

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ JAN 28 2020 ★

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

BROOKLYN OFFICE

UNITED STATES OF AMERICA,

Plaintiff,

v.

JON KAHEN, a/k/a JON KAEN, GLOBAL
VOICECOM, INC., GLOBAL
TELECOMMUNICATION SERVICES INC., and
KAT TELECOM, INC.,

Defendants.

COMPLAINT

Civil Action No.

CV 20 - 00474

COGAN, J.

Plaintiff, the UNITED STATES OF AMERICA, by and through the undersigned attorneys,
hereby alleges as follows:

INTRODUCTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.

2. Since at least 2017 and continuing through the present, Defendant John Kahen, a/k/a Jon Kaen ("Kaen"), together with one or more co-conspirators, has used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims. Kaen controls various corporate entities that he utilizes in furtherance of the fraudulent scheme, including Defendants Global Voicecom, Inc.; Global

Telecommunications Services Inc.; and KAT Telecom, Inc. (the “Corporate Defendants,” and together with Kaen, the “Defendants”). The Corporate Defendants, based in New York, are VoIP¹ carriers that serve as “gateway carriers”² facilitate the delivery of millions of fraudulent “robocalls”³ every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2) paying money to the perpetrators of the schemes.

3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by “spoofing”⁴ legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient’s social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient’s assets are being frozen; the recipient’s bank and credit accounts have suspect activity; the recipient’s

¹ VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

² As set forth in further detail herein, “gateway” carriers are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to recipients in the United States.

³ “Robocall” means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.

⁴ The practice of making a false number appear on the recipient’s caller ID is known as “spoofing.”

benefits are being stopped; the recipient faces imminent deportation; or combinations of these things—all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to “resolve” these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the individual’s assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.

4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return-calling services to the fraudsters used to establish contact with potential victims. Robocall messages will often provide domestic and toll-free call-back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to extort and defraud the potential victims.

5. The Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. In addition, on at least one occasion Defendants received a direct payment from a victim of one of the fraudulent schemes.

6. Since 2017 and continuing through the present, as a result of their conduct, Defendants and their co-conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.

7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants’ ongoing scheme to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.⁵

⁵ This case is one of two cases being filed simultaneously in which the United States Department of Justice, for the first time, seeks to enjoin telecommunications companies from participating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.

JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

9. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2).

PARTIES

10. Plaintiff is the United States of America.

11. Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of the Defendants also conducts business as “IP Dish.”

12. Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom’s principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen as the corporation’s Chief Executive Officer.

13. Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service’s principal place of business is located in Great Neck, New York, in the Eastern District of New York.

14. Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom’s principal place of business is located in Great Neck, New York, within the Eastern District of New York.

OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

A. Robocalling Fraud Targeting Individuals in the United States

15. The robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system every day with millions of robocalls intended to defraud individuals in the United States. Many of these fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

16. Foreign fraudsters operate many different schemes targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

- a. *Social Security Administration ("SSA") Imposters*: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the individual's Social Security benefits will be suspended, the individual has failed to appear before a grand jury and face imminent arrest, or the individual's social security number will be terminated. When a call recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the individual's funds purportedly will be returned.

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.