

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.

NICHOLAS PALUMBO, NATASHA
PALUMBO, ECOMMERCE NATIONAL, LLC
d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a
sipretail.com,

Defendants.

COMPLAINT

Civil Action No.

CV 20-473

KORMAN, J.

MANN, M.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 2016 and continuing through the present, Defendants, together with one or more co-conspirators, have 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.

Defendants are VoIP¹ carriers, and their principals, that serve as “gateway carriers,”² facilitating 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 benefits are being stopped; the recipient faces imminent deportation; or combinations

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 greater 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.”

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 the fraudsters use 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. Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. Often, these payments consist of victim proceeds, a portion of which is deposited directly into Defendants’ accounts in the United States, before the remainder is transmitted to the fraudsters overseas.

6. Since at least 2016 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 schemes 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. Defendants Nicholas and Natasha Palumbo own and control Ecommerce National, LLC, doing business as TollFreeDeals.com and SIP Retail, LLC, also doing business as SipRetail.com (the “Corporate Defendants”), which the Palumbos utilize in furtherance of the fraudulent robocall schemes. The Palumbos operate the Corporate Defendants from their home in Paradise Valley, Arizona, and on information and belief, the Palumbos operate SIP Retail as an alter ego of Ecommerce. From their home in Paradise Valley, Arizona, the Palumbos operate the Corporate Defendants as fraudulent enterprises.

12. Defendant Ecommerce is a corporation organized and existing under the laws of the State of Arizona. Ecommerce does business as TollFreeDeals.com, and will be referred to throughout this Complaint as TollFreeDeals. TollFreeDeals’ principal place of business is located at the Palumbos’ home in Paradise Valley, Arizona. Nicholas Palumbo is the Chief Executive Officer of TollFreeDeals and Natasha Palumbo is the Vice President of Business Development.

13. Defendant SIP Retail, LLC, also doing business as SipRetail.com (“SIP Retail”), is a corporation organized and existing under the laws of the State of Arizona. SIP Retail’s principal place of business is located at the Palumbos’ home in Paradise Valley, Arizona. Natasha Palumbo is the Chief Executive Officer of SIP Retail. SIP Retail provides VoIP carrier services for some of the same customers as TollFreeDeals, including foreign VoIP carriers that

transmit millions of calls every week destined for the phones of residents of the Eastern District of New York.

OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

A. Robocalling Fraud Targeting Individual in the United States

14. 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 daily 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.

15. Foreign fraudsters operate many different scams 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 recipient's Social Security benefits will be suspended, the recipient has failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be

terminated. When a 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 funds purportedly will be returned.

- b. Internal Revenue Service ("IRS") Imposters: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, has avoided attempts to enforce criminal laws, has avoided court appearances, or the recipient faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically directs the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.
- c. United States Citizenship and Immigration Services ("USCIS") Imposters: Defendants transmit recorded messages in which USCIS imposters falsely claim that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or deportation, the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.
- d. Tech Support Imposters: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech

companies such as Apple or Microsoft, and falsely claim that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

- e. Loan Approval Scams: Defendants transmit recorded messages in which fraudsters operating loan approval scams impersonate a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a customer connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is pay a one-time fee up front.

16. These robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, local police departments, 911, or the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the caller's identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

17. Individuals who answer or return these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal

information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

18. Since October 2018, the most prolific robocalling scam impersonating U.S. government officials—and one engaged in by Defendants—is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-XXX-XXXX I repeat 619-XXX-XXXX thank you.

19. SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed \$14 million. Similarly, the Federal Trade Commission ("FTC") reported that during 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposters, with estimated victim losses of approximately \$11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately

166,000 with associated losses of more than \$37 million.⁶ Complaint numbers substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

B. How Calls From Foreign Fraudsters Reach U.S. Telephones

20. The Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoIP and related technology to create the calls. VoIP calls use a broadband Internet connection – as opposed to an analog phone line – to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S. based telecommunications companies – referred to as “gateway carriers” – to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoIP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoIP calls will pass through a series of U.S.-based VoIP carriers before reaching a consumer-facing “common carrier” such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

21. Each provider in the chain that transmits a VoIP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source

⁶ Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting \$128,479,054 in losses for 2018, and 389,563 complaints reflecting \$152,946,623 in losses for 2019.

number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as “least-cost routing.” Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this process as “traceback.”

22. Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

DEFENDANTS’ ONGOING PARTICIPATION IN ROBOCALLING FRAUD SCHEMES

23. Since at least 2016, and continuing through the present, Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. phone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

24. There is substantial evidence of the Defendants’ knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-

duration, unanswered calls⁷ passing through their systems by the millions; thousands of spoofed calls originating from overseas, purporting to be from “911” and similar numbers; dozens of complaints and warnings from other telecommunications companies about fraud, spoofing, and short-duration “junk” calls; repeated warnings and inquiries from a telecommunications industry trade group about the fraudulent robocalls passing through the Defendants’ system; and receipt of payment from their foreign customers in the form of large, suspicious cash deposits by various individuals throughout the United States directly into Defendants’ bank accounts.

A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

25. Defendants provide inbound VoIP calling to the United States telecommunication system (referred to in the industry as “U.S. call termination”) to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP calling, meaning they do not monitor or restrict the inbound calls a customer can place for either volume of calls or call duration. Defendants are paid for each call they pass into and through the U.S. phone system.

26. Defendants specifically market their services to foreign call centers and foreign VoIP carriers looking to transmit high volumes of robocalls to individuals in the United States. The TollFreeDeals website states “TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!”

⁷ Short-duration and unanswered calls include calls where recipients immediately hang up and calls that do not connect, because robocalls are sent to numerous telephone numbers that are not in service.

27. The FAQs on the TollFreeDeals website state, “Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center VoIP termination minutes. If you are looking for USA Dialer, Canada Dialer, or Australia Dialer please fill out our online interop form to test our routes.”

28. Defendants regularly transmit massive volumes of short duration calls. For example, over 23 days in May and June of 2019, TollFreeDeals transmitted more than 720 *million* calls. Of those calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. More than 24 million of those calls were placed to phone numbers with area codes in the Eastern District of New York. As Defendants’ phone records show the ultimate destination number of every VoIP call they transmit, Defendants know they transmit fraudulent calls to potential victims in the Eastern District of New York.

29. During May and June of 2019, the Palumbos facilitated the delivery of more than 182 million calls through TollFreeDeals from a single India-based VoIP carrier co-conspirator to phones in the United States. One thousand different source numbers (the number from which a call is placed, and that shows up on the recipient’s caller ID) accounted for more than 90% of those calls. According to data obtained from a robocall blocking company about calls identified as fraudulent robocalls in 2019, 79% of those 1000 source numbers have been identified as sending fraudulent robocalls. Consequently, TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of that single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan

approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.

30. Defendants' knowledge of the fraudulent nature of the telephone calls they deliver to potential victims on behalf of their co-conspirators is also evidenced by the numerous complaints, inquiries, and warnings regarding fraudulent robocalls that Defendants received from other telecommunications carriers and a telecommunications industry trade association since at least 2017. Despite receiving these complaints, inquiries, and warnings, Defendants nevertheless continued to transmit massive volumes of fraudulent robocalls from their co-conspirators to potential victims in the United States.

31. For example, in May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by its customers that spoofed phone numbers belonging to USCIS and the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not use any of the phone numbers at issue as a legitimate outbound caller ID. Nicholas Palumbo responded that the calls were transmitted to TollFreeDeals from an India-based VoIP carrier, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number as the caller ID number for their fraud calls.

32. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls were transmitted to TollFreeDeals from the same India-based VoIP carrier that had

transmitted spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this foreign VoIP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

33. The Palumbos have also received numerous warnings from telecommunications industry trade association USTelecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

34. From May 2019 through January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced USCIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone. In every case, either the email itself or the traceback portal included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign, such as:

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million

per day. Because Caller-ID changes with each call, blocking the ANI [“Automatic Number Identification”⁸] is not effective.

35. After receiving each of these notifications from USTelecom, Nicholas Palumbo logged into the USTelecom portal and provided information regarding the customers of TollFreeDeals that had transmitted the fraudulent calls. Many of these fraudulent calls repeatedly traced back to the same India-based customers of TollFreeDeals.

36. From August 2019 through January 2020, USTelecom also notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, three tracebacks of Tech Support impersonation fraud calls, and one traceback of USCIS Impersonation fraud calls. Those notifications were emailed to help@sipretail.com. Upon information and belief, the Palumbos are the only individuals who monitor email traffic to @sipretail.com domain email addresses. SIP Retail logged into the USTelecom traceback portal and notified USTelecom that all 10 of the SSA impersonation calls were sent to SIP Retail by two India-based companies. Both of these companies were also sending fraudulent SSA imposter call traffic through TollFreeDeals.com, as the Palumbos have been notified by USTelecom on multiple occasions.

37. Further, Defendants regularly receive payment from their customers in the form of substantial cash deposits directly into Ecommerce’s bank account, from locations throughout the United States raising red flags about the nature of the business of Defendants’ customers.

B. Defendants Provide Toll-Free Services for Robocall Schemes

38. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that

⁸ ANI refers to the origination telephone number from which a call is placed.

potential victims can call them back. These toll-free telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

39. While toll-free numbers used for return-calling purposes cannot be “spoofed” like outgoing robocalls, the use of a U.S. toll-free number in Defendants’ robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims’ return calls from the United States to the foreign fraudsters’ call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

40. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission (“FCC”) as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers “Responsible Organizations,” that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more Responsible Organizations.

41. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

We received a call yesterday (at 6 pm) that we didn't answer.
Calling Number: +844[XXXXXXX]
Requesting to call back: 844-[XXX]-[XXXX]

Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

The attached audio file of a voicemail message stated:

tomorrow \$399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

42. Over the course of the next two weeks, employees of the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded simply that he had let the customer of TollFreeDeals know.

43. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

Good afternoon Nick,

I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

Nicholas Palumbo responded “I let him know,” then responded further, “I will be porting clients over[.] Can’t take that chance.” In the telecommunications industry, to “port a number” means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers.

HARM TO VICTIMS

44. Defendants’ fraudulent schemes have caused substantial harm to numerous victims throughout the United States, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

45. In addition to the massive cumulative effect of these fraud schemes on victims throughout the United States, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

46. Defendants’ fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims’ losses will continue to mount.

COUNT I

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

47. The United States realleges and incorporates by reference paragraphs 1 through 46 of this Complaint as though fully set forth herein.

48. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by executing or conspiring to execute schemes or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud, and in so doing, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such schemes or artifices.

49. Upon a showing that Defendants are committing or about to commit wire fraud, conspiracy to commit wire fraud, or both, the United States is entitled, under 18 U.S.C. § 1345, to a temporary restraining order, 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 victims of fraud.

50. As a result of the foregoing, Defendants' conduct should be enjoined pursuant to 18 U.S.C. § 1345.

PRAYER FOR RELIEF

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

- A. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination on the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them are temporarily restrained from:

- i. committing and conspiring to commit wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349;
 - ii. providing, or causing others to provide call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;
 - iii. providing toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities;
 - iv. destroying, deleting, removing, or transferring any and all business, financial, accounting, call detail, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants.
- B. That the Court further order, pursuant to 18 U.S.C. § 1345, that within two days from Defendants' receipt of this Temporary Restraining Order and Order to Show Cause, Defendants shall provide copies of this Temporary Restraining Order and Order to Show Cause to all of their customers for whom they provide (1) United States call termination services, (2) United States toll-free call origination services; and to all entities (a) with whom Defendants have a contractual relationship for automated or least-cost call routing, or (b) from whom Defendants acquire toll-free numbers.
- Within four days from Defendants' receipt of the Temporary Restraining Order and Order to Show Cause, Defendants shall provide proof of such notice to the Court and the United States, including the names and addresses or email addresses of the entities and/or individuals to whom the notice was sent, how the notice was sent, and when the notice was sent.

- C. That the Court further order, pursuant to 18 U.S.C. § 1345, Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.
- D. That the Court further order, pursuant to 18 U.S.C. § 1345, that any Toll-Free Service Provider that receives notice of this Temporary Restraining Order and Order to Show Cause and has a contractual relationship with one of the Defendants in this matter to provide toll-free numbers, shall provide to Somos, Inc. a list of all toll-free numbers provided to that Defendant that are currently active.
- E. That the Court further order, pursuant to 18 U.S.C. § 1345, that any individual or entity who has obtained a toll-free number through one of the Defendants in this matter, either directly or through another intermediate entity, and wishes to continue using that toll-free number may submit a request to the Court, copying counsel for the United States, and identifying: (1) the individual or entity's name, address, phone number, email address, website URL, and the nature of their business; (2) the end-user of the toll-free number's name, address, phone number, email address, and website URL if the end-user did not obtain the toll-free number directly from Defendants; (3) the nature of the end-user's business; (4) the purpose for which the end-user utilizes the toll-free number; (5) the date on which the individual or entity obtained the toll-free number and, if applicable, provided it to the end-user; and (6) whether the toll-free number is used by the individual, entity, or end-user in connection with robocalls. The United States shall then notify the Court within four

business days whether the United States has any objection to removing the specifically identified toll-free number from the list of suspended numbers.

- F. That the Court issue a preliminary injunction on the same basis and to the same effect.
- G. That the Court issue a permanent injunction on the same basis and to the same effect.
- H. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: January 28, 2020

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney



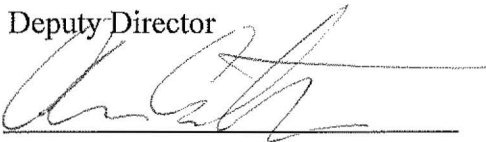
DARA OLDS
BONNI J. PERLIN
Assistant United States Attorneys
Eastern District of New York
271-A Cadman Plaza East
Brooklyn, New York 11201
Tel. (718) 254-7000
Fax: (718) 254-6081
dara.olds@usdoj.gov
bonni.perlin@usdoj.gov

JOSEPH H. HUNT
Assistant Attorney General
Civil Division
United States Department of Justice

DAVID M. MORRELL
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director



ANN F. ENTWISTLE
CHARLES B. DUNN
Trial Attorneys
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
Tel. (202) 307-0066
Tel. (202) 305-7227
Fax: (202) 514-88742
Ann.F.Entwistle@usdoj.gov
Charles.B.Dunn@usdoj.gov

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

UNITED STATES OF AMERICA

(b) County of Residence of First Listed Plaintiff

(EXCEPT IN U.S. PLAINTIFF CASES)

CV 20 - 473

(c) Attorneys (Firm Name, Address, and Telephone Number)

Dara Olds, Bonni Perlin

U.S. Attorney's Office, Eastern District of New York

271-A Cadman Plaza East, 7th Fl., Brooklyn, NY 11201; (718) 254-7000

DEFENDANTS

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com

County of Residence of First Listed Defendant Maricopa

(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

☒ 1 U.S. Government Plaintiff☐ 3 Federal Question

(U.S. Government Not a Party)

☐ 2 U.S. Government Defendant☐ 4 Diversity

(Indicate Citizenship of Parties in Item III)

KORMAN, J.

MANN, M.J.

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Citizen of This State ☐ 1 ☐ 1Citizen of Another State ☐ 2 ☐ 2Citizen or Subject of a Foreign Country ☐ 3 ☐ 3

PTF DEF

Incorporated or Principal Place of Business in This State ☐ 4 ☐ 4Incorporated and Principal Place of Business in Another State ☐ 5 ☐ 5Foreign Nation ☐ 6 ☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT

- ☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

PERSONAL INJURY

- ☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Federal Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury
☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY

- ☐ 365 Personal Injury - Product Liability
☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability
☐ 368 Asbestos Personal Injury Product Liability
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

PERSONAL PROPERTY

- ☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY

- ☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 690 Other

BANKRUPTCY

- ☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS

- ☐ 820 Copyrights
☐ 830 Patent
☐ 840 Trademark

LABOR

- ☐ 710 Fair Labor Standards Act
☐ 720 Labor/Management Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Employee Retirement Income Security Act

SOCIAL SECURITY

- ☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS

- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES

- ☐ 375 False Claims Act
☐ 376 Qui Tam (31 USC 3729(a))
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit
☐ 490 Cable/Sat TV
☐ 850 Securities/Commodities/Exchange
☒ 890 Other Statutory Actions
☐ 891 Agricultural Acts
☐ 893 Environmental Matters
☐ 895 Freedom of Information Act
☐ 896 Arbitration
☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 950 Constitutionality of State Statutes

REAL PROPERTY

- ☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

CIVIL RIGHTS

- ☐ 440 Other Civil Rights
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/Accommodations
☐ 445 Amer. w/Disabilities - Employment
☐ 446 Amer. w/Disabilities - Other
☐ 448 Education

PRISONER PETITIONS

- Habeas Corpus:
☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
☐ 530 General
☐ 535 Death Penalty
 Other:
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding☐ 2 Removed from State Court☐ 3 Remanded from Appellate Court☐ 4 Reinstated or Reopened☐ 5 Transferred from Another District (specify)☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

Request for relief pursuant to 18 U.S.C. § 1345

Brief description of cause:

Violations of wire fraud statutes, 18 U.S.C. §§ 1343, 1349

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

CERTIFICATION OF ARBITRATION ELIGIBILITY

Local Arbitration Rule 83.7 provides that with certain exceptions, actions seeking money damages only in an amount not in excess of \$150,000, exclusive of interest and costs, are eligible for compulsory arbitration. The amount of damages is presumed to be below the threshold amount unless a certification to the contrary is filed.

Case is Eligible for Arbitration ☐

I, Dara Olds, counsel for United States of America, do hereby certify that the above captioned civil action is ineligible for compulsory arbitration for the following reason(s):

☐
☒
☐

monetary damages sought are in excess of \$150,000, exclusive of interest and costs,

the complaint seeks injunctive relief,

the matter is otherwise ineligible for the following reason

DISCLOSURE STATEMENT - FEDERAL RULES CIVIL PROCEDURE 7.1

Identify any parent corporation and any publicly held corporation that owns 10% or more of its stocks:

RELATED CASE STATEMENT (Section VIII on the Front of this Form)

Please list all cases that are arguably related pursuant to Division of Business Rule 50.3.1 in Section VIII on the front of this form. Rule 50.3.1 (a) provides that "A civil case is 'related' to another civil case for purposes of this guideline when, because of the similarity of facts and legal issues or because the cases arise from the same transactions or events, a substantial saving of judicial resources is likely to result from assigning both cases to the same judge and magistrate judge." Rule 50.3.1 (b) provides that "A civil case shall not be deemed 'related' to another civil case merely because the civil case: (A) involves identical legal issues, or (B) involves the same parties." Rule 50.3.1 (c) further provides that "Presumptively, and subject to the power of a judge to determine otherwise pursuant to paragraph (d), civil cases shall not be deemed to be 'related' unless both cases are still pending before the court."

NY-E DIVISION OF BUSINESS RULE 50.1(d)(2)

- 1.) Is the civil action being filed in the Eastern District removed from a New York State Court located in Nassau or Suffolk County? ☐ Yes ☒ No
- 2.) If you answered "no" above:
 - a) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in Nassau or Suffolk County? ☒ Yes ☒ No
 - b) Did the events or omissions giving rise to the claim or claims, or a substantial part thereof, occur in the Eastern District? ☒ Yes ☐ No
 - c) If this is a Fair Debt Collection Practice Act case, specify the County in which the offending communication was received:

If your answer to question 2 (b) is "No," does the defendant (or a majority of the defendants, if there is more than one) reside in Nassau or Suffolk County, or, in an interpleader action, does the claimant (or a majority of the claimants, if there is more than one) reside in Nassau or Suffolk County? ☐ Yes ☐ No

(Note: A corporation shall be considered a resident of the County in which it has the most significant contacts).

BAR ADMISSION

I am currently admitted in the Eastern District of New York and currently a member in good standing of the bar of this court.

☒

Yes

☐

No

Are you currently the subject of any disciplinary action (s) in this or any other state or federal court?

☐

Yes (If yes, please explain

☒

No

I certify the accuracy of all information provided above.

Signature: Dara Olds

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.

NICHOLAS PALUMBO, NATASHA
PALUMBO, ECOMMERCE NATIONAL, LLC
d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a
sipretail.com,

Defendants.

CV 20 - 473

Civil Action No.

KORMAN, J.

MANN. M.J.

DECLARATION OF SAMUEL BRACKEN

I, Samuel Bracken, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Postal Inspector with the United States Postal Inspection Service ("USPIS") since February 2004. I am currently assigned to the Elder Fraud Task Force at the Department of Justice, Consumer Protection Branch. I am assigned to investigate violations of federal law, including mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1341 and 1343, respectively. I have received training in investigating elder fraud, social security fraud, IRS fraud, identity theft, credit card fraud, counterfeit check fraud, counterfeit identification card fraud, mail, and wire fraud offenses, including attending seminars and conferences hosted by the Inspection Service, the United States Department of Justice, the International Association of Financial Crimes Investigators, and various other law enforcement entities. During my employment as an Inspector, I have participated in hundreds of

investigations involving identity fraud, aggravated identity theft, mail fraud and wire fraud. In addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

2. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, USPIS records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application for a temporary restraining order, it does not set forth each and every fact that I learned during the course of this investigation.

SUSPICIOUS PAYMENTS TO TOLLFREEDEALS

3. In the course of this investigation, records were obtained from Wells Fargo Bank regarding an account held in the name of Ecommerce National LLC with a signer of Nicholas Palumbo. For the time period of May 28, 2019 through September 11, 2019, the account received nineteen cash deposits totaling \$130,250.00. These deposits occurred in locations across the United States, including in Minnesota, South Carolina, Florida, Alabama, and New Jersey. None of these cash deposits occurred in Arizona, the principle location of business for Ecommerce National.

4. Within days of receiving these cash deposits, Nicholas Palumbo would transfer the funds from the Wells Fargo Account, via wire transfers or checks maybe payable to Ecommerce National LLC, to two accounts held in the name of Ecommerce National LLC at JP Morgan Chase. The sixteen transactions totaled \$131,584.00.

5. Through my training and experience, I know that accounts known as “interstate funnel accounts” are one of the most efficient means for criminal organizations to rapidly move illicit proceeds within the U.S. and abroad. Based on my training as a federal law enforcement officer and fraud investigator, I know that funnel accounts offer the rapid movement of money across great distances with minimal fees and the anonymity of the depositors, since the deposits are usually under the reporting thresholds. Analysis of Bank Secrecy Act (BSA) reporting has identified that the following account activity is often associated with funnel accounts:

- out-of-state, anonymous cash deposits in multiple states;
- rapid cash withdrawals for amounts similar to cash deposits;
- use of counter deposit slips;
- individual deposits and withdrawals intentionally under \$10,000 (structuring);
- limited account credits besides cash deposits (i.e., no payroll, wire transfers);
- no legitimate business purpose evident;
- and deposit activity greater than expected income.

Based on my training and experience, it appears that TollFreeDeals is utilizing the Wells Fargo bank account as a funnel account to receive fraud proceeds from co-conspirators.

NEW YORK VICTIMS OF DEFENDANTS' FRAUDULENT ROBOCALLING CONSPIRACIES

6. On January 16, 2020, I interviewed victim J.K., an 84-year-old man who is a former member of the United States Marine Corps and who resides in Belle Harbor, New York. J.K. was the victim of a social security imposter scam. J.K. received a message on his cellular telephone on May 23, 2019, concerning his social security number. J.K. called back the phone number left in the message, 512-XXX-XXXX, and spoke with an individual who stated that he

was from the U.S. Marshals Service and that a warrant had been issued for J.K.'s arrest. He then transferred J.K. to a man named who claimed his name was "David" and that he was an employee with the Social Security Administration ("SSA"). David told him that a car had been rented in Houston, Texas using J.K.'s personal information, including his social security number, and that the car was found by local police with evidence of drugs and money laundering. J.K. was told there was a warrant for his arrest based on this activity.

7. David told J.K. he would help J.K. to straighten this situation out, and that J.K. needed to protect his bank accounts from forfeiture and that the government was going to seize his funds due to the criminal activity. David asked J.K. about his bank accounts, and directed J.K. to wire transfer all of the money out of his account to an account number David provided. David informed J.K. that his money was being wired to the U.S. Marshals Service, who would provide his money back to him at a later date after the situation with the warrant was cleared up. J.K. proceeded to transfer \$9,800.00 from his bank account to the account provided by David. J.K. spent several hours on the phone during this interaction. J.K. became suspicious after he wired the money, told David he would not be sending any more, and ended the phone call.

8. J.K. then received a call from an individual claiming to be with the warrant squad of the New York City Police Department (NYPD). The individual claiming to be from the NYPD told J.K. that in order to get the warrant lifted, J.K. needed to call David back. J.K. received several more calls, but he did not answer them. J.K. contacted his bank in an attempt to stop the wire transfer, and was told that the money had already been removed from the account to which it was sent.

9. I reviewed call detail records obtained from TollFreeDeals, and confirmed that multiple calls were made to J.K.'s cell phone on May 23, 2019. All of the calls spoofed the main

SSA toll-free customer service number, and were all sent to TollFreeDeals by the same India-based VoIP carrier.

10. On January 16, 2020, I spoke with C.E., who was a victim of an SSA impersonation scam. C.E. is a 36-year-old man who recently received U.S. citizenship and resides in Brooklyn, New York. C.E. received a telephone call on June 6, 2019, from a man who claimed his name was “George” and that he was from SSA. George told C.E. that SSA was investigating his name and social security number being used in connection with money laundering. George told C.E. that there was a warrant out for his arrest, and George already knew C.E.’s social security number. George told C.E. that the next step he needed to take to protect himself was to file a report with a police officer. George then connected C.E.’s phone call with a man claiming to be a police officer.

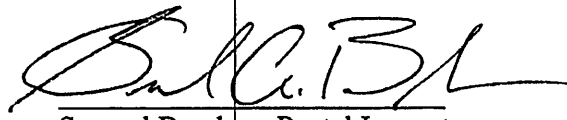
11. The police officer told C.E. that he had to secure his bank accounts by moving the money out of his accounts, so the money wouldn’t be seized. The police officer instructed C.E. to go to Best Buy and purchase gift cards using his debit card to remove the money from his bank account. C.E., who was working as a driver for Uber, then drove to a Best Buy in Queens, New York, where he purchased two Hotels.com gift cards with a combined value of \$700.00. He then provided the gift card numbers to the man on the phone. The man on the phone then requested more money, but C.E. didn’t have any more money in his bank accounts. After he got off the phone, C.E. realized he had been scammed, and he filed a police report and a complaint with the Federal Trade Commission (“FTC”). C.E. stated that he received another call from the same people later that day, and the caller told him that they would be coming to his apartment to provide him with his new social security number.

12. I reviewed call detail records obtained from TollFreeDeals, and confirmed that a call to C.E.'s phone lasting almost two hours was sent through TollFreeDeals on June 6, 2019, from India-based VoIP carrier Company A.

13. I have also reviewed a complaint filed with the Federal Trade Commission by L.U., a man in his forties who resides in Roosevelt, New York, in Nassau County. L.U. reported to the FTC that he received a call on June 5, 2019, from 877-382-4357. That is the phone number of the FTC's Consumer Response Center. On the FTC's website, FTC states that while they receive inbound calls at that number, FTC does not make outbound calls from that number. L.U. reported that the person who called him posed as the SSA, and informed L.U. that his social security number was going to be suspended due to criminal activity if he did not provide his personal information. L.U. reported that he lost \$2,200.00 as a result of this SSA imposter scam.

14. I have reviewed call detail records obtained from TollFreeDeals, and confirmed that two calls were sent from Company A through TollFreeDeals to L.U.'s phone number on June 5, 2019. Both calls spoofed FTC's Consumer Response Center as the source number.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27, 2020, in Phoenix, Arizona.


Samuel Bracken, Postal Inspector
United States Postal Inspection Service

★ JAN 28 2020 ★

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

BROOKLYN OFFICE

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA
PALUMBO, ECOMMERCE NATIONAL, LLC
d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a
sipretail.com,

Defendants.

CV 20 - 473

Civil Action No.

KORMAN, J.

MANN, M.J.

DECLARATION OF MARCY RALSTON

I, Marcy Ralston, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Special Agent with the Social Security Administration's Office of Inspector General ("SSA OIG"), Office of Investigations since October 2004. I have been employed as a federal law enforcement officer for approximately 16 years. From approximately August 2002 until December 2003, I was employed as a Postal Inspector with the United States Postal Inspection Service. My current duties include investigating violations of Federal and State laws, primarily as they relate to misuse of social security numbers and violations of laws and regulations administered by the SSA. This includes crimes of mail fraud, identity deception, welfare fraud, theft, perjury and forgery. I have participated in multiple search warrants. I have worked several large scale, multi-agency investigations and have interviewed multiple witnesses, suspects and cooperating individuals as a part of my duties. Before this, I received a Bachelor's Degree from Indiana University in Criminal Justice in 1997. I have attended twelve weeks of

federal law enforcement training from the Inspection Service, as well as continuing education with SSA-OIG.

2. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, USPIS records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application for a temporary restraining order, it does not set forth each and every fact that I learned during the course of this investigation.

3. SSA Imposter fraud has resulted in the filing of hundreds of thousands of complaints with the Administration in just the last fifteen months. Specifically, analysis of our complaints database reveals 465,000 complaints about fraudulent telephone impersonation of the Administration between October 1, 2018 and September 30, 2019; these complaints reflect aggregated losses of over \$14 million.

4. In addition, the Federal Trade Commission ("FTC") collects complaints in its Consumer Sentinel database on SSA and other government imposter scams. For 2018, the FTC received more than 39,000 fraud complaints about SSA imposters, with related victim losses of approximately \$11.5 million. SSA imposter fraud complaints for 2019 include approximately 166,000 complaints relating more than \$37 million in losses.¹ In my experience, these complaint

¹ Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting \$128,479,054 in losses for 2018, and 389,563 complaints reflecting \$152,946,623 in losses for 2019.

numbers substantially underrepresent the extent of fraudulent activity because most victims do not report their losses to the government.

OVERVIEW OF DEFENDANTS' WIRE FRAUD SCHEME

5. This investigation involves a wire fraud scheme conducted and facilitated by husband and wife Nicholas and Natasha Palumbo (“the Palumbos”) through the entities Ecommerce National LLC d/b/a TollFreeDeals.com (“TollFreeDeals”) and SIP Retail, LLC d/b/a SIPRetail.com (“SIP Retail”) (collectively, “Defendants”). The Palumbos operate and control the named entities from their home in Paradise Valley, Arizona.

6. As relevant to this Declaration, “robocalling” refers to an automated process of placing 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. SSA OIG is investigating criminal schemes perpetrated by individuals operating one or more call centers located in India and other foreign locations. Fraudsters at the call centers impersonate government agencies and other entities – including the SSA, other government agencies, and businesses – and place millions of robocalls to phones in the United States. These robocalls convey recorded messages instructing the recipients to contact the impersonated entity regarding problems with their social security numbers, missed court dates, imminent asset freezes, and other such lies that are intended to secure the recipient into establishing phone contact with a criminal. In all of these schemes, the criminals attempt to defraud and extort money from anyone who contacts them in response to their messages.

7. Since at least 2016, despite repeated warnings from various government entities and industry actors, the Palumbos and the entities they control have provided robocallers with unfettered access to the U.S. phone system and thus the ability to deluge U.S. residents with

millions of fraudulent robocalls. The Palumbos, through their companies, have also provided fraudsters with toll-free phone numbers used in furtherance of the robocall fraud schemes that allow victims to return calls to the fraudsters in foreign locations at what appears to the potential victim to be a legitimate U.S. toll-free phone number.

8. Defendants' participation in these fraudulent robocall schemes is essential to the success of the schemes. Without someone willing to accept the fraudsters' robocall traffic into the U.S. telephone system, even though the fraudsters have internet access they would be unable to contact any potential victims in the first instance. The Palumbos provide the crucial interface between foreign internet-based phone traffic and the U.S. telephone system, and our investigation reveals that they do so with full knowledge that they are participating in massive frauds. Similarly, by providing toll-free services, Defendants not only enable initial contact with potential victims, but also provide legitimate U.S. toll-free numbers that cloak the fraud in a façade of legitimacy and allow the unwitting to become victims when they return calls to fraudsters after they receive a robocall voicemail message.

9. The robocall imposters in this investigation use a variety of methods to receive funds from victims, including but not limited to asking victims to: purchase gift cards or other stored value cards and transmit the numbers from the back of the cards to the fraudsters; send bank wires; and send cash payments by overnight carrier.

10. Victims will often send these funds to individuals referred to by law enforcement as "money mules" located in the United States, who receive and collect victim payment funds from fraud schemes, and then conduct transactions on behalf of their "handlers," who will instruct them what to do with the funds. "Money mules" will often send money from the United States back to India, via money transmitting businesses, and/or pay the business expenses for the call centers,

including paying U.S. based companies that are helping to route scam calls to U.S. victims. These payments will often consist of cash deposits into the bank accounts of the U.S. based companies.

11. In the course of this investigation, we have learned that TollFreeDeals and SIP Retail have transmitted robocalls as part of numerous fraudulent robocalling schemes, including:

- a) SSA Imposters – SSA Imposters send recorded messages falsely claiming that the recipient's social security number has been used in criminal activity, the recipient's social security benefits will be suspended, the recipient failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be terminated. When an individual 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 the individual is issued a new social security number, at which point the individual's funds will be returned.
- b) Internal Revenue Service ("IRS") Imposters: IRS imposters send recorded messages falsely claiming that the recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.
- c) United States Citizenship and Immigration Services ("USCIS") Imposters: USCIS imposters send recorded messages falsely claiming that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or

deportation, that the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

- d) Tech Support Imposters: Fraudsters operating tech support scams impersonate various well-known tech companies, such as Apple or Microsoft, and send recorded messages falsely claiming that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster often convinces the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.
- e) Loan Approval Scams: Fraudsters operating loan approval scams leave messages impersonating a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a call recipient connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is to pay a one-time fee up front.

TECHNOLOGIES USED IN THE ROBOCALLING FRAUD SCHEMES

12. The technical ability to place the fraudulent calls at issue in the investigation is dependent on (1) voice-over-internet-protocol ("VoIP")² calling and related technology to create the calls, and (2) a "gateway carrier" to introduce the foreign call traffic into the U.S. phone system.

² VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

In the telecommunications industry, the term “gateway carrier” refers to a U.S. based person or entity that agrees with a foreign person or entity (often by contract) to accept foreign-source VoIP telephone traffic. VoIP uses a broadband internet connection – as opposed to an analog traditional phone line – to place phone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional wired phone. The technology employed by modern telecommunication providers mediates between digital VoIP signals and regular telephone signals so that communication is seamless between VoIP and non-VoIP users at either end. VoIP is used in the schemes both to place robocalls to U.S. phones and to communicate with individuals who either answer the robocall or call the number contained in the recorded robocall message.

13. VoIP relies upon a set of rules for electronic communication called Session Initiation Protocol (“SIP”). Much like the way browsing websites on the Internet use HyperText Transfer Protocol (“HTTP”) to initiate and conduct information exchanges between devices through exchanges of packets of information, SIP is a set of rules used to initiate and terminate live sessions for things such as voice and video communication between two or more points connected to the Internet. Both SIP voice communication and HTTP web-browsing rely on exchanging data packets between two points. For example, web browsing via HTTP requires an individual to request information from another point on the internet, usually by clicking on a hyperlink or entering a web address in a browser’s address bar, usually preceded by “http://www,” which tells the device that it is making a request for information on the World Wide Web via HTTP. A device receiving that request will send back information to the requesting device, and thus, the requesting device will display the requested website.

14. Similarly, a voice call via SIP starts as a data packet sent to initiate a call, a responsive packet sent back that indicates whether the call has been answered, and numerous other packets transiting back and forth; amongst these data packets is information that machines at either end turn into audible signals, i.e., a conversation that can be heard by the participants. In the case of robocalls, a recorded message is transmitted once the call is answered by a live person or by voicemail.

15. Robocalls should not be understood as traditional telephone calls, but rather, requests for information and responsive data packets transiting the internet via SIP. An outgoing robocall begins as a request for information sent by an automatic telephone dialing system known as an “autodialer” that—in conjunction with VoIP services—enables the caller to make millions of sequential requests for information (i.e., outbound VoIP phone calls) in a very short time. A VoIP autodialer is a specialized type of telecommunications equipment having the capacity to (1) store or produce telephone numbers to be called, and (2) request responsive information from devices at the other end of the call, i.e., dial the telephone numbers. The autodialer’s requests for information are directed to devices (here, telephones) that send back responsive information when the call is answered either by a live person or the person’s voicemail. When the autodialer receives the information from the called device indicating that the call is answered, the autodialer will then send information back to that device (the phone) in the form of a recorded message. As relevant here, fraudsters created the recorded message that conveys false threats while impersonating a U.S. agency or the other entities described above.

16. A fraudster making these robocalls can not only send a recorded message to the potential victim’s phone, but can misrepresent the origin of the call on the call recipient’s caller ID. Normally, a recipient’s caller ID will display information identifying the caller by means of a

telephone number that is automatically displayed because the caller owns the right to use that phone number; however, many VoIP software packages allow the caller to specify the information appearing on the call recipient's caller ID, much in the same way an email's subject line can be edited to state whatever the sender wishes. This practice of specifying what appears on the recipient's caller ID is called "spoofing." This feature of VoIP technology permits a caller with an illicit motive to spoof a legitimate phone number, such as that belonging to a government entity, in order to cloak the fraudsters with indicia of authority and induce the recipients to answer the call. Spoofing also encourages potential victims to return calls when they look up the spoofed number and see that it is a number used by an official government entity. In these robocalling schemes, spoofing serves the purpose of deceiving the potential victim about who is calling them.

17. Spoofing any phone number is a simple matter of editing an SIP file to state the desired representation on the caller ID. These files can then be loaded into an autodialer to become robocalls, replicated millions of times with the spoofed, fraudulent caller ID information.

18. The fraudulent robocalls generally leave prerecorded, threatening messages for recipients. Some of the fraudulent messages direct the recipient to press a key to speak with a live operator. Other fraudulent messages leave a domestic telephone number as a "call-back" number. In either case, whether the recipient presses a key or calls the call-back number, the recipient will be connected to a fraudster in a foreign call center.

19. A gateway carrier is also essential to these fraud schemes perpetrated through these robocall schemes. Foreign call centers and VoIP carriers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign call traffic. For example, a fraudulent call center in India cannot directly upload tens of millions of robocalls to the U.S. telephone

system, even where they have broadband internet and VoIP service. Foreign VoIP telephone traffic cannot enter the U.S. telephone system without travelling through a gateway carrier willing to accept the foreign traffic and introduce it to the U.S. telephone system. In the course of this investigation, SSA OIG has determined that Defendants act as gateway carriers for calls originating abroad that are bound for the United States. In the context of the schemes, fraudulent robocalls are “US terminat[ed]” calls, and return calls to fraudsters in other countries are “international voice terminat[ed]” calls.

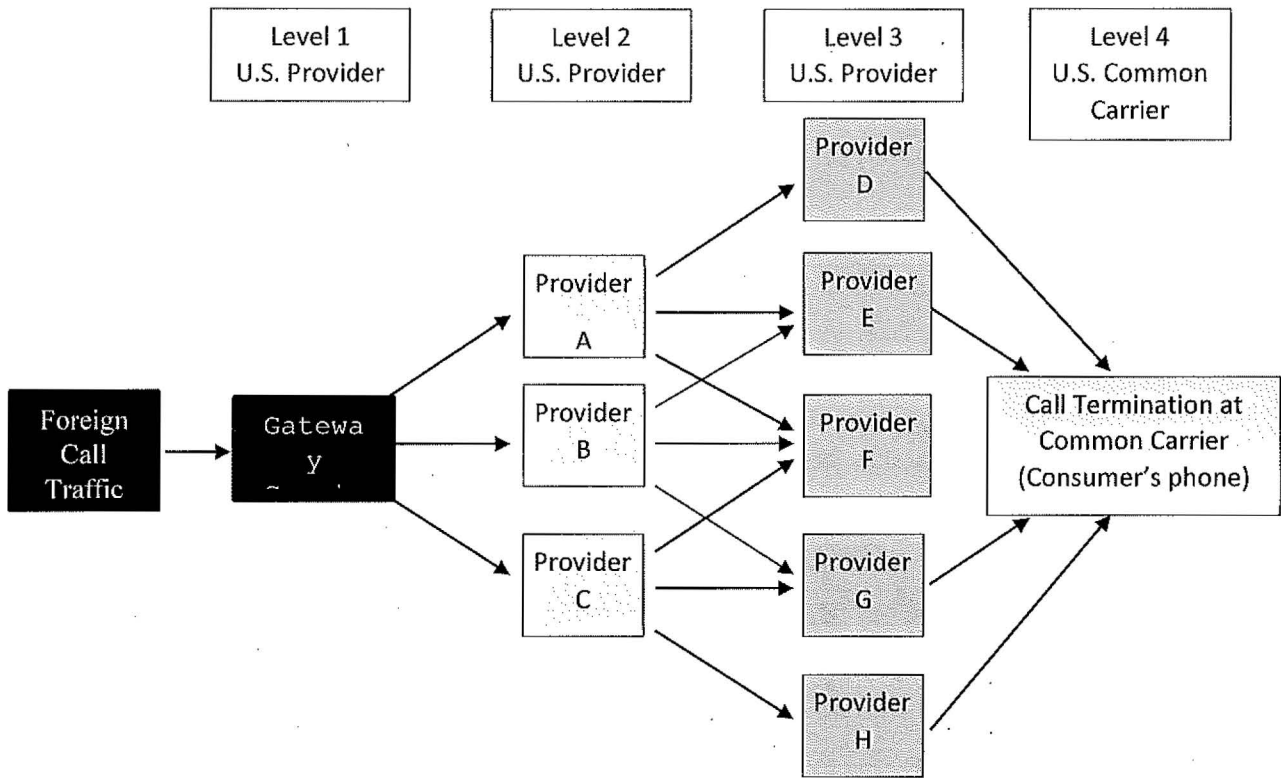
20. In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.

LEAST-COST CALL ROUTING AND TRACEBACKS

21. When foreign call centers route fraudulent robocalls through Defendants to recipients in the United States through VoIP technology, the calls typically pass through many different VoIP carriers. First, the calls typically pass from a foreign VoIP carrier to Defendants as the U.S. gateway carrier. From Defendants, calls typically pass through multiple other carriers until they reach a common carrier such as AT&T or Verizon. Consumer-facing companies like Verizon and AT&T are known in the industry as “common carriers.”

22. With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the system routes calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, the company at each routing step will have numerous existing contracts through which it can route

outbound calls through intermediate providers to the common carriers as the last routing step before an individual in the United States can answer the call. This automated routing process is called “least-cost routing,” illustrated in the following diagram beginning with a first-level U.S. gateway carrier:



In this simple example, arrows represent possible routing paths between providers based on preexisting contracts. Here, the gateway carrier has three contracts with second-level U.S. providers A, B, and C, each of which in turn has three contracts with third-level providers further into the U.S. phone system (denoted by Providers D, E, F, G, and H). Each of the third-level providers is able to pass calls to the fourth-level common carrier that provides telephone service to the U.S. individual. The call will move through one of many paths, depending on the effective contract terms between the gateway carrier, providers, and common carriers at the time the call is

routed that achieve the lowest cost to transmit the call, i.e., “least-cost routing.” In real-world application, least-cost routing may involve more than four levels of U.S. companies.

23. In light of least-cost routing and the prevalence of spoofing telephone numbers, identifying the source of any specific robocall requires a labor-intensive process known in the telecommunications industry as “traceback.” In order to conduct the traceback, an investigator must trace backwards each individual “hop” the call took in its least-cost-routing journey from the gateway carrier. For example and referencing the diagram above, the common carrier will be able to query its own system and determine which Level 3 Provider it received the call from, but it will not be able to see beyond that. The common carrier must contact the Level 3 Provider and ask that carrier to determine from its records what Level 2 Provider it received the call from. The common carrier must then contact the Level 2 Provider and ask them to determine which Level 1 provider they received the call from. This process continues at each “hop” until a provider identifies a foreign source – that carrier is then the “gateway carrier” that permitted the foreign telephone traffic to enter the U.S. phone system.

DEFENDANTS’ ROLE IN AND KNOWLEDGE OF ROBOCALLING WIRE FRAUD CONSPIRACIES

24. Documents and other evidence obtained and reviewed in the course of this investigation, including Arizona Secretary of State and Arizona Corporation Commission records, the FCC 499 Filer Database, and a review of LinkedIn profiles, have revealed that Nicholas Palumbo has been the Chief Executive Officer of Ecommerce National LLC d/b/a TollFreeDeals.com (“TollFreeDeals”) since approximately 2003. Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals

as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona.

25. As of January 25, 2020, the TollFreeDeals.com website identifies Nicholas Palumbo as the President/Founder of TollFreeDeals.com, and Natasha Palumbo as the Vice President of Business Development. Through TollFreeDeals, the Palumbos provide inbound VoIP calling to the United States (also known as “U.S. VoIP termination,” because the calls “terminate” in the United States) to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP dialing, meaning that they place no restriction on the number of calls their customers can place or the duration of those calls.

26. Through TollFreeDeals, the Palumbos specifically cater to call centers placing robocalls. The company’s website states, “TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!” The “FAQs” page of the website states, “Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center voip termination minutes.” The website header also contains the statement “Call Center Minutes Terminated,” followed by a number that updates every few seconds. As of January 23, 2020, that number was 10,491,500,323. Based on SSA OIG’s investigation and as described above, all foreign fraudsters committing SSA impersonation fraud, as well as other government impersonation fraud and tech support impersonation fraud utilize robocalls and call centers. Defendants specifically market their U.S. call termination services to these types of customers.

27. A review of Arizona Corporation Commission records revealed that Natasha Palumbo is the registered owner and CEO of SIP Retail LLC, and has served in this capacity since registering the company on August 29, 2017. Arizona Corporation Commission records also reveal that Nicholas Palumbo is an officer/agent of SIP Retail, and that SIP Retail's current statutory agent address is the same as that for TollFreeDeals – the Palumbos' current home address in Paradise Valley, Arizona. I also viewed the website for SIP Retail, which lists Natasha Palumbo as the CEO and Founder and offers VoIP call termination services into the United States, just like TollFreeDeals. SIP Retail's website is nearly identical to the website for TollFreeDeals, including listing the same phone number for customer inquiries.

28. The websites for both TollFreeDeals and SIP Retail state that the companies use the switching platform Sip Navigator to carry VoIP termination traffic.

29. Over the past two years, Defendants received many notices, inquiries, warnings, complaints, and subpoenas concerning fraudulent robocalls transiting their systems. These warnings and inquiries came from other telecommunications companies, an industry trade group, and law enforcement agencies. Further, a review of the call detail records in the Palumbos' possession reveals that the call traffic transmitted by the majority of their customers is filled with the indicia of fraud. Nevertheless, Defendants continue to enable these massive fraud schemes to be perpetrated on U.S. individuals.

Warnings and Traceback Requests from USTelecom

30. USTelecom is a nonprofit trade association for the U.S. broadband and communications industry. USTelecom has developed an Industry Traceback Group across the telephonic communications industry to trace robocalls to their sources. Based on tracebacks

conducted with the assistance of the Industry Traceback Group, SSA OIG has identified TollFreeDeals as the number one gateway carrier of SSA imposter calls in 2019.

31. When the Industry Traceback Group conducts a traceback of a fraudulent robocall, USTelecom sends a series of email messages, starting with the common carrier whose customer received the fraudulent robocall, and getting information from each VoIP carrier in the chain about who sent the call to that VoIP carrier. These emails are referred to below as “traceback emails.”

32. The Palumbos received USTelecom traceback emails about fraudulent calls that had been transmitted through TollFreeDeals and SIP Retail. Every USTelecom traceback email stated that a suspicious call has been traced back to TollFreeDeals or SIP Retail and provided the call date and time, the source number (the number that appears on the call recipient’s caller ID, as well as in the gateway carrier’s call records as the source of the call) and the call recipient’s phone number to allow TollFreeDeals or SIP Retail to identify the specific call at issue in its call detail records. Each email also provided a link to USTelecom’s web-based traceback portal, where further information is provided about the specific fraudulent call at issue, including a recording of the fraudulent voicemail message that was left on a recipient’s voicemail. USTelecom traceback emails were sent to the Palumbos at nick@tollfreedeals.com or to help@sipretail.com.

33. Each traceback email from USTelecom included a short description of the type of fraudulent robocall at issue and the details of the fraudulent robocall campaign. Prior to August 2019, those descriptions were included in the traceback portal, but beginning in August 2019, those descriptions were also included in the text of the traceback email itself. An example of a traceback email sent to TollFreeDeals on August 14, 2019, is attached hereto as Exhibit 1. That email includes the following description of the fraud scheme:

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

The abbreviation “ANI” stands for “Automatic Number Identification,” and for these purposes refers to the purported source number. Evidence obtained in this investigation indicates that, in response to traceback emails, Defendants blocked the single source number identified in the each email.

34. The traceback emails include a hyperlink that when clicked leads to USTelecom’s online traceback portal, specifically, to a page with information regarding the specific fraudulent robocall that was the subject of the email. The portal includes audio of the voicemail message left as part of this SSA imposter robocalling campaign. I listened to the recorded audio linked to a call transmitted by TollFreeDeals on December 19, 2019, which states:

We have been forced to suspend your social security number with immediate effect. Due to this, all your social benefits will be cancelled until further clearance. In case you feel this is due to an error, you may connect with legal [unintelligible] Social Security Administration. In order to connect with a Social Security Administration officer, press one now. In case we do not hear from you your social will be blocked permanently. To connect with the officer now, press 1 and you will automatically be connected with the concern departments. We did not receive any input. Dear citizen, in order to speak with Social Security personal regarding your social security, press 1 and this automated system will connect you with the officials. Press....

35. On June 3, 2019, USTelecom sent a traceback email to TollFreeDeals regarding an SSA imposter call. A consultant hired by USTelecom named David Frankel then corresponded directly with Nicholas Palumbo regarding the original SSA impersonation call traceback. In response, Nicholas Palumbo identified Company A, an India-based telecommunications company,

as the provider that had transmitted the SSA impersonation call to TollFreeDeals. In further email correspondence over the course of the day, David Frankel identified several different calls that were all part of the same SSA impersonation fraud campaign and all appeared on caller-ID to be coming from different source numbers. Nicholas Palumbo identified all seven calls as having been transmitted to TollFreeDeals by Customer A.

36. Three days after this email exchange, victim C.E. who was later interviewed by the Postal Inspection Service, was defrauded by an SSA imposter call. TollFreeDeals call detail records show that the SSA imposter call was transmitted from Company A to TollFreeDeals and eventually to victim C.E.'s cell phone. *See* Declaration of Samuel Bracken, Postal Inspector with the United States Postal Service, dated January 27, 2020, ¶¶ 10-12.

37. Based on the volume of traceback emails that TollFreeDeals and SIP Retail have received from USTelecom, Defendants were warned repeatedly that many of their customers were transmitting millions of fraudulent robocalls. From May 2019 through January 2020, TollFreeDeals received a total of 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced a USCIS impersonation fraud call. TollFreeDeals reported to USTelecom that it had received these 144 calls from 14 different customers, and that all of the SSA Impersonation calls traced back to the same two Indian entities.

38. From August 2019 through December 2019, USTelecom notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, six tracebacks of Tech Support fraud calls, and one traceback of USCIS impersonation fraud calls. SIP Retail reported back to USTelecom that it had received these 35 fraudulent calls from seven

different companies, and that all 19 of the SSA impersonation calls were sent to SIP Retail by two India-based companies that sent SSA imposter calls through TollFreeDeals.

Notifications of Fraudulent Robocall Traffic From AT&T

39. In May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by AT&T customers in which the source number was spoofed to show a number belonging to USCIS; another number was spoofed to show the Office of the Inspector General of the U.S. Department of Homeland Security (“DHS-OIG”). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T’s customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not make outbound calls from either of the spoofed phone numbers. Nicholas Palumbo responded that the calls had been transmitted to TollFreeDeals from an India-based customer, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number for their fraud calls.

40. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to “extort money from our customers.” In Nicholas Palumbo’s response to AT&T, he acknowledged that those calls had been transmitted to TollFreeDeals from the same India-based VoIP carrier that had transmitted the spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this customer was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

Records of the Calls Transmitted by TollFreeDeals are Filled with Evidence of Fraud

41. SSA obtained call detail records from TollFreeDeals for all call traffic transmitted from India-based VoIP carrier Company A to TollFreeDeals between May 6, 2019 and June 30, 2019. During that period, Company A transmitted 182,023,773 calls to phones of U.S. call recipients through TollFreeDeals. These calls came from more than ten million unique source numbers, the vast majority of which were U.S. phone numbers. Based on my training and experience, there is no legitimate business purpose for which one or several foreign call centers would use millions of different U.S. source numbers to transmit calls originating abroad. This massive volume of different source numbers, as well as the ratio of source numbers to calls, is indicative of the use of random, spoofed source numbers in order to: (1) make it appear to potential victims that the calls originate in the United States, and (2) mask from legitimate U.S. carriers and law enforcement the fact that all of these millions of fraudulent calls are originating from the same source.

42. Of these more than 182 million calls, more than 2.8 million were made to phone numbers with area codes locating them within the Eastern District of New York.

43. In the call detail records related to Company A, one thousand different unique source numbers accounted for more than 90% of the calls, more than 164 million calls. SSA OIG requested records regarding these 1,000 source numbers from YouMail, a company that provides robocall-blocking software that can be downloaded for free on any cellular phone, and which maintains detailed analytics records regarding all calls blocked on behalf of its more than 10 million subscribers. Specifically, YouMail maintains data regarding the type of scam voicemails left for its customers. Records obtained from YouMail demonstrate that 79% of the top 1,000 source numbers from the Company A call detail records have been identified as sending scam

calls. Aggregating the number of calls made by each of the source numbers identified by YouMail as sending fraudulent robocalls, Company A transmitted more than 143 million fraudulent robocalls to U.S. call recipients through TollFreeDeals between May 6, 2019 and June 30, 2019. Based on YouMail's categorization of those scam calls, almost 20% (more than 31 million calls) were SSA imposter calls, another 35% (more than 57 million calls) were loan approval scams, and 14% (more than 23 million calls) were Microsoft Refund Scams,³ a subset of Tech Support impersonation scams.

44. The Consumer Sentinel database maintained by the FTC contained consumer complaints regarding 923 of the 1,000 source numbers from the call detail records related to Company A. As of August 2019, the Consumer Sentinel database contained 58,225 complaints regarding those 923 source phone numbers.

45. SSA OIG also obtained call detail records from TollFreeDeals regarding all VoIP call traffic terminated in the United States by TollFreeDeals on behalf of all customers between May 20, 2019 and June 11, 2019. During that 23 day time period, TollFreeDeals transmitted a total of 720,008,294 calls from its customers to U.S. call recipients. TollFreeDeals also provided records to SSA-OIG demonstrating that these roughly 720 million calls were terminated on behalf of 67 unique customers. Those calls originated from more than 133 million unique source numbers, the vast majority of which were U.S. phone numbers. Of those more than 720 million calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. SSA

³ In a Microsoft Refund Scam, call recipients receive a message stating that a tech support company is going out of business and the recipient is entitled to a refund for services previously purchased. Once a call recipient returns the call, a fraudster in a call center convinces the recipient that the tech company's refund department inadvertently refunded the call recipient thousands of dollars, rather than hundreds of dollars. The fraudster then convinces the call recipient to wire money to return the purported refund overpayment.

OIG has learned from discussions with U.S. telecommunications carriers and with employees of USTelecom, that in the telecommunications industry, such high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Calls from Company A accounted for roughly 11% of TollFreeDeals' total call traffic during this 23 day period.

46. Of the more than 720 million calls transmitted by TollFreeDeals during this 23 day period, 24,371,682 were made to phone numbers with area codes locating them within the Eastern District of New York. More than 14 million calls had a duration of less than one second, and more than 22 million calls had a duration of less than 30 seconds.

47. Department of Justice analysts identified the top 1,000 source numbers that sent the highest volume of calls across all TollFreeDeals customers during this 23-day period. Those top 1,000 source numbers combined sent more than 169 million calls, roughly 23.5% of all calls. SSA OIG obtained records related to these 1,000 phone numbers from YouMail and from FTC's Consumer Sentinel database. FTC received complaints regarding 460 of the top 1,000 source numbers, accounting for more than 112 million calls. YouMail records revealed that 441 of the source numbers, accounting for more than 90 million were categorized as scam calls. Based on just these top 1,000 source numbers sending the highest volume of calls, 29 unique TollFreeDeals customers transmitted call traffic from source numbers that YouMail and/or FTC records associated with fraudulent robocalls.

Defendants Provide Toll Free Numbers to Foreign Robocall Fraudsters

48. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free telephone numbers and related services are

provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

49. While toll-free numbers used for return-calling purposes cannot be “spoofed” like outgoing robocalls, the use of a U.S. toll-free number in Defendants’ robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims’ return calls from the United States to the foreign fraudsters’ call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

50. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission (“FCC”) as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers “Responsible Organizations,” that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more responsible organizations.

51. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

We received a call yesterday (at 6 pm) that we didn't answer.

Calling Number: +844[XXXXXXX]
Requesting to call back: 844-[XXX]-[XXXX]

Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

I listened to the audio file, and the statement below is a true and correct transcription of the audio

I heard:

tomorrow \$399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

52. From August 1, 2019, through August 9, 2019, the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded to the effect that he had informed his customer.

53. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

Good afternoon Nick,

I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

54. That same date, Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers. The August 12, 2019, email correspondence referenced in this paragraph is attached as Exhibit 2.

55. On May 11, 2019, Nicholas Palumbo emailed himself a reminder to "Order 10 toll frees" for India-based VoIP carrier Company A.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27th, 2020, in Scottsdale, Arizona.



Marcy Ralston
Special Agent, SSA OIG

EXHIBIT 1

2019-08-14 18:16:02 UTC: Sent Formal email to nick@tollfreedeals.com

USTELECOM

THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Farhan Chughtai, and I coordinate the efforts of USTelecom's Industry Traceback Group. We are writing to request your assistance on industry efforts focused on our shared interests of protecting consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's Industry Traceback Group recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

Please note that the FCC's Enforcement Bureau recently reached out to carriers that were not supporting these traceback efforts (discussed below). In addition, USTelecom has recently initiated an automated system for conducting tracebacks. We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, can you please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please state as such and identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

Regarding this request, USTelecom has a group of members and non-members dedicated to tracing back fraudulent, abusive, and/or unlawful traffic to its source (called the "Trusted Carrier Framework") so that such calls never reach consumers. USTelecom is a 501(c)(3) industry trade association that is coordinating the efforts of the Trusted Carrier Framework. This cooperative framework includes a broad range of industry participants (including ILECs, CLECs, VoIP providers, long distance companies, and wholesale providers), who are working to reduce the number of robocalls consumers receive and help identify their origins. This traceback framework - and others like it - operate under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI).

We invite you to join our industry traceback efforts; there is no cost to do so. Please call or email to have your preferred contact information added to our systems.

Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." Recently the FCC's Enforcement Bureau sent a series of letters - some under its Section 403 investigation authority - to carriers that have been non-responsive to USTelecom's traceback request (see here: <https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf>). The letters "urged" carriers to "cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls."

In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessary incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of USTelecom's Trusted Carrier Framework, disclosure of this information fits within that exception. To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom advises the appropriate law enforcement agencies so that they can take appropriate action against the caller, should they elect to do so. Similarly, if this industry effort fails to trace these calls their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to contact me should you have any questions, or would like to discuss.

Thanks,
Farhan

Farhan Chughtai
Director, Policy & Advocacy
USTelecom - The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
<https://traceback.ustelecom.org/Form/Login/r:REDACTED?t=kF9qfzR7iyG>
(URL is a private login; do not share.)

Call Details for Incident #690 (new)

Date/Time: 2019-08-05 15:07:00 UTC
To: +13013437570
From: +18004038700
Campaign: SSA-BenefitsCanceled

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective.

Call Details for Incident #724 (new)

Date/Time: 2019-08-12 14:03:00 UTC
To: +15864892755
From: +18883716781
Campaign: SSA-Jun2019

Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

Call Details for Incident #723 (new)

Date/Time: 2019-08-12 14:10:00 UTC
To: +12488083416
From: +19562547097
Campaign: SSA-Jun2019
(see description above)

Call Details for Incident #722 (new)

Date/Time: 2019-08-12 14:40:00 UTC
To: +12485055710
From: +19567226365
Campaign: SSA-Jun2019
(see description above)

Call Details for Incident #687 (9d3h ago)

Date/Time: 2019-08-05 14:10:00 UTC
To: +12155344889
From: +18786525758
Campaign: SSA-Jun2019
(see description above)

EXHIBIT 2

On Mon, Aug 12, 2019 at 2:23 PM -0700, "JR Voltaggio" <jr@teli.net> wrote:

Good afternoon Nick,

I wanted to reach out to inform you that we have disabled the account of [REDACTED] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your re-seller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

teli

JR Voltaggio

Customer Success Manager
Office (844) 411-1111
jr@teli.net
www.teli.net

To	JR Voltaggio < jr@teli.net >
From	nick palumbo < nick@tollfreedeals.com >
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:36:58 PM
Subject	Re: Account [REDACTED]
Body	I let him know

To	JR Voltaggio < jr@teli.net >
From	nick palumbo < nick@tollfreedeals.com >
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:37:15 PM
Subject	Re: Account [REDACTED]
Body	I will be porting clients over Can't take that chance

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.

NICHOLAS PALUMBO, NATASHA
PALUMBO, ECOMMERCE NATIONAL,
LLC d/b/a Tollfreedeals.com, and SIP
RETAIL d/b/a sipretail.com,

Defendants.

CV 20 - 473

Civil Action No.

KORMAN, J.

MANN. M.J.

CERTIFICATION PURSUANT TO FED. R. CIV. P. 65(b)(1)(B)

1. I am an Assistant United States Attorney in the Civil Division at the U.S. Attorney's Office for the Eastern District of New York. I make this certification pursuant to Fed. R. Civ. P. 65(b)(1)(B) in support of the United States' application for a temporary restraining order pursuant to 18 U.S.C. § 1345, whereby defendants Nicholas Palumbo, Natasha Palumbo, Ecommerce National, LLC d/b/a Tollfreedeals.com, and SIP Retail d/b/a sipretail.com (collectively, "Defendants") would be enjoined from engaging in an ongoing wire fraud scheme in violation of 18 U.S.C. §§ 1341 and 1349.

2. As set forth in detail in the accompanying Complaint and the Declarations of Special Agent Marcy Ralston of the Social Security Administration's Office of the Inspector General, and Postal Inspector Samuel Bracken of the United States Postal Inspection Service, the Defendants are utilizing the U.S. telecommunications network to participate in an ongoing scheme to defraud through facilitating the delivery of vast numbers of fraudulent telephone calls to victims,

among other fraudulent conduct, resulting in harm to victims throughout the United States, including elderly and vulnerable victims.

3. The Ralston and Bracken Declarations, together with the Complaint and accompanying exhibits, specifically set forth facts showing that the Defendants' conduct subjects thousands of victims to immediate and irreparable financial loss or other harm. The Declarations and Complaint further establish that the frauds are ongoing, and will continue to cause harm to victims during the interval between Defendants being given further notice and the Court's ruling on the United States' application for temporary relief. The Declarations and Complaints establish that Defendants continue to transmit large volumes of fraudulent telephone calls on a regular basis.


4. The temporary restraining order sought by the United States would enjoin Defendants from: (1) committing wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349; (2) providing, or causing others to provide, call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States; (3) providing toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities; and (4) destroying, deleting, removing, or transferring any and all business, financial, accounting, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants. The requested relief would therefore immediately prevent harm to new victims.

5. The Court should not require the United States to provide notice to the Defendants prior to the entry of the requested relief, because notice potentially could allow the Defendants to destroy relevant business records before the parties are heard by the Court. In addition, during the time it would take to give Defendants notice, additional persons could be victimized through Defendants' regular delivery of fraudulent telephone calls through U.S. telecommunications

network, Defendants' provision of toll-free calling services used to further the wire fraud schemes, and through other conduct by Defendants in furtherance of the scheme such as through Defendants' receipt of funds from defrauded victims.

6. Therefore, the United States respectfully requests that the Court issue the proposed temporary restraining order without notice to Defendants.

Dated: January 28, 2020
Brooklyn, New York



DARA A. OLDS
Assistant United States Attorney
Tel. (718) 254-6148
dara.olds@usdoj.gov