

STATE OF MINNESOTA
COUNTY OF HENNEPIN

DISTRICT COURT
FOURTH JUDICIAL DISTRICT

Case Type: Civil
(Consumer Protection)

State of Minnesota, by its Attorney General,
Lori Swanson,

Court File No. _____

Plaintiff,

COMPLAINT

vs.

Teknicians, Inc.,

Defendant.

The State of Minnesota by its Attorney General, Lori Swanson, ("State") for its Complaint against Teknicians, Inc. ("Defendant" or "Teknicians"), alleges as follows:

INTRODUCTION

1. Defendant Teknicians, Inc. has engaged in what is commonly referred to as a "tech support" scam, whereby it used fraudulent practices to deceive consumers into believing their computers were infected with severe viruses or malware, gain remote access to their computers, and then further mislead consumers over the telephone into making payments of hundreds of dollars for its purported and unnecessary anti-virus services and/or products.

2. In carrying out its tech support scam since at least 2014, Teknicians generally used computer pop-up windows that appeared on consumers' computer screens, which misled them into believing that their computers were infected with serious viruses or malware that could render their computers inoperable and/or compromise their data. Teknicians' pop-up window further directed consumers to call it at a specific telephone number to fix these purported problems. When a consumer called Teknicians, the company gained remote access to the

consumer's computer, misrepresented that it was performing diagnostic tests, and then further misled the consumer into believing that their computer's data and operations were severely compromised by computer viruses and malware. Sometimes Teknicians' also falsely presented itself as affiliated with hardware or software companies like Microsoft or Netgear. After making its false diagnosis, Teknicians informed consumers that they must purchase its services or products—by making an up-front payment of up to \$300 or more—to remove the dangerous virus or malware and allow the user to regain the normal use of their computer. Teknicians' practices are deceptive, fraudulent, and unlawful. As a result, the State brings this action to remedy Teknicians' unlawful conduct and enforce Minnesota's consumer protection laws.

PARTIES

3. Lori Swanson, Attorney General of the State of Minnesota, is authorized under Minnesota Statutes chapter 8; the Prevention of Consumer Fraud Act, Minnesota Statutes 325F.68-.694; the Uniform Deceptive Trade Practices Act, Minnesota Statutes section 325D.43-.48; and has common law authority, including *parens patriae* authority, to bring this action to enforce Minnesota's laws, vindicate the state's sovereign and quasi-sovereign interests, and to remediate all harm arising out of—and provide full relief for—violations of Minnesota's laws.

4. Teknicians is incorporated as a Minnesota corporation with a principal place of business located at 9120 Penn Avenue South, Suite 100-D, Bloomington, Minnesota 55431. The company's chief executive officer is Ashwani Malhotra, who resides or has resided at 6232 12th Avenue South, Richfield, Minnesota 55423.

JURISDICTION

5. This Court has jurisdiction over the subject matter of this action pursuant to Minn. Stat. § 8.01, 8.31, 8.32, 325D.45, 325F.70, and common law.

6. This Court has personal jurisdiction over Teknicians because it transacted business in Minnesota, conducted business as a Minnesota corporation, and committed acts in Minnesota causing injury to the public and in violation of Minnesota law.

VENUE

7. Venue is appropriate in Hennepin County under Minn. Stat. § 542.09 because the cause of action arose, in part, in Hennepin County, and Teknicians' principal office, primary place of business, and reported registered agent are located within Hennepin County.

FACTUAL BACKGROUND

8. In recent years, so-called "tech support" scams have become increasingly used by bad actors to target consumers. Typically, the scammer uses pop-up windows that exploit concerns about data security and malware, prompt the consumer to make telephone contact with the scammer to prevent harm to their computer and data, and then use remote-access tools that permit the scammer to gain access and control of the consumer's computer. Scammers then exploit this control over the computer and false and misleading statements to pressure consumers into paying hundreds of dollars. See Vindu Goel & Suhasini Raj, *That Virus Alert on Your Computer?*, THE NEW YORK TIMES (Nov. 28, 2018); Susan Tompor, *Beware of Tech Support Scams*, USA TODAY, May 23, 2017; Najmeh Miramirkhani et al, *Dial One for Scam: A Large-Scale Analysis of Technical Support Scams*, NDSS 2017.

9. As described below, since at least 2014, Teknicians has operated a textbook tech-support scam from Bloomington that targeted consumers across the United States, including Minnesota, by carrying out the following fraudulent tactics to charge and collect money from consumers for its unnecessary tech-support services and/or products.

I. TEKNICIANS USED DECEPTIVE POP-UP WINDOWS TO LURE CONSUMERS INTO CONTACTING THE COMPANY OVER THE TELEPHONE.

10. While consumers would browse the internet, Teknicians caused a pop-up window to display on consumers' computers. This pop-up window was designed to appear to be generated by the computer's operating system or internet browser, indicate that a virus, malware, or other serious vulnerability has been detected on the computer, and convey a sense of emergency or danger to the consumer.

11. The pop-up window also sometimes included reference to Microsoft or another well-known technology company along with a toll-free number for the user to call. As a result, Teknicians' pop-up windows sometimes led consumers to falsely believe that they were calling a well-known technology company, rather than Teknicians. Teknicians' pop-up windows were also often difficult for consumers to close and sometimes caused their computers to freeze or become otherwise inoperable.

12. In addition to pop-up messages as described above, Teknicians also made contact with consumers through its website (www.teknicians.com) or by marketing its phone number online as affiliated with companies like Microsoft, Netgear, or D-Link. Consumers would then call Teknicians' phone number when they encountered technical problems with those companies' hardware or software, believing they were calling the company or an affiliate of that company to troubleshoot or solve the problem.

13. Upon calling Teknicians, consumers were connected to a Teknicians telemarketing agent. The agent then delivered a sales pitch designed to convince the consumer that their computer was in urgent need of repair or security software or services, even though Teknicians had not actually detected any virus or malware on the consumer's computer and did

not have any knowledge of whether or not the consumer's computer required technical or security repairs.

14. In an effort to gain or maintain the user's trust, Teknicians sometimes represented to consumers over the phone that it was affiliated with Microsoft or other reputable technology companies. In fact, Teknicians is not affiliated or certified by Microsoft, Netgear, D-Link or any other reputable technology company. Teknicians is also not authorized by such companies to diagnose problems with their computer hardware or software products.

II. TEKNICIANS NEXT GAINED REMOTE ACCESS TO CONSUMERS COMPUTERS IN ORDER TO PURPORTEDLY "DIAGNOSE" THEIR COMPUTER TROUBLES.

15. After a consumer called Teknicians in response to its deceptive pop-up messages (or otherwise), a Teknicians' agent stated that the consumer would only have received the deceptive pop-up message if something were seriously wrong with their computer. In order to purportedly "diagnose" the problem with the consumer's computer, Teknicians then claimed that it needed to remotely access the consumer's computer. Sometimes, in order to pressure the consumer to grant it remote access, Teknicians represented that the consumer's computer would remain inoperable and compromised unless and until Teknicians was allowed to gain remote access to it and fix the problem.

16. Upon gaining remote access, Teknicians was able to control the user's computer, which included: viewing the consumer's computer screen; opening the computer's web camera to view the consumer or his or her surroundings; moving the cursor; entering commands; running applications; and accessing stored information. Teknicians thus potentially gained access to consumers' sensitive and personal data, as well as viewed consumers and their surroundings, through the company's fraudulent statements and practices.

17. After gaining control of the computer, Teknicians next represented that it was running a series of free diagnostic evaluations (again, sometimes purportedly on behalf of Microsoft or other company from whom the user had purchased hardware or software). Rather than run true diagnostic tests, however, Teknicians merely would display for the consumer standard background information tools for the computer, such as the “system configuration” tool, the “event viewer,” or the “command prompt.” Each of these functions merely revealed innocuous information about the normal background operations of the consumer’s computer and did not demonstrate the presence of a computer virus or infection. Nevertheless, Teknicians routinely falsely represented to consumers that such information were malicious computer viruses or infections that were the “root cause” of the problem that could render the consumers’ computer inoperable.

III. AFTER GAINING CONTROL OF THEIR COMPUTERS, TEKNIANS CHARGED AND COLLECTED UP-FRONT PAYMENTS FROM CONSUMERS FOR ITS SUPPOSED TECH-REPAIR SERVICES AND/OR PRODUCTS.

18. After Teknicians ran its deceptive “diagnostic tests” and convinced consumers that their computer was compromised or in danger of being compromised by malicious viruses or malware, Teknicians represented that they could fix the problem in exchange for an up-front payment of \$100, and that the user also needed to purchase its ongoing support services for between one and three years of service at a cost of up to \$299. During this sales pitch, Teknicians did not allow consumers to review any contract, conditions, or terms before agreeing to make the purchase. Sometimes consumers felt they had no choice but to purchase Teknicians’ services and/or products.

19. Generally, while Teknicians still had remote access (and control) over the consumer’s computer, Teknicians collected the consumer’s pertinent credit card or other

payment information and then charged or otherwise processed the up-front payment. After collecting this up-front payment, Teknicians continued to maintain their control over the consumer's computer and often took around an hour to several hours purportedly "working" on the user's computer and performing unnecessary "services" to fix the purported issue. In some cases, the company may have left the computer in a worse condition than before the pop-up appeared. Consumers have reported having to pay additional money to legitimate technical-support services to ensure the removal of all traces of and effects from Teknicians' interference with their computers' operation.

20. After the agency completed this purported "work," they would often call the user to let them know that the work was complete.

IV. REPRESENTATIVE EXAMPLES OF HOW TEKNICIANS' CARRIED OUT ITS FRAUDULENT TECH SUPPORT SCHEME.

A. The Attorney General Office's March 1, 2018 Investigatory Contact.

21. A representative example of a typical consumer experience with Teknicians was recorded¹ by the Attorney General's Office on March 1, 2018, when an investigator called the company and indicated that she was a consumer located in St. Paul, Minnesota who was directed by a pop-up window to call the company's phone number.

22. Upon being contacted, a Teknicians agent, who introduced himself as "Tom" and stated that he was "in Bloomington, Minnesota," immediately proceeded to gain remote access to the investigator's computer using the GoToAssist application. Upon gaining control over the

¹ The telephone call between an investigator with the Attorney General's Office and Teknicians was recorded. In addition, all activities (including keystrokes and screenshots) that Teknicians' made after it obtained remote access to the investigator's computer were forensically captured and preserved.

investigator's computer, Teknicians made numerous false and deceptive representations, including but not limited to:

a. The investigator stated that a pop-up window indicated that a virus was on her computer and that the issue could be repaired by calling Teknicians' phone number. Teknicians' agent responded by confirming that there was "an infection virus," that he would "clean it up," and that he "need[ed] to put a virus protection on [the] computer."

b. Teknicians' agent then claimed he was using a diagnostic tool, which he falsely stated showed "errors" and "warnings" related to the virus. In reality, the agent was merely displaying Microsoft Windows system tools that showed regular computer tasks and did not show viruses, security breaches, or corrupted files. The agent, however, stated that the system displayed "1,000" "infections" because the computer was infected by a "strong virus." When the investigator later asked about particular viruses, the agent claimed it was a "general virus" that "could make your computer crash and it is crashing your computer because the Microsoft platform which is there that is getting stopped." The agent stated that the virus "could damage [the investigator's] computer system" and "make your computer die" unless the investigator purchased necessary "virus protection."

c. When the investigator then asked the agent "what company are you with?" Teknicians' agent responded "we are working for [Microsoft] Windows." He later stated that the phone number appeared on the pop-up window because "97 percent of the software [on the computer was] from Microsoft corporation."

d. Teknicians' agent then falsely stated that the investigator did not have any "virus protection," which the agent explained was "the reason the infection was able to get inside

the computer from the internet.” The agent falsely stated that the “heart and the back bone of the computer” were “crashed because of the infection.”

e. Teknicians’ agent then said that, because he was from Microsoft, he would be able to fix the problem. He proceeded to falsely explain that he would conduct “coding” and “programming” and “install 50 drivers” to “remove the infection,” “secure your data,” and “filter your computer from errors, and warnings.” He said he would install “antivirus protection” so that she would not encounter an “infection from the virus.” He claimed she needed to pay \$50 for the “drivers” (“\$1.00 per driver”) and “antivirus protection” for \$99.99. For a one-year plan she could pay \$149.99 and for a three-year plan she would pay \$249.99.

B. The Attorney General Office’s March 9, 2018 Investigatory Contact.

23. Another representative example of a typical consumer experience with Teknicians was recorded by the Attorney General’s Office on March 9, 2018, when a different investigator called the company and indicated that she was directed by a pop-up window to call Teknicians’ phone number. A Teknicians’ agent, who introduced himself as “Bryan” and stated that he was in “Bloomington, Minnesota,” also immediately gained remote access to the investigator’s computer using the GoToAssist application. Upon gaining control over the investigator’s computer, Teknicians made numerous misrepresentations, including but not limited to:

a. When asked whether he worked for Microsoft, the Teknicians’ agent falsely stated: “That’s right, ma’am, we’re the online support for Microsoft for the kindle devices.”

b. Teknicians’ agent then claimed he was diagnosing the investigator’s computer for viruses. In reality, the agent merely ran a Microsoft DOS “tree” command, which displays the directory structure of the computer through hundreds of lines of file paths per

minute. Running this command in no way detects viruses or malware on a computer. Nevertheless, upon showing these hundreds of lines of file paths to the investigator, the Teknicians' agent stated:

We have found them. . . . This is the root cause of your problems. So this if the problem that your network signal has been damaged. There is a high possibility that your computer information can get compromised.

. . .

So these kind of malware or errors, all these things, need to be removed. These things need to get wiped off.

c. The Teknicians' agent also manually typed the message: "Network Security has been crashed! malware found!" within the Microsoft DOS "tree" command window to make it appear as though the computer had generated this message itself, when in reality, the agent manually typed this fraudulent message.

d. The Teknicians agent further misrepresented that the investigator's computer contained "infections," "that can even crash [her] computer." The agent stated that "these malware or errors" need to be removed through "advanced troubleshooting," and that Teknicians would make sure that the investigator would not "get the same problem again."

e. The agent subsequently stated that Teknicians could provide one year of "security with online support" for \$199.99 for all of the investigator's devices or three-years of "security with online support" for \$299.99, "[s]o time to time you can optimize your computer, you can clean up, everything will be included." The agent further told the investigator that "[she] cannot use [her] computer until I fix it," and then told the investigator: "[y]ou get 10 minutes to make a decision."

f. After the investigator terminated the call with the Teknicians' agent, the agent continued to stay connected to the investigator's computer. Subsequently, the agent began

examining documents on the investigator's computer by looking at the files in the computer's document folder and on the computer's desktop. Next, on two separate occasions the Teknicians agent started the web camera (which was covered) on the computer in an attempt to view the investigator. The agent also opened a document on the laptop called "Household Budget.xls," and clicked into various cells of this spreadsheet.

24. Special circumstances existed that triggered a duty on the part of Teknicians to disclose material facts to consumers about its services, products, and/or conduct. Teknicians had special knowledge—none of which consumers had at the time—that, among other things: (1) the pop-up windows that it initiated did not detect viruses or malware on consumers' computers; (2) Teknicians was not affiliated in any way with large technology companies such as Microsoft, Netgear, or D-Link; (3) Teknicians was not running actual diagnostic procedures to identify viruses and malware on consumers' computers upon obtaining remote access to their computers; and (4) Teknicians was manipulating innocuous functions on consumers' computers in order to misrepresent that their computers were infected with serious viruses and malware that required the purchase of Teknicians' services and/or products to remedy. Moreover, the nature and quality of the representations made by Teknicians were so incomplete that Teknicians did not say enough to prevent the representations it made to consumers from being deceptive and misleading.

COUNT I

THE PREVENTION OF CONSUMER FRAUD ACT, Minn. Stat. § 325F.69, et seq.

25. The State re-alleges all prior paragraphs of this Complaint.

26. Minnesota Statute section 325F.69, subdivision 1 provides:

The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the

intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoined as provided in section 325F.70.

27. The term “merchandise” within the meaning of Minn. Stat. § 325F.69 includes computer-technical and other services and products sold by Teknicians pursuant to the scheme alleged herein. *See* Minn. Stat. § 325F.68, subd. 2.

28. The term “person” includes Teknicians (as a “corporation” or “business entity”) as well as “any agent, employee, salesperson, . . . thereof.” *Id.* § 325F.68, subd. 3.

29. Teknicians has repeatedly violated Minn. Stat. § 325F.69, subd. 1 by engaging in fraud, false pretenses, false promises, misrepresentations, misleading statements and deceptive conduct described in this Complaint with the intent that others rely thereon in connection with the sale of its computer-technical services and/or products. This conduct includes, but is not limited to:

- (a) Initiating pop-up windows that falsely appeared to be generated by computer users’ operating system or internet browser and made it difficult or impossible for users to close the window,
- (b) Falsely instructing users through the pop-up window that their computer had been subject to a computer virus, malware, or otherwise compromised,
- (c) Misleading consumers as to the source of the pop-up window and representing a phone number that called Teknicians as affiliated with Microsoft or other company that sold the consumer computer hardware or software,
- (d) Misleading users to believe that they needed to call the number in the pop-up window in order to identify and expel the purported computer virus or otherwise fix or resolve a serious problem with the computer,
- (e) Engaging in other internet advertising that misled consumers into believing that the phone number used to reach Teknicians was affiliated with Microsoft, D-Link, Netgear, or other company that sells computer hardware or software to consumers,
- (f) Falsely representing to users who called the phone number that their computer was infected by a virus and in urgent need of repair,

- (g) Falsely representing to users who called the phone number that the telemarketer who answered was affiliated with Microsoft, D-Link, Netgear, or other company that sells computer hardware or software,
- (h) Using the above misrepresentations to gain permission to remotely access the user's computer, gaining access to their sensitive personal and financial information and inhibiting the user's operation of the computer,
- (i) Falsely representing that that the telemarketer was conducting sophisticated diagnostic evaluations that showed viruses, corrupted files and programs, and malware when in fact the telemarketer was showing routine actions that were incapable of detecting viruses or malware, and
- (j) Falsely representing that the user needed to pay from \$99.99 to \$299.99 for computer-technical services or software in order to expel the purported virus and resolve the problems caused to the computer by the purported virus.

30. By failing to disclose and omitting material facts which Teknicians had a duty to disclose in connection with the sale of its computer-technical services and/or products, Teknicians further engaged in deceptive and fraudulent practices in violation of Minnesota Statutes section 325F.69. These failures to disclose and material omissions include, but are not limited to:

- (a) Failing to disclose that the pop-up window was not initiated by the user's own computer software provider and was instead initiated by Teknicians,
- (b) Failing to disclose that the computer was not infected by a virus and that Teknicians did not have any knowledge as to whether the computer was actually affected by a virus,
- (c) Failing to disclose that the phone number identified in pop-up windows or internet advertising was not affiliated with Microsoft or other third-party companies that sell computer hardware or software and was in fact a number to call Teknicians, Inc., which was not affiliated those companies or approved to provide technical support services related to those companies hardware or software in any way,
- (d) Failing to disclose to users who called the phone number that their computer was not actually infected by a virus and in urgent need of repair,
- (e) Failing to disclose that the telemarketer was not conducting sophisticated diagnostic evaluations and instead, was merely displaying routine background functions of the computer that were incapable of detecting viruses and/or malware, and

- (f) Failing to disclose that the user did not need to purchase Teknicians' computer-technical services or software in order to expel a purported virus and resolve purported problems caused to the computer by the purported virus.

31. Due to the deceptive and fraudulent conduct as described in this Complaint, consumers made payments to Teknicians for computer-technical services and/or products that they otherwise would not have purchased, thereby causing harm to the consumers and enriching Teknicians.

32. Given the representations made and the circumstances described in this Complaint, Teknicians had a duty to disclose all material facts to potential customers in connection with its marketing and offering of computer-technical services and/or products to said persons.

33. Teknicians's conduct, practices, actions, and material omissions as described herein constitutes multiple, separate violations of Minn. Stat. §325F.69, subd. 1.

COUNT II
UNIFORM DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §325D.44, et seq.

34. The State re-alleges all prior paragraphs of this Complaint.

35. Minnesota Statutes section 325D.44, subdivision 1 provides, in part as follows:

A person engages in a deceptive trade practices when, in the course of business . . . , the person:

- (1) passes off goods or services as those of another,
- (2) causes likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services,
- (3) causes likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another,

. . . .

(5) represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have; [and]

....

(13) engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

36. Teknicians is a “person” within the meaning of Minnesota Statutes section 325D.44.

37. Teknicians repeatedly violated Minnesota Statutes section 325D.44, subdivision 1, by, in the course of business, engaging in deceptive and fraudulent conduct described in this Complaint, including by making false, deceptive, fraudulent, and/or misleading representations and material omissions to consumers that caused a likelihood of confusion or of misunderstanding in connection with the sale of its computer-technical services and software. Those fraudulent and deceptive practices and material omissions include but are not limited to those listed in paragraphs 29 and 30, above.

38. Due to the deceptive and fraudulent conduct described in herein, consumers made payments to Teknicians for computer-technical services and/or products that they otherwise would not have purchased, thereby causing harm to the consumers and enriching Teknicians.

39. Given the representations made and the circumstances described in this Complaint, Teknicians had a duty to disclose all material facts to consumers in connection with its marketing and offering of its computer-technical services and/or products to said persons.

40. Teknicians’ conduct, practices, actions, and material omissions as described herein constitutes multiple, separate violations of Minn. Stat. § 325D.44.

PRAYER FOR RELIEF

WHEREFORE, the State of Minnesota, by its Attorney General, Lori Swanson, respectfully asks this Court to award judgment against Defendant as follows:

1. Declaring that Teknicians' acts and material omissions as described in this Complaint constitute multiple, separate violations of Minnesota Statutes sections 325F.69, *et seq.*, and 325D.44, *et seq.*;
2. Enjoining Teknicians and its employees, officers, directors, agents, successors, assignees, affiliates, merged or acquired predecessors, parent or controlling entities, subsidiaries, and all other persons acting in concert or participation with it, from engaging in the unlawful acts and material omissions described in this Complaint or violating in any other way Minnesota Statutes sections 325F.69, *et seq.*, and 325D.44, *et seq.*;
3. Awarding judgment against Teknicians for restitution under the *parens patriae* doctrine, Minnesota Statutes section 8.31, as well as the general equitable powers of this Court and any other authority, for all persons injured by Teknicians' acts and material omissions described in this Complaint, including but not limited to ordering Teknicians and its employees, officers, directors, agents, successors, assignees, affiliates, merged or acquired predecessors, parent or controlling entities, subsidiaries, and all other persons acting in concert or participation with it to identify and refund all amounts paid by purchasers of Teknicians' services related to its false and deceptive scheme;
4. Awarding judgment against Teknicians for civil penalties pursuant to Minnesota Statutes section § 8.31, subdivision 3, for each separate violation of Minnesota Statutes sections 325F.69, *et. seq.*, and 325D.44, *et seq.*;
5. Awarding the State its costs, including costs of investigation and attorneys' fees, as authorized by Minnesota Statutes section 8.31, subdivision 3a; and
6. Granting such further relief as provided by law or as the Court deems appropriate and just.

Dated: January 3, 2019

Respectfully submitted,

LORI SWANSON
Attorney General
State of Minnesota

JAMES W. CANADAY
Deputy Attorney General

JASON PLEGGENKUHLE
Assistant Attorney General

s/ Adam Welle
ADAM WELLE
Assistant Attorney General
Atty. Reg. No. 0389951
adam.welle@ag.state.mn.us

445 Minnesota Street, Suite 1200
St. Paul, Minnesota 55101-2130
(651) 757-1425

Attorneys for the State of Minnesota

MINN. STAT. § 549.211 ACKNOWLEDGMENT

The party on whose behalf the attached document is served acknowledges through its undersigned counsel that sanctions, including reasonable attorney fees and other expenses, may be awarded to the opposite party or parties pursuant to Minnesota Statutes section 549.211.

s/ Adam Welle
ADAM WELLE