UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT PIERCE DIVISION

CASE NO.: 2:19-cv-14079

UNITED STATES OF AMERICA,

Plaintiff,

vs.

INFOTAGG TECHNOLOGY SOLUTIONS, LLC,

Defendant.
_____/

UNITED STATES OF AMERICA'S COMPLAINT FOR PRELIMINARY AND PERMANENT INJUNCTIONS

Plaintiff, the United States of America ("United States"), through its undersigned counsel, hereby sues Defendant Infotagg Technology Solutions, LLC ("Defendant") and alleges as follows:

INTRODUCTION

1. Starting as early as 2017 and continuing to the present, Defendant has used the electronic wires to further a predatory wire fraud scheme that primarily victimizes senior citizens of the United States.

2. Defendant maintains the U.S. operations of a technical-support fraud scheme based in India. That scheme operates by fraudulently inducing consumers to purchase phony or otherwise misrepresented technical-support services related to computers and to make further payments based on additional fraudulent misrepresentations.

3. The United States seeks to prevent continuing and substantial injury to consumers by bringing this action for preliminary and permanent injunctions and other equitable relief under 18 U.S.C. § 1345 to enjoin the ongoing commission of wire fraud in violation of 18 U.S.C. § 1343.

JURISDICTION AND VENUE

4. The Court has subject matter jurisdiction over this action under 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

5. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(3).

PARTIES

6. Plaintiff is the United States.

7. Defendant Infotagg Technology Solutions, LLC is a Delaware limited liability corporation with its primary address listed as 108 West 13th Street Wilmington, Delaware 19801. Defendant originally registered as a limited liability corporation in Delaware in April 2015. Defendant transacts or has transacted business in this district and throughout the United States.

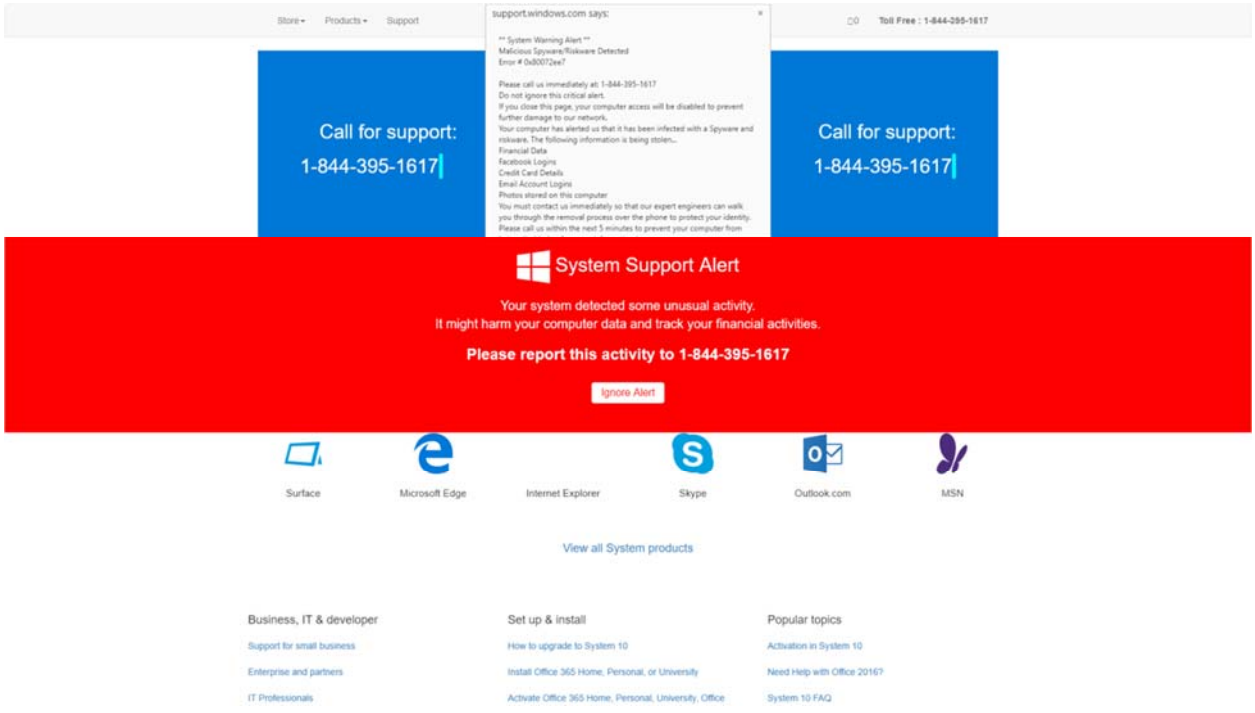
DEFENDANT'S ONGOING FRAUDULENT SCHEME

8. Since at least 2017, Defendant has conducted the U.S. operations of a large-scale technical-support fraud scheme that targets consumers throughout the United States. Defendant furthers the scheme in a number of ways, including by maintaining a website (infotagg.us), email addresses, several telephone numbers, credit card merchant accounts, and other infrastructure used in the scheme. Defendant also processes fraudulently induced consumer payments for the scheme and generally provides a veneer of domestic legitimacy.

9. As part of the scheme, telemarketers in India use telephone numbers, email addresses, and the infrastructure maintained by Defendant to contact consumers and induce them to pay money for phony technical-support services and other false purposes. Telemarketers misrepresent that they work for large, legitimate high tech companies such as Microsoft.

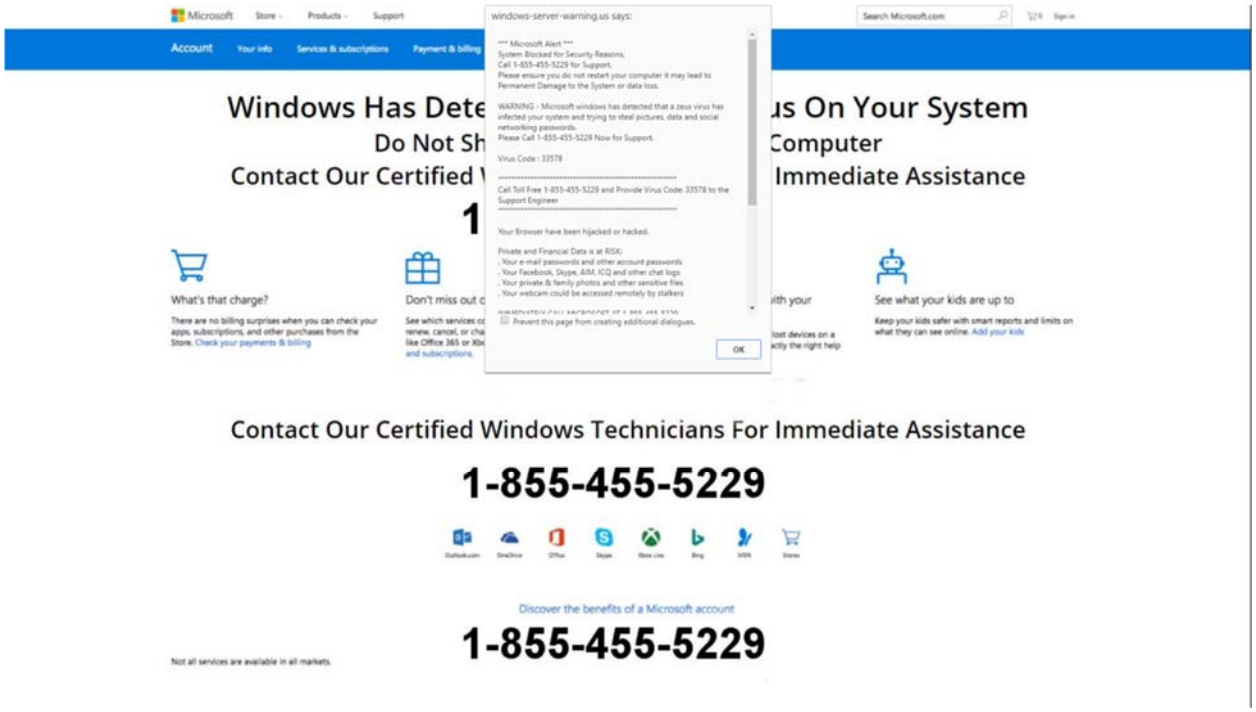
10. The telemarketers working for the scheme contact consumers either by calling them or by using pop-up computer advertisements disguised as security alerts to direct the consumers to call immediately one of Defendant's maintained telephone numbers, which the telemarketers answer. Defendant uses false and threatening Internet pop-up messages in its fraud campaign. At the government's request, the real Microsoft Corporation has provided the government with the

following images of pop-up messages with relevant phone numbers that consumers have sometimes experienced when using the Internet.[1]

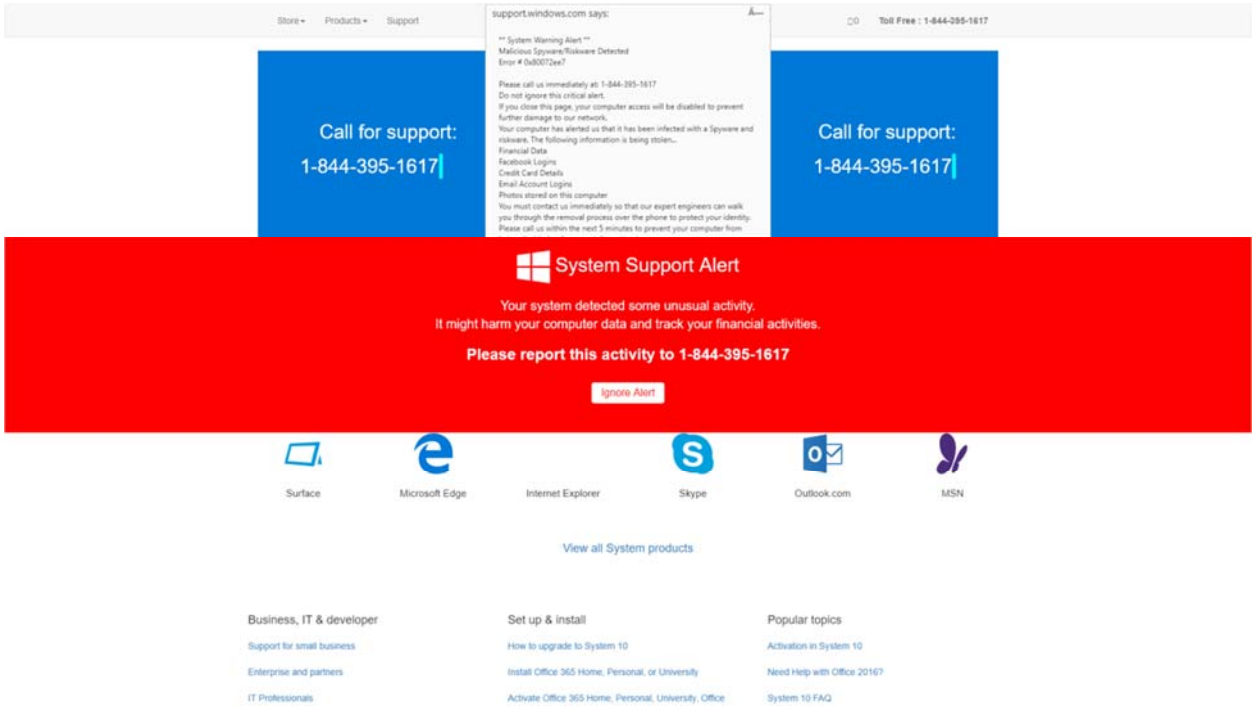


(Image 1)

[1] Microsoft has publicly described the process by which it identifies these sorts of pop-up messages. https://blogs.microsoft.com/ai/microsoft-used-ai-help-crack-tech-support-scams-worldwide/.



(Image 2)



(Image 3)

11. The pop-up messages appear to be legitimate security alerts and warn consumers to call a "Certified Windows Technician," due to the detection of a malicious virus or other issue.

Consumers who call the numbers listed in these pop-ups are misled into believing they are contacting Microsoft, but, in reality, they reach Defendant's call center.

12. Regardless of the initial method of contacting a consumer, the scheme proceeds similarly once a telemarketer working for the scheme has the consumer on the phone. Emphasizing the need for immediate action and often claiming to work for or be affiliated with well-known technology companies, the telemarketer falsely claims that the consumer's computer is at risk and that the telemarketer can assist the consumer but first needs remote access to the consumer's computer. Once remotely connected, the telemarketer purports to confirm the existence of a serious computer virus or other security threat to the consumer's computer, sometimes claiming that a hacker will soon be able to access the consumer's personal information, including financial account numbers, social security numbers, and passwords. The telemarketer imparts a sense of urgency, and then offers to install expensive and high-quality network security software to resolve the threat in exchange for a substantial sum of money.

13. After the telemarketer purports to have installed high-quality network security software, he then instructs the consumer to pay for the purported software installation by a credit card or electronic check payment to Defendant. The typical cost to consumers deceived into making payments ranges from between several hundred to thousands of dollars.

14. At times during the scheme, consumers who have already paid Defendant once for technical-support services receive additional calls from telemarketers working for the scheme. During these calls, the telemarketers concoct new phony reasons why the consumer must purchase additional security software to avoid a new, serious alleged computer virus or other threat to the consumer's computer.

15. At times during the scheme, telemarketers purport to offer refunds to consumers for sums paid to Defendant based on prior false representations about so-called "technical-support" services. Instead of refunding money to consumers, however, the telemarketers actually just move money within the consumers' online bank accounts to convince the consumers that too much money was refunded. The telemarketers then induce consumers to send payments, purportedly to reimburse Defendant for its "over-refund." Consumers have lost hundreds, and up to thousands, of dollars to this bogus refund scheme.

16. Since 2017, consumers have filed numerous complaints about Defendant on Consumer Sentinel, a consumer complaint database maintained by the Federal Trade Commission

("FTC"). At least one victim in the Southern District of Florida filed a complaint in Consumer Sentinel.

DEFENDANT'S KNOWLEDGE OF FRAUD

17. Upon information and belief, the United States alleges that Defendant has knowledge of the pervasive fraud perpetrated in its name. Consumers specifically complain about Defendant's impersonation of legitimate technology companies and their telemarketer's misrepresentations about security threats present on consumers' computers and the value of software purportedly installed.

HARM TO CONSUMERS

18. Consumers suffer financial losses from Defendant's wire fraud scheme. Those victimized by the scheme reside across the United States, including in the Southern District of Florida.

19. The scheme disproportionately affects elderly consumers. In particular, of the consumers who reported their ages in FTC Consumer Sentinel complaints about Defendant and its associated telemarketers, most of them reported that they were 60 years of age or older.

20. Defendant continues to perpetrate the technical-support fraud scheme. Absent injunctive relief by this Court, Defendant's conduct will continue to cause injury to consumers across the United States.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

21. The United States re-alleges and incorporates by reference Paragraphs 1 through 20 of this Complaint as though fully set forth herein.

22. By reason of the conduct described herein, Defendant violated, is violating, and is about to violate 18 U.S.C. § 1343 by executing a scheme and artifice to defraud for obtaining money or property by means of false or fraudulent representations with the intent to defraud, using wire communications in interstate and foreign commerce.

23. Upon a showing that Defendant is committing or about to commit wire fraud, the United States is entitled, under 18 U.S.C. § 1345, to seek a preliminary injunction and a permanent

injunction restraining all future fraudulent conduct and any other action that this Court deems just in order to prevent a continuing and substantial injury to the consumers.

24. As a result of the foregoing, the Court should enjoin Defendant's conduct under 18 U.S.C. § 1345.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff United States of America, requests of the Court the following relief:

A. That the Court issue a preliminary injunction and permanent injunction, pursuant to 18 U.S.C. § 1345, that Defendant, its agents, officers, and employees, and all other persons or entities in active concert or participation with them, are restrained from:

(1) using wire communications in interstate or foreign commerce for the purpose of executing any scheme and artifice to defraud for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;

(2) conducting or purporting to conduct any consumer technical-support services; and

B. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: March 4, 2019

Respectfully Submitted,

GUSTAV W. EYLER
Acting Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director
Consumer Protection Branch

By: DANIEL K. CRANE-HIRSCH
Daniel K. Crane-Hirsch
Trial Attorney
Consumer Protection Branch
United States Department of Justice
P.O. Box 386
Washington, DC 20044
Tel.: 202-616-8242
Email: daniel.crane-hirsch@usdoj.gov

ARIANA FAJARDO ORSHAN
UNITED STATES ATTORNEY

By: JAMES A. WEINKLE
James A. Weinkle
Assistant United States Attorney
Florida Bar No. 0710891
United States Attorney's Office
99 N.E. 4th Street, Suite 300
Miami, Florida 33132
Tel.: 305.961.9290
Email: James.Weinkle@usdoj.gov

Counsel for United States of America

Counsel for United States of America