IfrahLaw
FTC Beat
FTC and State AG News for E-commerce

FTC Cracks Down on Bogus Virus-Removal Software

February 10, 2011

It's a gut-wrenching feeling when a computer owner realizes that his or her computer may be infected with a virus. Immediately, one's thoughts turn to the data that could be permanently lost — documents and pictures that may be difficult or impossible to replace. Next comes the realization that if the documents can be recovered (if the computer can even be saved) it will be a costly and time-consuming process to obtain and install effective virus-removal software.

Companies and individuals who took advantage of these fears recently settled with the FTC in the amount of $8.2 million. Defendant Marc D'Souza and others who did business under several names, including Innovative Marketing and ByteHosting Internet Services, used online advertisements that falsely claimed that viewers' computers were infected with viruses. The advertisements made it appear that the computer was running a scan that detected viruses, spyware, and illegal pornography on consumers' computers. The "scan" then recommended that in order to remove the malware, the consumer buy the defendant's bogus security software, which cost $39.95 or more.

According to the FTC, the defendants used an "elaborate ruse" to get Internet advertising networks and popular websites to carry their advertisements. They

falsely claimed they were placing the ads on behalf of legitimate companies and then inserted hidden programming code which delivered the fake scan instead.

As part of the settlement, D'Souza is barred from making deceptive claims in connection with computer security software, using domain names registered with false information, and misrepresenting that he is authorized to act on behalf of third parties. He is required to turn over $8.2 million in ill-gotten gains, which will be used to reimburse the estimated one million victims of the scam.

This case serves as a reminder that the FTC is likely to target sellers who blatantly cloak their advertisements in deceptive fear tactics to get sales. The more distressing the interaction is for a consumer, especially for a highly successful and lucrative campaign, the more likely the FTC is to take notice and step in.

FTC Beat is authored by the Ifrah Law Firm, a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. We look forward to hearing your thoughts and comments!