

Velva L. Price  
District Clerk  
Travis County  
D-1-GN-19-001015  
Victoria Benavides

D-1-GN-19-001015

CAUSE NO. \_\_\_\_\_

THE STATE OF TEXAS,  
Plaintiff,

§  
§  
§  
§  
§  
§  
§  
§  
§

IN THE DISTRICT COURT OF

v.

TRAVIS COUNTY, TEXAS

WE BRAND BETTER, LLC, LATITUDE  
SOLUTIONS & CONSULTING LLC,  
SAHIL MIGLANI, and HARNEET OBEROI,  
Defendants.

200TH  
\_\_\_\_\_ JUDICIAL DISTRICT

**PLAINTIFF'S ORIGINAL PETITION**

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff, STATE OF TEXAS, acting by and through Attorney General of Texas, KEN PAXTON, complains of Defendants WE BRAND BETTER, LLC, LATITUDE SOLUTIONS & CONSULTING LLC, SAHIL MIGLANI, individually, and HARNEET OBEROI, individually, and for causes of action would respectfully show as follows:

**I. DISCOVERY CONTROL PLAN**

1.1. The discovery in this case is intended to be conducted under Level 3 pursuant to Tex. R. Civ. P. 190.4.

1.2. This case is not subject to the restrictions of expedited discovery under Tex. R. Civ. P. 169 because the relief sought by the State includes non-monetary injunctive relief and the State's claims for monetary relief, including penalties, consumer redress, and attorneys' fees and costs, are in excess of \$1,000,000.00.

**II. PRELIMINARY STATEMENT**

2.1. Since at least early 2015, Defendants have conspired with one another and others to operate a sophisticated scheme throughout Texas and the rest of the United States to deceive and scare consumers into paying hundreds—sometimes thousands—of dollars for unnecessary

computer services.

2.2 Defendants directly impersonate or represent that they are affiliated with well-known and legitimate companies like Microsoft, Apple, and Dell in order to gain consumers' trust. Taking advantage of these companies' reputations and goodwill, Defendants convince consumers to allow them remote access to the consumers' computers. Defendants then make misleading and deceptive representations regarding normal computer status messages, convincing consumers they have been infected by a virus or have other serious problems with their computers.

2.3. Through their deceptive scheme, Defendants have collected hundreds of thousands of dollars per month from consumers, particularly elderly consumers. Defendants quickly transfer most of this money to co-conspirators in India, including Defendant Oberoi's brother-in-law.

### **III. JURISDICTION**

3.1. This action is brought by Plaintiff, Attorney General Ken Paxton, through his Consumer Protection Division, in the name of the State of Texas and in the public interest under the authority granted to him by § 17.47 of the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code § 17.41 et seq. (hereafter the "DTPA"), upon the grounds that Defendants have engaged in false, deceptive, and misleading acts and practices in the course of trade and commerce as defined in, and declared unlawful by, DTPA §§ 17.46(a)-(b). The Attorney General is further authorized to seek civil penalties, redress for consumers, and injunctive relief in enforcement suits filed under DTPA § 17.47.

### **IV. DEFENDANTS**

4.1. Defendant We Brand Better, LLC ("We Brand Better"), is a Delaware limited liability company that does business throughout the United States and in Texas, and this proceeding arises out of its business in this state. Defendant We Brand Better has also done

business as “My Tech Advise” and “My Expert Advise.” Defendant We Brand Better can be served by serving its registered agent, The Company Corporation, at 2711 Centerville Rd, Ste. 400, Wilmington, DE 19808.

4.2. Defendant Latitude Solutions & Consulting LLC (“Latitude”) is a Texas limited liability company that does business throughout the United States and in Texas, and this proceeding arises out of its business in this state. Defendant Latitude has also done business as “MTE Solutions US,” “MTE Help,” and “My PC Wizard.” Defendant Latitude can be served by serving its registered agent, The Fein Law Firm P.C., at 15455 Dallas Parkway, Ste. 1225, Addison, TX 75001.

4.3. Defendant Sahil Miglani is an individual residing in Emeryville, CA. Defendant Miglani does business throughout the United States and in Texas through We Brand Better, which he personally controls and of which he acts as the guiding spirit. Defendant Miglani can be served with process at his home at 1228 Vienna Dr., Spc. 908, Sunnyvale, CA 94089, or wherever he may be found.

4.4. Defendant Harneet Oberoi is an individual residing in Irving, TX. Defendant Oberoi does business throughout the United States and in Texas through Latitude, which he personally controls and of which he acts as a guiding spirit. Defendant Oberoi can be served with process at his home at 1416 Guthrie Ln, Allen, TX 75013, or wherever he may be found.

## **V. VENUE**

5.1. Under DTPA § 17.47(b), venue of this suit lies in Travis County, TX, because Defendants have done business in Travis County, TX.

## **VI. PUBLIC INTEREST**

6.1. Plaintiff, the State of Texas, has reason to believe that Defendants are engaging in,

have engaged in, or are about to engage in, the unlawful practices set forth below and that Defendants have caused and will cause adverse effects to legitimate business enterprises lawfully conducting trade and commerce in this state. Further, Plaintiff has reason to believe that Defendants will cause immediate and irreparable damage to the State of Texas and to persons from whom monies or properties are unlawfully acquired. The Consumer Protection Division of the Office of the Attorney General of Texas therefore believes and is of the opinion that these proceedings are in the public interest.

## **VII. TRADE AND COMMERCE**

7.1. Defendants have, at all times described below, engaged in conduct which constitutes “trade” and “commerce” as those terms are defined by § 17.45(6) of the DTPA.

## **VIII. ACTS OF AGENTS**

8.1. Whenever in this Petition it is alleged that any Defendant did any act, it is meant that such Defendant performed or participated in the act, Defendant’s officers, agents, or employees performed or participated in the act on behalf of and under the authority of the Defendant, or one of Defendant’s co-conspirators or its agents performed or participated in the act.

## **IX. NOTICE BEFORE SUIT**

9.1. The Consumer Protection Division did not contact Defendants before suit was filed to inform them in general of these unlawful allegations because there is good cause to believe and Plaintiff does believe that Defendants would seek to avoid service of process and/or destroy relevant records if such prior contact were made. For example, the Individual Defendants are both citizens of India and continue to have friends and family in India. Therefore, Plaintiff believes Defendants may seek to avoid service of process by returning to India.

9.2. Additionally, Plaintiff believes such an emergency exists that a delay in obtaining



a Temporary Restraining Order would cause an immediate and irreparable injury, loss, or damage to occur.

## **X. SPECIFIC FACTUAL ALLEGATIONS**

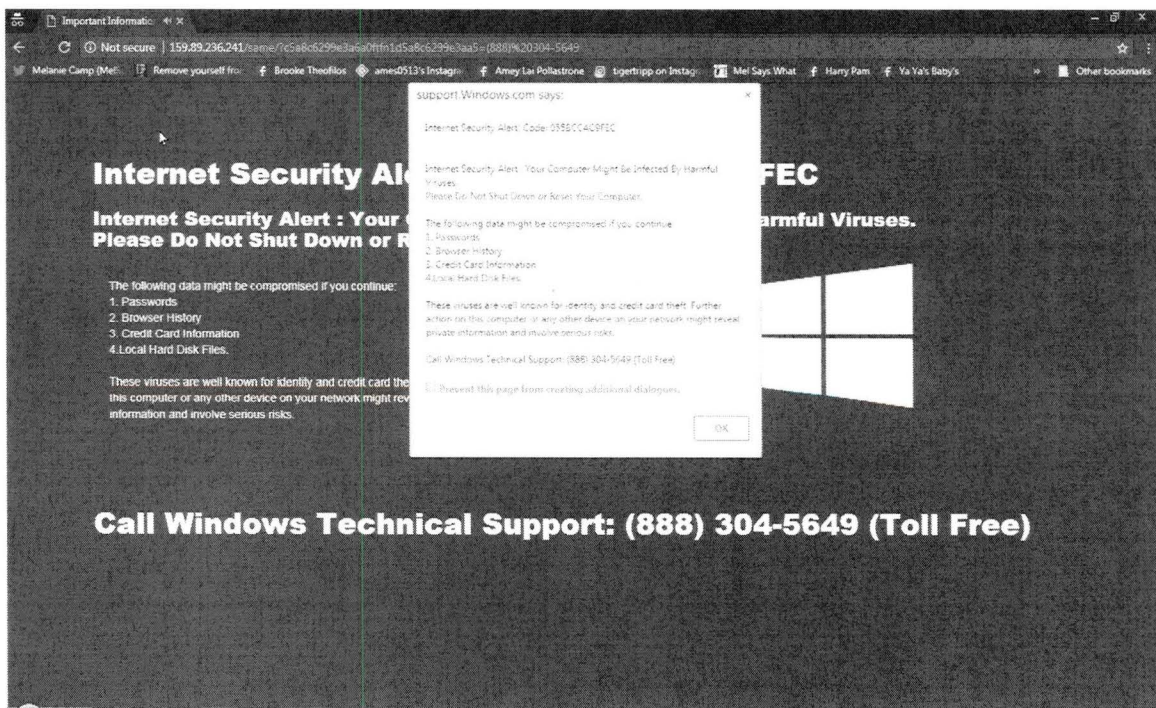
### **Overview**

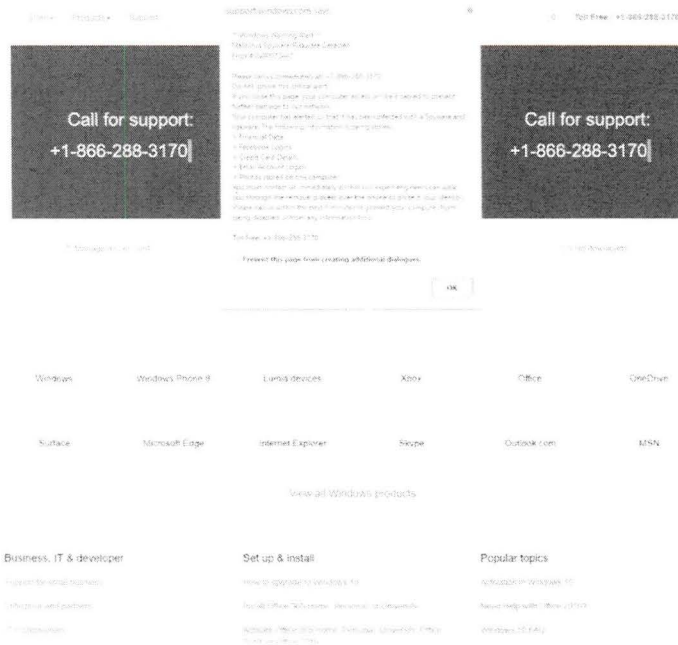
10.1. Defendants purport to provide on-demand technical support and trouble-shooting services for all PC-related issues. However, since at least 2015, Defendants have conspired with one another and other third parties to engage in deceptive scare tactics to convince vulnerable or technologically-unsophisticated consumers to pay hundreds or thousands of dollars for completely unnecessary technical support services. Defendants typically initiate contact with consumers, including consumers located in Travis County, TX, through deceptive pop-up ads that trick consumers into calling Defendants' boiler rooms. Defendants' pop-ups and oral statements misrepresent that they are affiliated with Microsoft, Apple, or other legitimate technology companies, and scare consumers with claims that consumers' computers are infected with viruses, malware, or adware, or are otherwise compromised. Defendants' deceptive scheme has caused millions of dollars in harm to consumers, many of whom are elderly, throughout the United States.

### **Initial Solicitation**

10.2. While a consumer is browsing the internet, Defendants cause a pop-up window to be displayed on the consumer's computer. Defendants' pop-up windows, which are often designed to appear to be generated by the computer's operating system or Internet browser, typically represent that some virus, malware, or other serious vulnerability has been detected on the computer. The pop-up ads also generally include references to Microsoft, Apple, or other well-known technology companies along with a toll-free number to call, leading consumers to believe they are calling the legitimate technology company. Moreover, the pop-up messages are often

difficult or impossible for consumers to close, and cause their computers to freeze or become otherwise inoperable. Defendants' pop-up windows sometimes include a loud alarm to create a further sense of emergency and danger, or include dire warnings that shutting down the computer will result in a loss of all data. Below are examples of pop-up windows like the ones Defendants cause to be displayed on consumers' computers:





### Sales Call Using High Pressure Scare Tactics

10.3. A consumer who calls a telephone number contained in one of Defendants’ pop-ups is connected to one of Defendants’ telemarketers. Defendants’ telemarketers deliver a sales pitch designed to convince the consumer that his or her computer is in urgent need of repair, even though Defendants have not detected an actual problem.

10.4. In an effort to gain the consumer’s trust, Defendants claim they are affiliated with Microsoft, Apple, Dell, or other reputable technology companies. In some cases, Defendants actually answer the phone using the legitimate company’s name. Other times, they reference the name in the course of their conversation with the consumer or respond affirmatively if asked whether they are the company. In fact, Defendants are not affiliated with or certified by Microsoft, Apple, Dell, or other reputable technology companies, and are not authorized by such companies to diagnose problems with those companies’ products.

10.5. Once Defendants have gained a consumer’s trust by misrepresenting their affiliation with legitimate companies, they seek to convince the consumer that the pop-up message

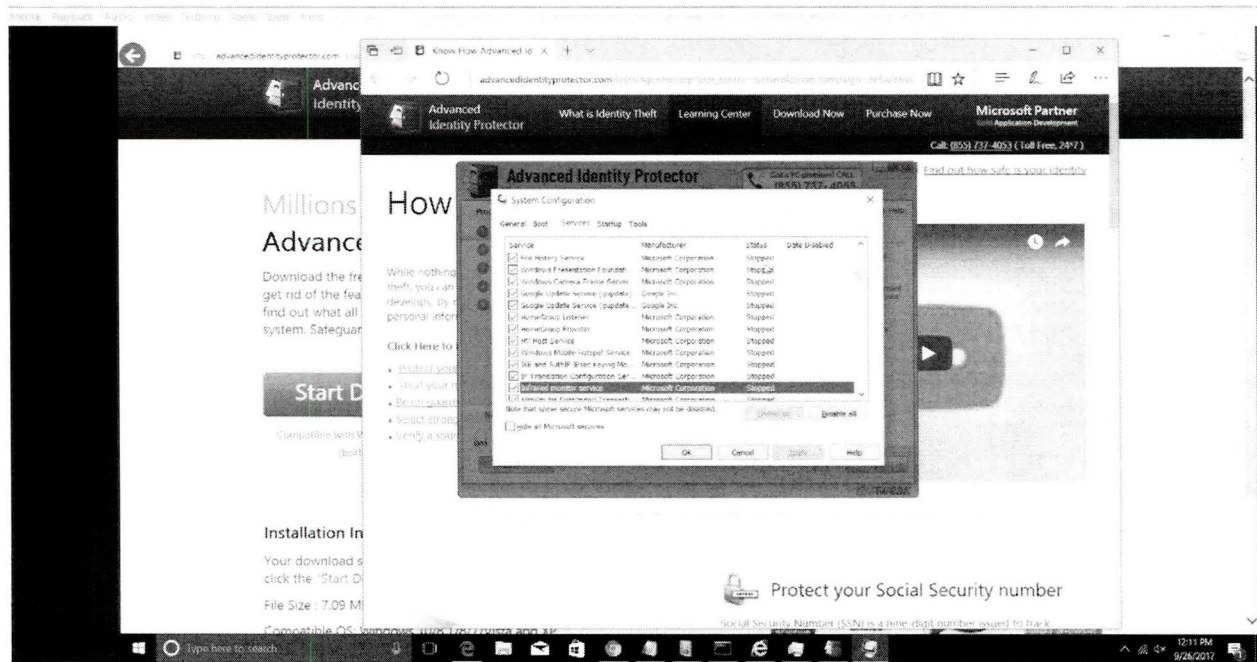
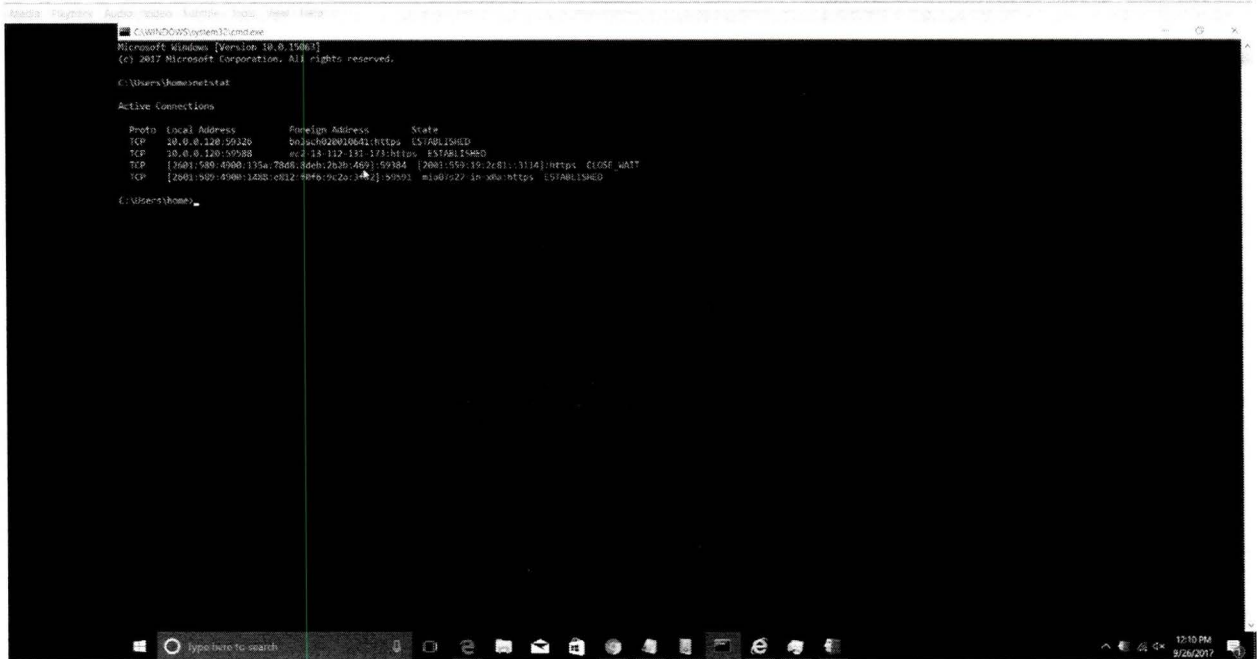


the consumer received indicates serious problems with the consumer's computer. Defendants further seek to obtain remote access to the consumer's computer, which they usually gain by directing the consumer to a website from which Defendants' telemarketers can make a remote access.

10.6. By gaining remote access, Defendants are able to control the consumer's computer. Among other things, Defendants can view the computer screen, move the cursor, enter commands, run applications, and access stored information. At the same time, the consumer can see what Defendants are seeing and doing on his/her computer.

10.7. After gaining control of the consumer's computer, Defendants represent that they are running a series of diagnostic evaluations. But the supposed "diagnostics" Defendants run are nothing more than a high-pressured, deceptive sales pitch designed to scare the consumer into believing that his or her computer is corrupted, hacked, or otherwise compromised. As part of this sales pitch, Defendants often use standard system information tools in the Windows operating system. Such tools include the System Configuration tool, the Event Viewer, or the Command Prompt, each of which displays certain innocuous information about a consumer's computer. Samples of Defendants' use of the Command Prompt and System Configuration tool are displayed below:





10.8. In some instances, after Defendants’ telemarketers have conducted some initial diagnostics, they will inform the consumer that the issue is too complicated for them and that they need to transfer the consumer to a “Level 5 Technician” or some other technician who is more qualified.

10.9. Throughout Defendants' diagnostic tests, Defendants misrepresent the technical significance of information from the tests and tools they use, and in virtually every instance, claim to have identified performance or security problems on the consumer's computer that must be resolved immediately. In many instances, Defendants claim that the consumer has been hacked and purport to show the consumer "evidence" of intruders accessing the consumer's computer.

10.10. For example, using the Command Prompt displayed above, Defendants commonly represent that the information in the column under "Foreign Address" shows the presence of hackers from foreign countries. In fact, the "netstat" command that Defendants run in the Command Prompt will *always* display a "Foreign Address," and does not indicate the presence of hackers. Similarly, Defendants will often point out that the System Configuration tool as displayed above shows numerous "stopped" services. Defendants often represent that these are security services that have been stopped and that the hackers who have connected to the consumer's computer have stopped these services. In fact, all Windows installations come with services that are, by default, stopped in order to preserve computing resources.

10.11. Once Defendants have convinced a consumer that his or her computer is compromised or in danger of being compromised, they represent that they can fix the consumer's computer and offer their services for a fee ranging anywhere between \$99.99 to over \$1,000.00.

10.12. According to Defendants' websites, Defendants typically offer different tiers of service, usually featuring one fee for a one-time fix, and then increasing amounts for varied-length service contracts, or for coverage for multiple devices. Defendants' various websites often advertise the same services with the same descriptions, but at different prices. Moreover, the prices listed on Defendants' websites seem to have little or no correlation with the prices Defendants represent to consumers on the telephone.

10.13. Defendants typically accept payments from consumers via credit card. After obtaining a consumer's payment, Defendants "work" on the consumer's computer, generally performing unnecessary "services." In many cases, Defendants do little more than remove their own advertisement that initially caused the computer to freeze. Defendants sometimes run free, typically outdated, system-cleanup system utilities. In some cases, Defendants actually leave the consumer's computer in a worse condition than it started. For example, Defendants sometimes remove or disable the consumer's existing security software, even when the consumer has paid for such software, and replace it with a free alternative downloaded from the internet or an unauthorized version of other security software.

10.14. After Defendants have completed their "work," they call the consumer back and represent that their "work" is complete. In some cases, Defendants will have the consumer electronically sign a document acknowledging that the services have been performed and the consumer is happy with Defendants' services. Defendants may also send the consumer an invoice via email detailing the "work" that has been done.

### **Revictimizing Consumers**

10.15. Defendants are not satisfied victimizing consumers once. Defendants often call consumers they have previously victimized and represent that they have detected other issues with the consumers' computers. Defendants then go through the same process of gaining remote access to the consumer's computer, running fake diagnostics, and "repairing" the new problem.

10.16. Defendants also re-victimize some consumers using a fraudulent refund scam. In those cases, Defendants call the consumer and explain that Defendants are providing the consumer a refund for some reason. Inevitably, Defendants later claim that they accidentally over-refunded the consumer by a thousand dollars or more. Defendants then ask the consumer to either wire the



difference to an individual typically residing overseas or purchase iTunes gift cards and provide the numbers off the backs of the gift cards.

### **Individual Defendants are Personally Liable**

10.17. The individual Defendants each participate in and control the day-to-day operations of, or act as the guiding spirit of, one or more of the corporate entities. As such, each individual Defendant is personally liable for Defendants' deceptive conduct. Moreover, each individual Defendant has conspired with the other individual Defendant and other third parties to accomplish the deceptive scheme.

#### *Sahil Miglani*

10.18. Defendant Sahil Miglani is the majority owner and a managing member of Defendant We Brand Better. In March 2015, Defendant Miglani applied for Defendant We Brand Better's credit card merchant account with Electronic Merchant Systems ("EMS"). Defendant Miglani is listed as the sole contact for the account, used his home address as the physical address for the company, and personally guaranteed the account. Defendant Miglani also signed an addendum to We Brand Better's merchant agreement with EMS certifying that all technical support services for which We Brand Better charges any customer would be performed by We Brand Better and would not be referred, re-directed, or outsourced to any third-party. Defendant Miglani routinely contacted EMS to update information about We Brand Better, including changing its address and phone number, and changing its DBA from mytechadvise.com to myexpertadvise.com. As the contact on We Brand Better's EMS account, Defendant Miglani received notice of every chargeback initiated in the account. Defendant Miglani also applied for and/or controlled private mailboxes and/or virtual offices for Defendant We Brand Better. Defendant Miglani also received numerous complaints describing We Brand Better's deceptive

conduct, including complaints forwarded by the Minnesota Attorney General's Office, the Pennsylvania Attorney General's Office, and the New York Department of State. Defendant Miglani also paid for toll-free numbers used by Defendants, as well as for Defendants' websites mtesolutions.us, mypcwizard.us, and myexpertadvise.com on numerous occasions.

*Harneet Oberoi*

10.19. Defendant Harneet Oberoi is the sole owner and managing member of Defendant Latitude. Defendant Oberoi, with the help of Defendant Miglani, applied for Defendant Latitude's credit card merchant account with EMS. Defendant Oberoi is listed as the sole contact for the account, used his home address as the physical address for the company, and personally guaranteed the account. Defendant Oberoi also signed an addendum to Latitude's merchant agreement with EMS certifying that all technical support services for which Latitude charges any customer would be performed by Latitude and would not be referred, re-directed, or outsourced to any third-party. As the contact on Latitude's EMS account, Defendant Oberoi received notice of every chargeback initiated in the account. Defendant Oberoi is also the sole signatory on a bank account Latitude has with Comerica Bank. Defendant Oberoi also applied for and/or controlled private mail boxes and/or virtual offices for Defendant Latitude. Defendant Oberoi is or was also the registrant of Defendants' websites mtesolutions.us and pcwizard.us, and regularly paid for the registration and hosting of the websites.

**XI. FALSE, MISLEADING, OR DECEPTIVE ACTS**

11.1. Plaintiff incorporates and adopts by reference the allegations contained in each and every preceding paragraph of this petition.

11.2. Defendants, as alleged and detailed above, have in the course of trade and commerce engaged in and conspired with one another to engage in false, misleading, and deceptive

acts and practices declared unlawful in § 17.46(a) of the DTPA, including by engaging in conduct specifically defined to be false, deceptive, or misleading by § 17.46(b) such as:

- A. Passing off services as those of another, in violation of DTPA § 17.46(b)(1);
- B. Causing confusion or misunderstanding as to the source, sponsorship, approval, or certification of services, in violation of DTPA § 17.46(b)(2);
- C. Causing confusion or misunderstanding as to affiliation, connection, or association with, or certification by, another, in violation of DTPA § 17.46(b)(3);
- D. Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he does not have, in violation of DTPA § 17.46(b)(5);
- E. Representing that services are of a particular standard, quality, or grade, if they are of another, in violation of DTPA § 17.46(b)(7);
- F. Knowingly making false or misleading statements of fact concerning the need for repair service, in violation of DTPA § 17.46(b)(13);
- G. Representing that work or services have been performed on goods when the work or services were not performed, in violation of DTPA § 17.46(b)(22);  
and
- H. Failing to disclose information concerning goods or services which was known at the time of the transaction with the intent to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed in violation of § 17.46(b)(24).



11.3. Furthermore, Defendants' practices were likely calculated to acquire or deprive money or other property from a consumer who was 65 years of age or older when the act or practice occurred.

## **XII. NECESSITY OF IMMEDIATE RELIEF**

12.1. Pursuant to Tex. Bus. & Com. Code § 17.47(d), Plaintiff requests immediate relief by way of a Temporary Restraining Order ("TRO") and Temporary Injunction, as set forth in the Prayer. Unlike a private litigant seeking a TRO under Tex. R. Civ. P. 680, Plaintiff is not required to demonstrate a likelihood of success, irreparable injury, or balancing of the equities. *State v. Texas Pet Foods*, 591 S.W.2d 800, 805 (Tex. 1979); *West v. State*, 212 S.W.3d 513, 519 (Tex. App.—Austin 2006, no pet.) ("[W]hen an applicant relies upon a statutory source for injunctive relief, such as the DTPA, the statute's express language supersedes the common law injunctive relief elements such as imminent harm or irreparable injury and lack of an adequate remedy at law."). Plaintiff is entitled to a TRO upon a showing that (i) Defendants have engaged in or are about to engage in an unlawful act or practice under the DTPA; and (ii) the proceedings are in the public interest.

12.2. Despite the numerous complaints filed against Defendants and the fact that Defendants have "F" ratings with the Better Business Bureau under several of their DBAs, Defendants continue to engage in the deceptive and fraudulent business practices described herein. Immediate injunctive relief by way of Temporary Restraining Order and Temporary Injunction is necessary to prevent continuing harm prior to final trial.

12.3. In addition to restraining Defendants' conduct to prevent future illegal acts and continuing harm to consumers, Plaintiff requests immediate relief to preserve and protect the fraudulently obtained monies that have been paid by consumers to Defendants. Defendants are

acquiring large amounts of money through their deceptive scheme, most of which is quickly transferred to foreign bank accounts, primarily in India. Defendants' assets, therefore, are subject to dissipation and secretion; these assets should be frozen pending final trial so consumer restitution can be made and full and final relief can be awarded at final trial. Tex. Bus. & Com. Code § 17.47(d).

12.4. Plaintiff further requests that a temporary restraining order be issued *without prior notice* because Plaintiff has reason to believe that Defendants will evade service of process and/or destroy, secrete, or remove evidence. Defendants Sahil Miglani and Harneet Oberoi are both citizens of India with legal status in the United States, and both Defendants still have family in India. This presents a risk that Defendants will flee in order to evade service of process and/or to destroy, secrete, or remove evidence.

### **XIII. REQUEST TO CONDUCT EXPEDITED DISCOVERY PRIOR TO TEMPORARY INJUNCTION HEARING**

13.1. Plaintiff requests leave of Court to conduct telephonic, oral, and written depositions of parties and witnesses prior to any scheduled temporary injunction hearing and Defendants' answer date. There are numerous victims and other witnesses necessary for the temporary injunction hearing that reside outside of Travis County, Texas, and the State of Texas. Any depositions, telephonic or otherwise, would be conducted with reasonable, shortened notice to Defendants and their attorneys, if known. Further, Plaintiff requests that Defendants be ordered to produce documents on a reasonable shortened notice prior to any scheduled temporary injunction hearing. Plaintiff also requests that the filing requirements for business records and the associated custodial affidavits be waived for purposes of all temporary injunction hearings.

### **XIV. DISGORGEMENT/RESCISSION**

14.1. Defendants' assets are subject to the equitable remedy of disgorgement, which is

the court-ordered relinquishment of all benefits that would be unjust for Defendants to retain, including all ill-gotten gains and benefits or profits that result from Defendants' violations of Texas law. Defendants should be ordered to disgorge all illegally obtained monies from consumers, together with all the proceeds, profits, income, interest, and accessions thereto. Such disgorgement should be for the benefit of victimized consumers and the State of Texas.

#### **XV. TRIAL BY JURY**

15.1. Plaintiff herein requests a jury trial and will tender the jury fee to the Travis County District Clerk's Office pursuant to Tex. R. Civ. P. 216 and Tex. Gov't Code § 51.604.

#### **XVI. PRAYER FOR RELIEF AND APPLICATION FOR TEMPORARY RESTRAINING ORDER AND TEMPORARY INJUNCTION**

16.1. Defendants have engaged in the unlawful acts and practices described above and will continue to violate the law as alleged in this Petition. Unless immediately restrained by the Court, Defendants will continue to violate the laws of the State of Texas and cause immediate and irreparable injury, loss, and damage to the State of Texas and to the general public.

16.2. Plaintiff therefore requests a Temporary Restraining Order, Temporary Injunction, and Permanent Injunction as indicated below. Tex. Bus. & Com. Code § 17.47(d). The Court shall issue such injunctive relief without requiring a bond. Tex. Bus. & Com. Code § 17.47(b). Pursuant to Tex. Bus. & Com. Code § 17.47(b), Plaintiff requests that a Temporary Restraining Order be issued without prior notice to Defendants as allowed by statute to prevent irreplaceable loss of funds fraudulently obtained by Defendants.

16.3. Plaintiff further prays that Defendants be cited according to law to appear and answer herein; that a TEMPORARY RESTRAINING ORDER be issued; that after due notice and hearing, a TEMPORARY INJUNCTION be issued; and that upon final hearing, a PERMANENT



INJUNCTION be issued, restraining and enjoining Defendants, Defendants' officers, agents, servants, employees, and attorneys, and any other person in active concert or participation with any or all Defendants from engaging in the following acts or practices:

- A. Transferring, concealing, destroying, or removing from the jurisdiction of this Court any books, records, documents, or other written or computer-generated materials relating to the business of Defendants currently or hereafter in Defendants' possession, custody, or control, except in response to further orders or subpoenas in this cause;
- B. Transferring, spending, hypothecating, concealing, encumbering, withdrawing, removing, or allowing the transfer, removal, or withdrawal from any financial institution or from the jurisdiction of this Court any money, stocks, bonds, assets, notes, equipment, funds, accounts receivable, policies of insurance, trust agreements, or other property, real, personal, or mixed, wherever situated, belonging to or owned by, in the possession or custody of, standing in the name of, or claimed by any of Defendants, insofar as such property relates to, arises out of, or is derived from the business operations of Defendants, without further order of this Court;
- C. Advertising, marketing, promoting, offering for sale, or selling any computer security or computer-related technical support service;
- D. Assisting others engaged in advertising, marketing, promoting, offering for sale, or selling any computer security or computer-related technical support service;
- E. Disclosing, using, or benefitting from any consumer information, including,

but not limited to, any consumer's name, address, telephone number, email address, social security number, other identifying information, or any data that enables access to an account of any person which any named Defendant obtained from the conduct described above;

- F. Passing off a Defendant's services as those of another party;
- G. Causing confusion or misunderstanding as to the approval or certification of any of Defendants' services, including, but not limited to, representing, directly or by implication, that Defendants' services are approved by, certified by, or otherwise authorized by Microsoft or any other third party;
- H. Causing confusion or misunderstanding as to any Defendant's affiliation, connection, or association with, or certification by, another, including, but not limited to, representing, directly or by implication, that any Defendant is affiliated with, certified by, or otherwise authorized by Microsoft or any other third party;
- I. Representing, directly or by implication, that any services offered or sold by any Defendant have sponsorship, approval, characteristics, ingredients, uses, or benefits which they do not have, including, but not limited to:
  - i. Representing that a Defendant has removed or will remove any virus, hacker, or other problem with a computer that does not exist or that is not removed;
  - ii. Misrepresenting the effectiveness of any software or services offered by a Defendant; or
  - iii. Representing that a Defendant's services include lifetime coverage, or

some other term of coverage, if they do not;

- J. Representing, directly or by implication, that any Defendant has a sponsorship, approval, status, affiliation, or connection which it does not have;
- K. Representing that services are of a particular standard, quality, or grade, if they are of another, including, but not limited to:
  - i. Representing, directly or by implication, that any computer command that a Defendant executes or test a Defendant runs is effective in detecting viruses, malware, hackers, or other issues with a computer if it is not; or
  - ii. Representing, directly or by implication, that any computer command that a Defendant executes is effective in remediating any viruses, malware, unauthorized access, or other issues with a computer if it is not;
- L. Making any false or misleading statements of fact concerning the need for repair service, including, but not limited to:
  - i. Representing that the presence of “foreign addresses” in the results of any “netstat” command is evidence of a virus, the presence of hackers, unauthorized access to a computer, or other problem needing to be repaired;
  - ii. Representing that the existence of stopped services in the System Configuration tool is evidence of a virus, the presence of hackers, unauthorized access to a computer, or other problem needing to be



- repaired;
- iii. Misrepresenting that an “error” or “warning” found in a user’s Event Viewer is evidence of a virus, the presence of hackers, unauthorized access to a computer, or other problem needing to be repaired;
  - iv. Representing that any Defendant has detected a virus or other problem with a person’s computer when it has not; or
  - v. Representing that a computer has a virus, has been hacked, or is otherwise in need of repairs if there is no scientifically reliable evidence to substantiate such fact;
- M. Representing, directly or by implication, that a Defendant has performed any work or service that it has not performed, including, but not limited to:
- i. Representing that a Defendant has installed a network firewall or other security tool that it has not; or
  - ii. Representing that a Defendant has removed a virus, removed malware, removed hackers, disabled foreign addresses, or taken any other steps to secure a consumer’s computer that it has not taken;
- N. Representing, directly or by implication, that a Defendant has made a refund which it has not made;
- O. Representing, directly or by implication, that a Defendant intends to make a refund that it does not intend to make;
- P. Failing to disclose information concerning goods or services which was known at the time of the transaction with the intent to induce the consumer into a transaction into which the consumer would not have entered had the

information been disclosed; and

- Q. Collecting or attempting to collect any fee or payment for a service that was marketed through any method or means that would violate this injunction.

16.4. Plaintiff further prays that the Court grant leave to Plaintiff to conduct telephonic, oral, and other depositions prior to Defendants' answer date and any temporary injunction hearing, order Defendants to produce documents on a reasonable shortened notice prior to any scheduled temporary injunction hearing, and waive the filing requirements for business records and the associated custodial affidavits for purposes of any temporary injunction hearings.

16.5. Plaintiff further prays that upon final hearing, this Court will award judgment for the Plaintiff and order Defendants:

- A. To pay civil penalties of up to \$20,000.00 per violation for each and every violation of the DTPA as authorized by Tex. Bus. & Com. Code § 17.47(c)(1);
- B. To pay an additional amount of not more than \$250,000.00 as authorized by Tex. Bus. & Com. Code § 17.47(c)(2);
- C. To restore all money or other property acquired by means of unlawful acts or practices, or, in the alternative, to compensate identifiable persons for actual damages;
- D. To disgorge all sums, monies, and value taken from consumers by means of deceptive trade practices, together with all proceeds, interest, income, profits, and accessions thereto, making such disgorgement for the benefit of victimized consumers and Plaintiff; and
- E. To pay all costs of Court, costs of investigation, and reasonable attorneys'

fees pursuant to DTPA § 17.47 and Tex. Govt. Code Ann. § 402.006(c).

16.6. Plaintiff further prays for the Court to order an equitable lien and constructive trust on all of Defendants' assets, personal property, and real property, and grant the State an interest in said assets and property.

16.7. Plaintiff further prays for post-judgment interest and any such other relief to which Plaintiff may be justly entitled.

Respectfully submitted,

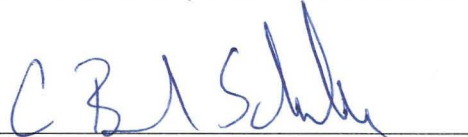
KEN PAXTON  
Attorney General of Texas

JEFFREY C. MATEER  
First Assistant Attorney General

BRANTLEY STARR  
Deputy First Assistant Attorney General

DARREN MCCARTY  
Deputy Attorney General for Civil Litigation

PAUL L. SINGER  
Division Chief, Consumer Protection Division



C. BRAD SCHUELKE  
State Bar No. 24008000  
brad.schuelke@oag.texas.gov  
LUCAS H. WOLLENZIEN  
State Bar No. 24106709  
Assistant Attorneys General  
Office of the Attorney General  
P.O. Box 12548 (MC-010)  
Austin, Texas 78711  
Telephone: (512) 463-1269  
Facsimile: (512) 473-8301

**ATTORNEYS FOR PLAINTIFF**