Prateek Shah, Sujoy Roy, Zulfiquar Ali, and Vikas Kumar Gupta 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

16. At all times material to this Complaint, the 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

17. The Defendants operate a massive telemarketing scheme that tricks consumers into spending from $159 - $259 to fix non-existent problems with their computers. By exploiting consumers' legitimate concerns about Internet threats like spyware and viruses, the Defendants scare consumers into believing that their computers are in imminent danger of crashing in order to sell consumers otherwise free software protection products and unnecessary computer security or technical support services.

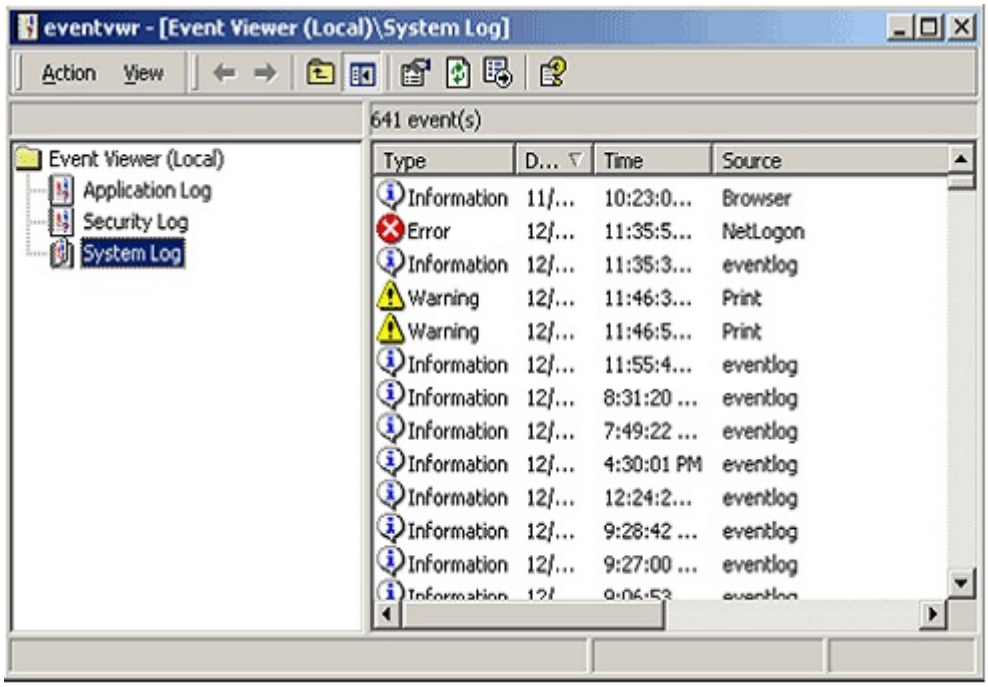
Defendants Lure Consumers to Purchase Their Services

18. Since at least 2008, the Defendants have been cold calling consumers in the United States and other English speaking countries and falsely claiming that they are from or affiliated with well-known computer manufacturers or computer security companies such as Microsoft.

19. After the Defendants have tricked the consumers into thinking they are dealing with their computer manufacturer or a computer security company, the Defendants scare the consumers into believing that they have viruses or other malware on their computers.

20. To mislead the consumers into believing that their computers are infected with viruses or other malware, the Defendants direct the consumers to a program on their computer called the Event Viewer. The Event Viewer is a log of the various activities that occur during a computer's operation. Many of the entries in the Event Viewer simply reflect that a computer operation was

completed successfully. Other entries, marked with a red X or a yellow triangle, are error or warning messages that indicate that a particular computer operation was not successful. If, for example, a program failed to run correctly because the user was not connected to the Internet, the Event Viewer may record an error or warning message. Despite their potentially alarming appearance, these messages are innocuous. They are generated during the normal operation of a computer. A screenshot of a sample Event Viewer appears below:



21. After directing the consumer to the Event Viewer, the Defendants often will ask the consumers if they see any entries with errors or warnings marked with red X's or yellow triangles. When the consumers respond that they do, the Defendants will state that these entries confirm that there are viruses or other malware present on the consumers' computers and that the computers are in danger of crashing.

22. This claim is baseless. It is impossible to know whether or not a computer is infected with viruses or malware based solely on the fact that the computer's Event Viewer contains

warning or error messages. Computers that are completely free of viruses or other malware will still create warning and error messages in their Event Viewers during normal operation. The Defendants mislead consumers who do not understand these messages' technical significance into believing that their computers are severely compromised.

23. Having convinced the consumers that their computers are in imminent danger, the Defendants then direct the consumers to a website and instruct them to enter a code or download a software application to allow the Defendants remote access to the consumers' computers. Once the Defendants have remote access, they are able to completely control the consumers' computers and can, for example, move the cursor, enter commands, run applications, and access stored information.

24. After gaining remote access, the Defendants continue their deception by focusing the consumer's attention on a list of innocuous files, emphasizing the risk these files supposedly pose, and stressing the urgent need for the consumer to buy the Defendants' products and services to prevent the computer from crashing.

25. The Defendants then attempt to sell the consumer illusory long-term "security" or "technical support" services and perform unnecessary "repairs," including installing otherwise free programs, such as trial versions of antivirus programs, and deleting the innocuous files they falsely claimed were viruses. The Defendants charge consumers for these services in an amount ranging from approximately $159 to $299.

26. The Defendants next direct the consumer to one of several websites they operate in order to pay for the computer security or technical support service. The Defendants' websites are highly interactive. They purport to allow consumers to chat directly with representatives, leave their contact information to request a call-back, and also browse and pay for various services

online. In numerous instances, the Defendants register their websites through privacy protection services that mask their true identity. As a result, consumers are unable to determine the true owner of the website or the fact that the same company operates multiple websites.

27. If consumers do not agree to pay for the service the Defendants typically apply pressure to the consumers. The Defendants will warn consumers about the harm that will come to their computers if they do not allow the Defendants remote access to fix the computers.

28. Afterwards, the Defendants assert they have fixed the non-existent problems. In reality, Defendants merely charged consumers for repair products and services they did not need.

29. In numerous instances, the Defendants call consumers who are registered on the National Do Not Call Registry.

30. In numerous instances, the Defendants call consumers who are within a given area code when the Defendants have not paid the required annual fee for access to telephone numbers within that area code that are included in the National Do Not Call Registry.

31. The Defendants also deliver misleading information to consumers' caller ID systems that indicates the calls are local to the country being called even though they originate in India. At least four telephone numbers commonly used by the Defendants have New York City area codes. When consumers ask the Defendants where they are calling form, the Defendants will often tell the consumers that they are calling from New York, even though the calls are being made from India.

32. The Defendants also call consumers using a phone number that belongs to Quinnipiac University. The name Quinnipiac appears on consumers' caller ID systems and the phone number is a legitimate Quinnipiac phone number. However, when consumers answer their telephones, it is not someone from Quinnipiac University, but rather the Defendants informing

consumers that their computers are infected.

The Role of Mahesh Kumar Shah

33. Mahesh Kumar Shah is the CEO and President of Pecon Software Ltd. and Pecon Infotech Ltd. Shah used his credit card to set up Ebay/PayPal accounts used to process consumers' credit cards. Shah's credit card was used to pay for the Defendants' domains through GoDaddy, including *peconsupport.com* and *joinmein.com* (Pecon's proprietary remote access website) and he is the registrant for some of the Corporate Defendants' domains, including *onlinepccare.com* and *pecon.co.in*. Shah also set up Google AdWord accounts to advertise for the Corporate Defendants' various "tech support" websites, such as *supportonclick.com* and *anantonline.com*.

34. The Better Business Bureau ("BBB") in California contacted Shah to suspend Pecon Software Ltd.'s BBB membership when it received complaints from consumers that the Corporate Defendants' website, *onlinepccare.com*, was responsible for scamming consumers.

35. In approximately January 2009, the Australian Communications and Media Authority ("ACMA") wrote a letter to Mahesh Kumar Shah as managing director of Supportonclick and notified him that it had received complaints regarding telemarketing calls made by the Defendants in violation of the Australian Do Not Call law. The letter says that the "significant number of complaints received against Supportonclick suggests that your business' compliance with the Do Not Call scheme is inadequate." A sample of complaints were included in the letter. Consumers complained that the company's representative told consumers their computers were infected with viruses, their computers needed repair, and they were calling from Microsoft.

The Role of Prateek Shah

36. Prateek Shah is a Director of Pecon Software Ltd. Prateek Shah is Mahesh Kumar

Shah's son. Prateek Shah attempted to open a merchant account with Bank of America in May 2012 under the d/b/a Pecon Services LLC and the Corporate Defendants' website, esolving.com. On the application, Prateek Shah listed himself as 50% owner of Pecon Services LLC and provided two phone numbers that are also listed on some of the Corporate Defendants' websites, including peconsoft.org and onlinepccare.com. In addition, Prateek Shah provided the email address sujoy@pecon.co.in and a Valley Cottage, NY address.

The Role of Sujoy Roy

37. Sujoy Roy is a Director and Chief Operating Officer of Pecon Software Ltd. Roy signs a newsletter that Pecon Software Ltd. sends out to consumers who purchased tech support from the Corporate Defendants. Roy also set up a Google AdWords account for a website called "*supportonclick.com.*" The majority of the keywords purchased for this advertising campaign had "windows" or "ms" in the keyword phrase and the campaign targeted California residents. Due to the large volume of complaints, this website, along with 18 other Corporate DefendantPecon websites, were targeted by the Metropolitan Police in London who took action and forced these websites to shut down in 2010.

The Role of Zulfiquar Ali

38. Zulfiquar Ali is the Technical Director at Pecon Software Ltd. and controls its entire IT infrastructure. Ali responded to the ACMA letter sent to Mahesh Kumar Shah regarding Do Not Call complaints for the Corporate Defendants' website, *supportonclick.com* and acknowledged in his response that the Corporate Defendants call consumers. In addition, Ali registered several of the Corporate Defendants' domains, including *anantonline.com.in* and *esolving.com*, as well as their employee website, *mis.peconsoft.com*, where trouble tickets are resolved and employees sign in on a daily basis. Ali is also the billing and technical contact for the Defendants' remote

access website, *joinmein.com*.

The Role of Vikas Kumar Gupta

39. Vikas Kumar Gupta is the Vice President of Business Development and a Customer Service Manager for Pecon Software Ltd. Gupta was listed on the California BBB's website as Customer Service Manager in 2010 and he was quoted as the spokesperson for the Corporate Defendants in the UK newspaper, The Guardian, after the UK's Metropolitan Police shut down 19 Corporate Defendant domains, including *supportonclick.com*, due to the high volume of tech scam complaints in July 2010. Gupta owns Arya Global Services, an unincorporated entity that he uses to register several other websites that operate in the same fashion as the Corporate Defendants' domains.

40. In April 2011, the ACMA sent a letter to Gupta regarding Do Not Call violations for his website, *pcserviceq.net.* In addition, *pcserviceq.net* and *onlinepccare.com* PayPal accounts were linked together and both accounts were frozen for violations of PayPal's service agreement.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

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

Count I

Deceptive Representations

43. In numerous instances, in the course of marketing, offering for sale, and selling computer security or technical support services, the Defendants represent or have represented, 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 viruses, spyware, or system errors.

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

45. Therefore, the Defendants' representations as set forth in Paragraph 43 are false, misleading, or were not substantiated at the time they were made, and thus, they constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II

Deceptive Representations

46. In numerous instances, in the course of marketing, offering for sale, and selling computer security or technical support services, the Defendants represent or have represented, expressly or by implication, through a variety of means, including telephone calls and Internet communications, that they are from, affiliated with, or calling on behalf of a well-known computer company such as Microsoft.

47. In truth and in fact, Defendants are not from, affiliated with, or calling on behalf of the well-known computer company.

48. Therefore, the Defendants' representations as set forth in Paragraph 46 are false or misleading, and thus, they 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

49. 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, in

1994. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively amended it in 2003, and amended certain provisions thereafter.

50. The Defendants are sellers or telemarketers engaged in "telemarketing" as defined by the TSR, 16 C.F.R. § 310.2(aa), (cc), and (dd).

51. The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 C.F.R. § 310.3(a)(4).

52. Under the TSR, "caller identification service" means a service that allows a subscriber to have the telephone number, and, where available, name of the calling party transmitted contemporaneously with the telephone call, and displayed on a device in or connected to the subscriber's telephone. 16 C.F.R. § 310.2(d).

53. It is an abusive telemarketing act or practice and a violation of the TSR for any seller or telemarketer to fail to transmit or cause to be transmitted the telephone number, and, when made available by the telemarketer's carrier, the name of the telemarketer, to any caller identification service in use by a recipient of a telemarketing call. 16 C.F.R. § 310.4(a)(8).

54. Among other things, amendments made to the TSR in 2003 established a do not call registry (the "National Do Not Call Registry"), maintained by the FTC, of consumers who do not wish to receive certain types of telemarketing calls. Consumers can register their telephone numbers on the National Do Not Call Registry without charge either through a toll-free telephone call or over the Internet at *donotcall.gov*.

55. Consumers who receive telemarketing calls to their registered numbers can complain of National Do Not Call Registry violations the same way they registered, through a toll-free telephone call or over the Internet at *donotcall.gov*, or by otherwise contacting law enforcement

authorities.

56. The FTC allows sellers, telemarketers, and other permitted organizations to access the National Do Not Call Registry over the Internet at *telemarketing.donotcall.gov*, to pay the fee(s) if required, and to download the numbers not to call.

57. Under the TSR, "outbound telephone call" means a telephone call initiated by a telemarketer to induce the purchase of goods or services or to solicit a charitable contribution. 16 C.F.R. § 310.2(v).

58. The TSR prohibits sellers and telemarketers from initiating an outbound telephone call to numbers on the National Do Not Call Registry. 16 C.F.R. § 310.4(b)(1)(iii)(B).

59. The TSR prohibits sellers and telemarketers from calling any telephone number within a given area code unless the seller on whose behalf the call is made has paid the annual fee for access to the telephone numbers within that area code that are included in the National Do Not Call Registry. 16 C.F.R. § 310.8.

60. 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

61. In numerous instances, in the course of telemarketing their goods and services, the 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 they have detected security or performance issues on consumers' computers, including viruses,

spyware, or system errors.

62. The Defendants' acts or practices, as described in Paragraph 61 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

Count IV

Deceptive Telemarketing Calls in Violation of the TSR

63. In numerous instances, in the course of telemarketing their goods and services, the 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 they are from, affiliated with, or calling on behalf of a well-known computer company such as Microsoft.

64. The Defendants' acts or practices, as described in Paragraph 63 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

Count V

Failing to Transmit Caller Identification

65. In numerous instances, in connection with telemarketing, defendant fails to transmit or cause to be transmitted the telephone number, and, when made available by the telemarketer's carrier, the name of the telemarketer, to any caller identification service in use by a recipient of a telemarketing call in violation of the TSR, 16 C.F.R. § 310.4(a)(8).

Count VI

Violating the National Do Not Call Registry

66. In numerous instances, in connection with telemarketing, the Defendants initiated or caused others to initiate an outbound telephone call to a person's telephone number on the National Do Not Call Registry in violation of the TSR, 16 C.F.R. § 310.4(b)(1)(iii)(B).

Count VII

Failing to Pay the National Registry Fees

67. In numerous instances, in connection with telemarketing, the Defendants have initiated, or caused others to initiate, an outbound telephone call to a telephone number within a given area code when the Defendants had not, either directly or through another person, paid the required annual fee for access to the telephone numbers within that area code that are included in the National Do Not Call Registry, in violation of the TSR, 16 C.F.R. § 310.8.

CONSUMER INJURY

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

THIS COURT'S POWER TO GRANT RELIEF

69. 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.

70. 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), authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the TSR, including the

rescission or reformation of contracts, and the refund of money.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 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 but not limited to temporary and preliminary injunctions, and an order providing for the turnover of business records, an asset freeze, and the disruption of domain and telephone services;

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

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the FTC Act and the TSR, 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 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,

WILLARD K. TOM
General Counsel

Dated: September 24, 2012

s/ Colleen Robbins

Colleen B. Robbins, SDNY Bar #CB5086
Christine M. Todaro, OH Bar #0084976
Kelly Horne, CA Bar #242675
Benjamin R. Davidson, DC Bar #975509
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2548; crobbins@ftc.gov
(202) 326-3711; ctodaro@ftc.gov
(202) 326-3031; khorne@ftc.gov
(202) 326-3055; bdavidson@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION