

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION**

MICROSOFT CORPORATION, a Washington corporation,)	
)	
Plaintiff,)	
v.)	
)	
SOLUTION HAT, LLC, an Indiana limited liability company, dba Think Global; and Saurabh Seth, an individual,)	
)	
Defendants.)	

Case No. 22-396

COMPLAINT

INTRODUCTION

1. Each year, hundreds of thousands of unwitting Americans fall victim to phony tech support schemes in which bad actors lure them into purchasing unnecessary “security services” for their computers by falsely claiming that the computers are infected with spyware or malware. The FBI’s 2020 Internet Crime Report lists tech support fraud among its top cybercrime trends, and the FBI’s Internet Crime Complaint Center IC3 reportedly received 15,421 complaints about tech support scams that cost victims more than \$146 million in 2020 alone.

2. To combat this fraud, Microsoft Corporation (“Microsoft”) employs sophisticated artificial intelligence and dedicated teams to identify individuals and companies engaged in fraudulent Microsoft-related tech support schemes. Microsoft then conducts test calls to further investigate companies believed to be offering phony tech support services.

3. Through these investigations, Microsoft discovered that Defendants have engaged in a pervasive and widespread tech support fraud scheme. To facilitate their scheme, Defendants

use pop up advertisements (“pop-ups”) and full-page advertisements warning computer users of dire consequences to their computer systems and directing them to “call Microsoft” at the Defendants’ toll-free number. The pop ups and advertisements prominently feature Microsoft’s well-known Windows flag logo, among other Microsoft trademarks, lending credibility to the alarming but false statements they contain. When people, who are naturally confused and concerned by the advertisements, call the number purported to be associated with Microsoft technical support, Defendants convince them to pay for computer “support services” by falsely claiming that the victims’ computers have serious security issues.

4. Microsoft brings this action to hold Defendants accountable for their actions and protect the public from the ongoing threat posed by Defendants’ fraudulent scheme.

5. Microsoft has suffered actual damages in excess of \$75,000 as a result of its investments in the investigation of this matter and bringing of this action, as well as damages to its brands and reputation.

6. This is an action for (i) deceptive telemarketing in violation of the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6102(a)(2), 6104(a); Telemarketing Sales Rule, 16 C.F.R. § 310.3(a)(2)(iii) & (vii), and 16 C.F.R. § 310.3(a)(4); (ii) false advertising in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a); (iii) trademark infringement in violation of Section 32(1) of the Lanham Act, 15 U.S.C. § 1114; (iv) false designation of origin and unfair competition in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a); (v) trademark dilution in violation of Section 43(c) of the Lanham Act, 15 U.S.C. § 1125(c); and (vi) cybersquatting in violation of Section 43(d) of the Lanham Act, 15 U.S.C. § 1125(d).

PARTIES

7. Microsoft is a Washington corporation with its principal place of business in Redmond, Washington. Microsoft develops, markets, distributes, and licenses computer software, among other products and services, and it provides technical support for that software.

8. Defendant Solution Hat, LLC (“Solution Hat”) is an Indiana limited liability company with its principal place of business in Indianapolis, Indiana. Solution Hat does business under the name Think Global. On information and belief, Solution Hat’s sole member is Defendant Saurabh Seth.

9. Defendant Saurabh Seth is an individual who, on information and belief, resides in Mount Laurel, New Jersey.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over Microsoft’s federal law claims brought under multiple sections of Title 15 of the United States Code, as set forth in the Causes of Action below. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332 because this action is between citizens of different states and the matter in controversy exceeds \$75,000 exclusive of interest and costs.

FACTS

A. The Global Reach of Technical Support Scams

11. According to a 2021 global survey, nearly seven out of ten Americans have encountered a technical support scam in the previous twelve months. Approximately ten percent of those respondents lost money from such scams.

12. In these scams, companies representing themselves to be technical service providers (hereinafter “the fake technicians”) deceive computer users into believing their personal

computers and software are infected with dangerous viruses and sell unnecessary services to purportedly “clean” the systems and software. Typically, victims of this type of scam permit the fake technicians to remotely access to their computers, and the fake technicians identify various computer files they tell victims contain dangerous malware when the files are, in fact, benign. The fake technicians’ misrepresentations that the victims’ computers have been infected with viruses mislead the victims about the quality and security of Microsoft’s computer software to convince them that they require support services.

13. One primary reason the perpetrators of technical support scams enjoy such success is that they create an impression that they represent or have an association with a well-known technology company such as Microsoft.

14. The techniques used by these companies include, but are not limited to, (a) making false representations that they are “from Microsoft” or “Windows”; (b) using Microsoft trademarks on their websites; and (c) using Microsoft’s trade name in their advertising. These misrepresentations are designed to, and in fact do, cause customers to believe that the fake technicians’ services are legitimate and offered by or affiliated with Microsoft.

15. In addition to the harm to Microsoft trademarks and Microsoft’s reputation, victims of the scheme are deceived into obtaining services they do not require and may even unwittingly expose themselves to security risks associated with the installation of malware by the fake technicians.

B. Microsoft’s Intellectual Property

16. Microsoft has duly and properly registered a number of trademarks and service marks in the United States Patent and Trademark Office on the Principal Register, including without limitation:

- (a) “MICROSOFT,” Service Mark Registration No. 1,689,468 for, *inter alia*, consulting and technical support services in the field of the design and use of computer programs, computers, computer hardware, and computers systems;
- (b) “WINDOWS,” Service Mark Registration No. 2,463,510 for, *inter alia*, computer services, namely providing technical support, information and consultation services in the fields of computer hardware, computer software and computer operating systems, all offered via computer networks and global communications networks;
- (d) “MICROSOFT CORPORATE LOGO,” Trademark and Service Mark Registration No. 4,560,827, for *inter alia*, providing technical support, consultation and resources in the fields of computer security, privacy and online safety.

(collectively, the “Microsoft Marks”).

17. True and correct copies of the Registration Certificates for the Microsoft Marks are attached hereto as Exhibits 1-3.

C. Defendants’ Technical Support Scams

18. Since its founding in the mid-1970s, Microsoft has made substantial investments in building goodwill with its billions of customers across the planet and established itself as a trusted provider of technology products and services, including software.

19. On information and belief, Defendants are engaged in a systematic and widespread technical support scam perpetrated on unwitting victims across the United States. Specifically, Defendants falsely represent themselves as Microsoft to mislead computer users into believing

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.