

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION**

CASE NO.:

UNITED STATES OF AMERICA,

Plaintiff,

vs.

**MICHAEL BRIAN COTTER, individually and
d/b/a Tech Live Connect, Premium Techie Support,
Global Digital Concierge Pte. Ltd., NE Labs Inc.,
Sensei Ventures Inc., Kevisoft UK LTD, and
Kevisoft LLC;**

**GLOBAL DIGITAL CONCIERGE PTE. LTD,
also d/b/a Tech Live Connect and Saburi TLC
Worldwide Services Pvt Ltd.;**

NE LABS INC.;

SENSEI VENTURES INC.;

KEVISOFT UK LTD;

KEVISOFT LLC;

Defendants.

**UNITED STATES OF AMERICA’S COMPLAINT FOR
TEMPORARY RESTRAINING ORDER, PRELIMINARY AND PERMANENT
INJUNCTIONS**

Plaintiff, the United States of America (“United States”), through its undersigned counsel, hereby sues Defendants Michael Brian Cotter (“Cotter”), Global Digital Concierge Pte. Ltd (“Global Digital Concierge”), NE Labs Inc., Sensei Ventures Inc., Kevisoft UK LTD, and Kevisoft LLC (collectively referred to herein as “Defendants”), and alleges as follows:

INTRODUCTION

1. Starting as early as 2011 and continuing to the present, Defendants have used interstate and foreign wire communications to further a predatory wire fraud scheme that victimizes residents of the United States, including many elderly victims.

2. Defendant Cotter, along with co-conspirators located in India, operates a technical support fraud scheme utilizing call centers based in India. That scheme operates by fraudulently inducing consumers to purchase unnecessary computer technical support services based on fraudulent misrepresentations, including false statements regarding viruses and threats on consumers' computers.

3. Defendant Cotter and his co-conspirators have operated this fraudulent technical support scheme under many business names, including Tech Live Connect, Premium Techie Support, and the internet domains listed in Attachment A to this Complaint.

4. Defendant Cotter has utilized all of the corporate defendants in this case to facilitate the fraudulent scheme, including establishing bank accounts and relationships with payment processors in the names of those entities.

5. 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

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

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

PARTIES

8. Plaintiff is the United States.

9. Defendant Cotter is a resident of Los Angeles County, California, and an officer, director, or managing member of Global Digital Concierge Pte. Ltd, NE Labs Inc. and Sensei

Ventures Inc. Cotter also conducts business under the names Kevisoft UK Limited and Kevisoft LLC, which are companies registered by nominees at Cotter's direction and over which Cotter exercises operational authority and control. Acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. In connection with the matters alleged herein, Cotter transacts or has transacted business in this district and throughout the United States.

10. Defendant Global Digital Concierge is a Singapore registered company. Global Digital Concierge is a wholly owned subsidiary of Defendant NE Labs, Inc. Cotter originally registered Global Digital Concierge in 2012 under the name "Tech Live Connect Pte. Ltd." In connection with the matters alleged herein, Global Digital Concierge transacts or has transacted business in this district and throughout the United States.

11. Defendant NE Labs Inc. is a Nevada registered corporation. NE Labs Inc. is the sole shareholder of Defendant Global Digital Concierge. Cotter is identified in corporate records as the director and president of NE Labs Inc. In connection with the matters alleged herein, NE Labs Inc. transacts or has transacted business in this district and throughout the United States.

12. Defendant Sensei Ventures Inc. ("Sensei") is a Nevada registered corporation. Cotter is identified in corporate records as the president and director of Sensei. In connection with the matters alleged herein, Sensei transacts or has transacted business in this district and throughout the United States.

13. Defendant Kevisoft UK LTD is a United Kingdom registered corporation. Defendant Cotter exercises management and control over the business operations of Defendant Kevisoft UK LTD, which is registered under the names of nominee directors. In connection with

the matters alleged herein, Kevisoft UK LTD transacts or has transacted business in this district and throughout the United States.

14. Defendant Kevisoft LLC is a New York registered corporation. Defendant Cotter exercises management and control over the business operations of Defendant Kevisoft LLC, which is registered in the names of nominee directors. In connection with the matters alleged herein, Kevisoft LLC transacts or has transacted business in this district and throughout the United States.

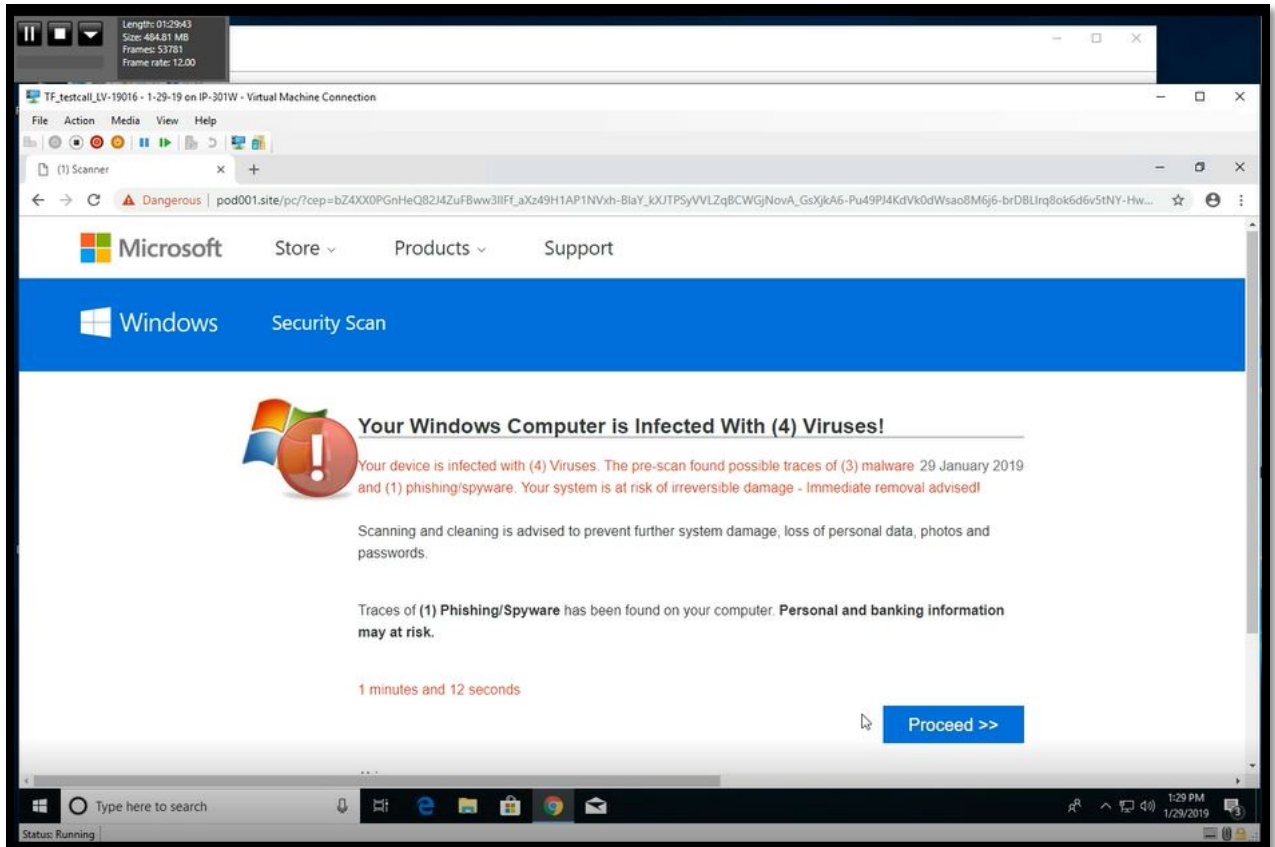
DEFENDANTS' ONGOING FRAUDULENT SCHEME

15. Since at least as early as 2011, Defendant Cotter, along with other individuals and entities located in India, has conducted a large-scale technical support fraud scheme that targets consumers throughout the United States, including in the Southern District of Florida.

16. As part of the scheme, telemarketers at call centers in India (“call center representatives”), working for Cotter and his Indian co-conspirators, utilize false claims to induce consumers in the United States to pay money for unnecessary technical support services.

17. The scheme contacts consumers by using pop-up computer advertisements disguised as security alerts. Typically, the pop-up messages claim that the consumer’s computer is infected by viruses and at risk of irreversible damage. The messages sometimes state that the computer should be scanned and/or cleaned to prevent further system damage and loss of personal information.

18. The pop-up messages are often falsely styled to appear as messages from well-known technology companies, such as Microsoft or Apple. The following is an example of a pop-up message used in the scheme:



19. The pop-up messages often contain a button – sometimes labeled “Scan Now” or “Proceed” – that purports to allow the victims to initiate the scanning and/or cleaning. After victims click the button, they receive additional notifications falsely claiming that multiple viruses were found on their computer and instructing the victims to download software to rectify the problem. At some point, either a pop-up message or a downloaded software package provides a toll-free phone number the consumer can call to contact a live agent to fix the purported problems. That phone number connects the consumer with one of the scheme’s call centers in India.

20. Upon receiving a consumer’s call to a provided toll-free number, a representative at a call center in India requests permission to access the consumer’s computer remotely to diagnose the purported problems with that computer. The call center representative sometimes

poses as a representative of or as affiliated with a technology company such as Microsoft or Apple, among others. Once remotely connected, the call center representative falsely confirms the existence of a serious computer virus or other security threat to the consumer's computer. The call center representative also falsely emphasizes the need for immediate action to repair the computer to prevent harm from online threats or loss of private information. The call center representative then offers to solve the problems if the consumer agrees to purchase security software and/or a support plan costing hundreds of dollars.

21. At times, the call center representative falsely tells the consumer that normal computer functions are in fact evidence of viruses or security threats in order to induce the consumer to make payments.

22. At times, malware from websites controlled by the call center representative is downloaded onto the consumer's computer to create an illusion that the computer contains viruses or security threats, and the call center representative warns the consumer of the malware's presence in an attempt to induce the consumer to pay for unnecessary software or technical support services.

23. To collect payments, the call center representative who is remotely connected to a consumer's computer directs the consumer to one of Defendants' websites to make payments via credit card. Defendants and their co-conspirators have created and utilize multiple websites to facilitate the technical support fraud scheme, including techliveconnect.com, premiumtechiesupport.com, saburitlc.com, and other website domains listed on Attachment A to this Complaint. These websites contain means for consumers to contact the scheme, including toll-free phone numbers, email addresses, and web forms, and some function as payments portals through which consumers make payments.

24. At times during the scheme, consumers who have already paid Defendants once for technical support services have received follow-up phone calls from call center representatives working for the scheme. During these follow-up calls, the call center representatives 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.

25. Since 2011, consumers have filed over 500 complaints on Consumer Sentinel, a consumer complaint database maintained by the Federal Trade Commission ("FTC"), that reference Tech Live Connect, Premium Techie Support, softwaretruehelp.com, softwarehelponline.com, assistmysoftware.com, techforsoftware.com, softwarebesthelp.com, softwarehotshot.com, or helpmysoftware.com.

DEFENDANTS' ROLE AND KNOWLEDGE OF FRAUD

26. Since at least as early as 2011, Defendant Cotter has operated this scheme, along with other individuals and entities located in India, under multiple business names. Cotter jointly operates the computer technical support scheme with a company registered in India, Saburi TLC Worldwide Services Pvt Ltd. ("Saburi TLC"), and its former and current directors. Cotter and his co-conspirators have operated the scheme under the names Tech Live Connect, Premium Techie Support, Saburi TLC and the domains listed in Attachment A.

27. All of the domains listed in Attachment A were registered either by Cotter himself or by a co-conspirator in India. The contents and format of all of the websites are similar. All of the websites offer technical support services and provide ways for consumers to contact the scheme. Many of the websites are designed to serve as payment portals where consumers can enter credit card information to purchase technical support services or software.

28. In 2018, Cotter directed the incorporation of New York registered company Kevisoft LLC and United Kingdom registered company Kevisoft UK Ltd. as part of the scheme, for purposes of establishing bank accounts and relationships with financial institutions to facilitate the collection of payments for technical support services. While both companies are registered in the names of nominee directors, Cotter exercises ultimate authority and control over both entities.

29. Cotter has also procured the services of critical infrastructure to support the operation of the scheme, including credit card merchant accounts and the services of payment processors, to facilitate the processing of credit card purchases by consumers. In this role, Cotter has been notified multiple times by multiple different payment processors that accounts associated with his technical support operation had high levels of chargebacks, which is an indicator of fraud under industry standards. Chargebacks refer to the reversal of the dollar value (in whole or in part) of a transaction, typically because a consumer has requested that their financial institution cancel or reverse the transaction. At least one payment processor terminated an account controlled by Cotter in connection with the technical support fraud scheme due to high rates of chargebacks.

30. In 2020, Cotter has managed credit card merchant accounts and relationships with payment processors in support of the scheme, doing business under the names Sensei Ventures Inc., Kevisoft UK Ltd, and Global Digital Concierge.

31. Cotter has also reviewed and responded to consumer complaints relating to Tech Live Connect and Premium Techie Support made to the Better Business Bureau. These complaints have included descriptions of the use of pop-up messages to contact consumers and

impersonation of well-known tech companies. For example, in June 2017 a consumer filed the following complaint regarding Tech Live Connect with the Better Business Bureau:

After downloading a file from the website www.solvusoft.com, I was redirected to a page claiming that there were multiple viruses detected on my computer. There was a phone number for “Apple Protection Plan,” which I called. I was redirected to Tech Live Connect. They convinced me that I needed their services to fix my computer, and got me to pay \$250 for “lifetime service.” They promised to fix my problems. I remotely gave them access to my computer, and they installed several “Malware cleaners,” which my antivirus later picked up as Adware. Specifically, they installed Advanced Mac Cleaner and Mac Adware Cleaner. Neither of these programs solved my problems at all, so I requested my money back. On their website, at <http://www.techliveconnect.com/en-us/index.php#our-guarantee>, they claim a money back guarantee if the customer is unsatisfied with the service. However, they have refused multiple times to refund my money, and instead keep insisting that they need to get back into my computer to fix the problem. I had to cancel my credit card, because I then found out that they wanted to charge me an additional \$38 fee for some software as well as \$9.99 a month for continued service. This is obviously a scam company. Thank you for your time.

Cotter responded to this complaint on behalf of Tech Live Connect and promised the customer a refund.

32. Cotter has had significant involvement in coordinating the scheme’s call center operations. In an email to the Better Business Bureau regarding Premium Techie Support, Cotter stated, “[M]y business owns the center that operates that brand, which is in India.” Cotter has also emailed with employees of Saburi TLC regarding the operation of the call center.

33. Defendants have knowledge of the fraudulent misrepresentations through which the scheme induces victims to purchase unnecessary computer technical support services, including misrepresentations contained in pop-up messages and misrepresentations made over the phone by call center representatives. Defendants are aware of complaints made by consumers to the Better Business Bureau, in which those consumers specifically complain about

pop-up messages referencing computer viruses and misrepresentations made by call center representatives acting on Defendants' behalf regarding threats present on consumers' computers.

HARM TO CONSUMERS

34. Consumers suffer financial losses from the wire fraud scheme perpetrated and facilitated by the Defendants. Those victimized by the scheme reside across the United States, including in the Southern District of Florida.

35. The scheme disproportionately affects elderly consumers. In particular, the majority of the consumers who reported their ages in FTC Consumer Sentinel complaints about Tech Live Connect and Premium Techie Support were 60 years of age or older.

36. On information and belief, Defendants are continuing to facilitate the technical support fraud scheme and are likely to continue facilitating 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
(U.S.C. § 1345 – Injunctive Relief)

37. The United States re-alleges and incorporates by reference Paragraphs 1 through 36 of this Complaint as though fully set forth herein.

38. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. § 1343 by devising and executing a scheme and artifice to defraud and for obtaining money or property by means of false or fraudulent pretenses, representations, and promises with the intent to defraud, and, in so doing, use interstate and foreign wire communications.

39. Upon a showing that Defendants are committing or are about to commit wire fraud, the United States is entitled, under 18 U.S.C. § 1345, to 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 consumers.

40. 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 temporary restraining order, pursuant to 18 U.S.C. § 1345, ordering that Defendants, their agents, officers, and employees, and all other persons or entities in active concert or participation with them, are restrained from:

- (1) committing wire fraud;
- (2) maintaining or doing business through the use of www.techliveconnect.com, www.premiumtechiesupport.com, www.saburitle.com, and the other domains listed in Attachment A;
- (3) impersonating any other technology company;
- (4) engaging in telemarketing activity related to the sale of any technical support service or software;
- (5) accepting consumer payments related to any purported technical support service or software; and
- (6) destroying records of any nature related to Defendant's business, financial, or accounting operations.

B. That the Court issue an order requiring the registry, Verisign, Inc., and the registrar, GoDaddy Inc., for the domains listed in Attachment A to take all necessary steps to prevent further use of the websites in Defendant's fraudulent scheme.

C. That the Court issue a preliminary injunction on the same basis and to the same effect.

D. That the Court issue a permanent injunction on the same basis and to the same effect.

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

Dated: October 14, 2020

JEFFREY BOSSERT CLARK
Acting Assistant Attorney General
Civil Division
United States Department of Justice

DANIEL J. FEITH
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JOHN W. BURKE
Assistant Director

Ann Entwistle
Trial Attorney
Consumer Protection Branch
United States Department of Justice
P.O. Box 386
Washington, DC 20044

Tel.: 202-305-3630

Email: aentwist@civ.usdoj.gov

Counsel for United States of America

Respectfully Submitted,

ARIANA FAJARDO ORSHAN
UNITED STATES ATTORNEY

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

Attachment A

to United States' Complaint for
Temporary Restraining Order
and Preliminary and
Permanent Injunctions

Attachment A

Internet Domains by Which Defendants are Doing Business

premiumtechiesupport.com
techliveconnect.com
saburitlc.com
assistmysoftware.com
gdconciierge.com
globaldigitalconciierge.com
helpforsoftware.com
helpmysoftware.com
myservicepeople.com
mysupportpeople.com
pcsupportninja.com
senseiware.com
softwarebesthelp.com
softwarehelponline.com
softwarehotshot.com
softwaremerchanthelp.com
softwaresellerhelp.com
softwaretruehelp.com
supportforsoftware.com