UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

DOV ZEITLIN, individually and on behalf of all others similarly situated,

Plaintiff,

-against-

NICHOLAS PALUMBO; NATASHA PALUMBO; ECOMMERCE NATIONAL, LLC d/b/a TollFreeDials.com; SIP RETAIL d/b/a sipretail.com; JON KAHEN a/k/a JON KAEN; GLOBAL VOICECOM, INC.; GLOBAL TELECOMMUNCATION SERVICES, INC.; and KAT TELECOM, INC.,

Defendants.

----------X

Case no.
20-cv-510

COMPLAINT

Jury trial demanded

Plaintiff, complaining of the defendants, by his attorneys, THE BERKMAN LAW OFFICE, LLC, alleges for his complaint, upon information and belief, as follows:

INTRODUCTION

1. The phenomenon of robocalls has become a scourge plaguing our society.

2. For years Americans have been constantly bombarded with robocalls seeking to draw them into all manner of fraudulent schemes with lies and deceit. Call recipients are told that their social security numbers will be "frozen" if they do not cooperate with a bogus investigator who needs money to be sent in immediately, that they will be arrested for money laundering or drug dealing, that they must provide their credit card or banking information, that their car warranties are about to expire, that they need to provide credit card information for cockeyed

reasons, that there are tax liens against them, that they are going to be deported, and the list goes on. Many have been bombarded with pointless calls playing recordings in Chinese, Spanish, and other foreign languages they do not even speak.

3. The problem has become so severe that in 2018 when the Swedish Royal Academy of Sciences called New York University professor Paul Romer to inform him that he had won the Nobel Prize in Economics, he let the call go to voicemail thinking that only a telemarketing call could be coming in at such an early hour. He told the media "I didn't answer the phone because I've been getting so many spam calls. I just assumed it was more spam."

4. Millions of Americans have had their children woken up, had their dinner hour disturbed, have their work interrupted, have been unable to keep their phones on so their families could reach them for fear of having it ring at an inopportune time, have had to put important calls on hold to answer what turns out to be a spam robocall, and have otherwise have had their lives made miserable by spam robocalls.

5. The Defendants in this case are responsible for this scourge. Disregarding all laws, ignoring complaints and warnings, and acting with a selfish quest for mammon regardless of the intrusive burden they placed on their fellow Americans, the Defendants deliberately facilitated hundreds of millions of spam robocalls, while hiding behind false telephone numbers and spoofed caller ID's.

6. In this action, plaintiff seeks justice on his own behalf, and on behalf of all the Defendants' other victims.

7. It is the plaintiff's hope that by imposing a financial cost on the defendants for the wanton aggravation they have caused to millions of Americans, the profit motive will be

eliminated, similar conduct by others will be deterred, and Americans' quality of life can be improved.

THE PARTIES

8. At all times relevant to this complaint, the plaintiff, DOV ZEITLIN ("ZEITLIN"), is a natural person, resident of the State of New York, County of Kings.

9. Upon information and belief, at all times relevant to this complaint, 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 "Palumbo 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.

10. Upon information and belief, at all times relevant to this complaint, 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.

11. Upon information and belief, at all times relevant to this complaint, 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.

12. Upon information and belief, at all times relevant to this complaint, Defendant Kaen resides in Nassau County, New York, in the Eastern District of New York. Kaen controls Defendants Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc., which he uses in furtherance of the fraudulent robocall scheme. Kaen operates the Corporate Defendants as a single enterprise from his home in the Eastern District of New York. One or more of these Defendants also conducts business as "IP Dish."

13. Upon information and belief, at all times relevant to this complaint, Defendant Global Voicecom, Inc. is a New York corporation. The New York Department of State, Division of Corporations Entity Information database identifies Global Voicecom's principal executive office as being located in Great Neck, New York, in the Eastern District of New York, and Kaen as the corporation's Chief Executive Officer.

14. Upon information and belief, at all times relevant to this complaint, Defendant Global Telecommunication Services Inc. is a New York corporation. Global Telecommunication Service's principal place of business is located in Great Neck, New York, in the Eastern District of New York.

15. Upon information and belief, at all times relevant to this complaint, Defendant KAT Telecom, Inc. is a New York corporation. KAT Telecom's principal place of business is located in Great Neck, New York, within the Eastern District of New York.

JURISDICTION

16. This court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, 47 U.S.C. § 227, as well as 28 U.S.C. § 1367.

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

CLASS ACTION ALLEGATIONS

18. This action is being commenced as a proposed class action, pursuant to Fed. R. Civ. P. 23.

19. The proposed class consists of all persons who received robocalls via the defendants' telecommunications services within the four years preceding the filing of this complaint.

20. This proposed class is so numerous that joinder of all members is impracticable.

21. There are questions of law or fact common to the class which predominate over any questions affecting only individual class members.

22. The claims of the representative plaintiff are typical of the claims of the class as a whole.

23. The representative plaintiff will fairly and adequately protect the interests of the class.

24. A class action is superior to other available methods of the fair and efficient adjudication of the controversy.

THE UNDERLYING FACTS

Overview of Robocalling Fraud Schemes

A. Robocalling Fraud Targeting Individuals in the United States

25. Upon information and belief, the robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system every day with millions of robocalls intended to defraud individuals in the United States. Many of these

fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

26. Upon information and belief, foreign fraudsters operate many different schemes targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

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

b. Internal Revenue Service ("IRS") and Treasury Imposters: Defendants transmit recorded messages in which IRS imposters falsely claim that the call 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: Defendants transmit recorded messages in which USCIS imposters falsely claim that the call recipient has failed to fill out immigration forms correctly, the individual faces imminent arrest or deportation, that the individual's home country has taken formal action that may result in deportation, or the individual has transferred money in a way that will result in deportation. When a call recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the individual to pay various fees or fines to avoid immigration consequences.

d. Foreign Government Imposters: Defendants transmit recorded messages in which foreign government imposters, often in foreign languages, falsely claim to be from the U.S.-based consulate of a foreign government and that the call recipient faces problems with immigration status or a passport. When a call recipient calls back or connects to the fraudster, the fraudster falsely claims that the individual must pay various fees or fines in order to avoid immigration consequences such as deportation.

e. 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 call 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.

27. Upon information and belief, 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, from local police departments, 911, or from 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 callers' 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.

28. Upon information and belief, individuals who answer or otherwise respond to 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 for safekeeping to the government agency the fraudsters are impersonating. The fraudsters often

claim that the victim's payment will be returned to them 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.

29. Upon information and belief, 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]-[X:XXX] I repeat 619-[:XXX]-[X:XXX] thank you.

30. Upon information and belief, 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 for 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposter calls, with estimated 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.[1] Complaint numbers

[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.

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

31. Upon information and belief, 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 ofU.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.

32. Upon information and belief, 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 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 tracing process as "traceback."

33. Upon information and belief, 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

34. Upon information and belief, since at least 2016, the 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. telephone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling the fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

35. Upon information and belief, 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 calls passing through their systems by the millions; thousands of spoofed calls purporting to be from "911" and similar numbers originating from overseas; dozens of complaints, warnings, and inquiries from vendors and other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from an industry trade group about the scam robocalls passing through

the Defendants' system; and receipt of numerous complaints from common-carrier telecommunications companies whose customers were victims of these fraud schemes.

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

36. Upon information and belief, 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. Defendants regularly transmit massive volumes of such calls. For example, a Government investigation has revealed a sample of more than 7.7 million calls that Defendant Global Voicecom routed through a single downstream VoiP carrier over 19 days in May and June 2019, months after Kaen's response to the FCC. Of those calls, approximately 86%, more than 6.6 million calls, were one second or less in duration, indicating exceedingly high levels of junk and fraudulent robocalls. Moreover, a small sample of approximately 330,000 of these calls was examined in greater detail; of these approximately 330,000 calls in that 19-day period, more than 270,000 (approximately 81%) were from source numbers (the numbers appearing on the recipients' caller IDs) identified as fraudulent robocalls. Similarly, of the more than 106,000 robocalls spoofing the SSA's toll-free customer service number in January and February 2019 that Defendant Global Voicecom transmitted into the United States, nearly 60% had a call duration of less than one second, and another 38% were between one and 60 seconds in duration. During that same period in January and February 2019, Defendant Global Voicecom also ran through its systems thousands of calls spoofing 911, 1911, and 11911, with similar short call durations.

37. Upon information and belief, 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.

38. Upon information and belief, 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!"

39. Upon information and belief, 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."

40. Upon information and belief, 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.

41. Upon information and belief, 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.

42. Upon information and belief, 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.

43. Upon information and belief, 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.

44. Upon information and belief, in February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a US CIS 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 US CIS 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.

45. Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

46. Upon information and belief, 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 US CIS 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.

47. Upon information and belief, in every case, either the email itself or the traceback pmial 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 transmitted spoofed US CIS calls in 2017.

48. Upon information and belief, despite repeated warnings from AT&T that this foreign VoiP canier 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.

49. Upon information and belief, the Palumbos have also received numerous warnings from telecommunications industry trade association US Telecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

50. Upon information and belief, from May 2019 tluough 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 US CIS 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.

51. Upon information and belief, 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.

52. Upon information and belief, since 2017, significant numbers of fraudulent robocalls have been traced back to the Defendants and brought to their attention. For example, U.S. common carrier AT&T has notified Defendants on numerous occasions about fraud traced back to Defendants' operations. These notices include a November 16, 2017, email to IP Dish:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigration[ ] Services personnel and defrauded an AT&T customer of $1,450.... Pursuant to the customer and carrier network fraud protection provisions of the

> Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

53. Upon information and belief, AT&T sent similar emails about USCIS impersonation scams to Defendants Kaen and Global Voicecom in September 2017, November 2017, April 2018, and July 2018. Similarly, AT&T emailed Defendants about SSA and other imposter robocalls on January 29, 2019:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration....
>
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications....
>
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

54. Upon information and belief, AT&T sent similar warning notices about SSA imposter calls to Defendants Kaen and Global Voicecom in February 2019 and May 2019.

55. Upon information and belief, another VoiP carrier that received call traffic from Defendants, Peerless Network, Inc., sent even more warning notices and inquiries to Defendants. For example, Peerless Network sent a warning notice about spoofed calls in September 2018 with a request that Defendants investigate and "take the appropriate action." Peerless Network sent approximately 12 of these warning notices between September 2018 and March 2019.

56. Upon information and belief, not only have other telecommunications companies provided warnings and notices to Defendants as a result of tracebacks, but a leading industry

trade group, USTelecom, has done the same. For example, USTelecom traced back an August 19, 2019 robocall that originated from India and came through Defendant Global Voicecom as the gateway carrier. The robocall was also routed through Defendant KAT Telecom. This robocall stated that there was "suspicious activity" associated with the individual's social security number. USTelecom provided the following warning notice in its correspondence to Defendant Global Voicecom on August 27, 2019:

> 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 8 is not effective.

57. Upon information and belief, blocking specific telephone numbers is an ineffective means to stop fraudsters who are willing- and have the ready ability-to spoof any number as the caller ID number for their fraudulent robocalls. For example, in January and February 2019, Defendants transmitted fraudulent robocalls spoofing 911, 1911, and 11911. Nevertheless, if the Defendants responded at all to these notices and warnings from other telecommunications-industry actors, they routinely responded that the "offending" number had been blocked, as though the spoofed telephone number and not the caller were responsible for the fraud.

58. Upon information and belief, similarly, USTelecom traced an October 3, 2019 robocall to Defendant Global Voicecom as the gateway carrier. This robocall also originated from India. USTelecom provided the following warning notice in its October 11, 2019 correspondence to Defendant Global Voicecom:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Calls placed from specific numbers obtained by scammers, using an automated

> voice to inform called party that they are in trouble with IRS and will be arrested. Called party is instructed to call back to speak to an agent. .. We are using traceback to try to find the source(s) of the millions of outbound calls that are being made to initiate the scam.

59. Upon information and belief, USTelecom's records indicate that this robocall was transcribed in part as follows:

> This call is from Federal Tax and audit division of internal revenue services. This message is intended to contact you regarding an enforcement action executed by the US treasury intending your serious attention. Ignoring this will be an intentional second attempt to avoid initial appearance before a magistrate judge or a grand jury for federal criminal offense. This is a final attempt to reach you to resolve this issue immediately and to speak to a federal agent to call us back on 510-[XXX]-[XXXX]. I repeat 510-[XXX]-[XXXX].

60. Upon information and belief, USTelecom identified Defendants as the gateway carrier for foreign fraudulent robocalls on at least eighteen other occasions in the latter half of 2019 alone, each time providing similar warning notices about the nature of the scam robocalls. USTelecom's records indicate that on nearly all of these 2019 tracebacks, the scam robocalls came from the same company in India.

61. Upon information and belief, Defendants transmitted another group of fraudulent robocalls that· spoofed the phone number for a foreign government consulate in New York, New York. These calls conveyed foreign-language messages about problems with the individual's immigration status or passport. Like with SSA imposter robocalls and other U.S. government-imposter scams, individuals who returned the calls to the consulate imposters were told lies intended to frighten them and make them think there are imminent consequences for involvement in criminal activity, and that funds must be transferred to the fraudsters to resolve the matters. Like with the SSA imposter scams, once the fraudsters are convinced they have extorted as much money as possible, they drop all contact with the victim. In 2018, the FCC

traced this consulate imposter scam back to Kaen and IP Dish, who informed the FCC that the calls came from a Hong Kong entity that was making tens of thousands of calls per day. The FTC's Consumer Sentinel database reflects more than 1,000 complaints related to the spoofed phone number of the consulate. These complaints relate hundreds of thousands of dollars in victim losses. Defendants continue to conduct business with this Hong Kong entity more than a year later.

62. Upon information and belief, despite these notices and numerous others, Defendants continue to pass fraudulent robocalls into the U.S. telephone system to millions of U.S. telephones every day.

B. Defendants Provide Return-Calling and Toll-Free Services for Robocall Schemes

63. Upon information and belief, 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 and direct-inward-dial ("DID") 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 actually a telephone number that Defendants register to an internet address designated by the foreign fraudsters. Thus, the DID and toll-free numbers can be used to ring telephones anywhere in the world.

64. Upon information and belief, while DID and toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. DID or toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing-deception.

The DID and 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 hundreds of these DID and toll-free numbers and associated calling services to foreign robocall fraudsters.

1. DID Numbers Used to Further Robocalling Fraud Schemes

65. Upon information and belief, like telephone numbers used to make U.S.-bound robocalls, DID numbers can be traced to identify their providers and users. This process was used to identify DID numbers provided by the Defendants for use in the fraudulent robocall schemes. For example, records obtained from one U.S. company demonstrate that it assigned 902 DID telephone numbers to Defendant Global Voicecom. Approximately 55% of these DID telephone numbers are associated with more than 28,000 complaints in the FTC's Consumer Sentinel database. One of the 902 DID telephone numbers appeared in a robocall sent to millions of U.S. telephones in early 2019:

> 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.

66. Upon information and belief, at the time of the robocalls, this DID telephone number was assigned to Defendant Global Voicecom, which used that DID telephone number to provide return-calling services to the overseas fraudsters. Individuals who return calls like these put themselves in a pool of likely victims, insofar as the individuals self-select through belief that the message was sufficiently credible to warrant a return call. Upon returning the call to 619-[:XXX]-[:XXXX], individuals were told that they were speaking to SSA agents, who offered to

resolve the purported problems that prompted the call by way of immediate payment of funds. In reality, the person speaking to the individual was a fraudster, unaffiliated with the U.S. government.

67. Upon information and belief, beginning as early as September 2017 and continuing through the present, the U.S. company that assigned these 902 DID numbers to Defendants provided numerous warning notices about how the numbers were being used to perpetrate fraud. For example, that company provided the following warning notice to Defendant Global Voicecom on September 13,2017 and included the substance of several complaints about fraud:

> The DID: 847[XXXXX:XX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[:XXX]-[:XXXX] claiming that I was a subject of Treasury Fraud. [T]hey said to call back at 847-[:X:XX]-[:XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury regarding tax fraud in my name. The call back number was 847-[XXX]-[:XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.

68. Upon information and belief, the voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the [U.S.] treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to

reach us is 847-[X:XX]-[:XXXX], let me repeat the number 847-[X:XX]-[:XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

69. Upon information and belief, through the course of the ensuing years, Defendants continued to receive numerous similar warning notices about DID numbers and related services they provide. Defendants effectively ignored the warnings and never terminated the fraudsters' access to DID numbers for return calls.

70. Upon information and belief, in the course of a Government investigation, SSA OIG agents obtained from Global Voicecom call records for seven of the 902 DID numbers assigned to Defendant Global Voicecom that are associated with SSA imposter robocalls. According to Defendants' own records, Defendants provided these seven DID numbers to the same Indian entity that Defendant Global Voicecom identified to USTelecom as the gateway carrier for numerous government imposter scam robocalls.

71. Upon information and belief, these DID call records reveal that more than 10 million calls were placed in 2019 from more than 4.5 million unique phone numbers to the 902 DID numbers assigned to Defendant Global Voicecom. More than 240,000 of these calls were from area codes for the Eastern District of NewYork.

2. Toll-Free Numbers Used to Further Robocalling Fraud Schemes

72. Upon information and belief, records from the FTC demonstrate that Defendants Global Voicecom and Jon Kaen are associated with more than 1000 October 2019 SSA-imposter robocalls to the FTC's offices. These robocalls appeared to originate from a toll-free telephone number. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. 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. On October 23 and 24, 2019, the FTC's offices received approximately 1,000 robocalls with the following recording:

> ...social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877-[:XXX]- [XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

73. Upon information and belief, the toll-free 877 number appeared on the FTC's caller ID as well as in the actual robocall message as the return-call number. On October 24, 2019, an FTC investigator contacted Somos to determine which responsible organization was associated with that toll-free number, which Somos duly provided. The FTC investigator then contacted that responsible organization, who informed the investigator that the number was assigned to Defendants Global Voicecom and Jon Kaen.

74. Upon information and belief, that responsible organization provided numerous notices to Defendants concerning the toll-free numbers assigned to Global Voicecom and how they were being used to facilitate robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[:XXX]-[:XXXX] and were asked to disconnect it. We dialed this number and found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[:XXX]-[:XXXX], which we see i[s] assigned to your account. This number was

reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XxX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" To each of the dozens of notices, Defendants responded to the effect that the "offending" number has been blocked, as if the spoofed telephone number and not the caller were committing fraud, but never that they terminated the sources of the fraudulent robocalls.

75. The FTC's Consumer Sentinel reflects more than 1,400 complaints associated with the toll-free numbers assigned to Defendant Global Voicecom.

76. Upon information and belief, 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.

77. Upon information and belief, 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.

78. Upon information and belief, 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.

79. Upon information and belief, 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-[XX:X:]-[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 fi·audulent calls from the same customer account will result in termination of said customer account. The number of 844-[XX:X:]-[X:X:XX] has been removed from your account in order to protect the integrity of our network.

80. Upon information and belief, 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 l-

> 844-[XX:X:]-[XX:X:X]. I'll repeat the help line number 1-844-[XX:X:]-[XXXX]. Thank you.

81. Upon information and belief, 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.

82. Upon information and belief, 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. Unfmiunately, 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.

83. Upon information and belief, 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

84. Upon information and belief, Defendants' fraudulent schemes have caused substantial harm to numerous victims, 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.

85. In addition to the massive cumulative effect of these fraud schemes on U.S. victims, 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.

86. 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.

Government Action

87. The Government has filed two actions on these facts, *USA v. Palumbo, et al.*, EDNY case no. 20-cv-473, and *USA v. Kahen, et al.*, EDNY case no. 20-474.

AS AND FOR A FIRST CLAIM FOR RELIEF

88. Plaintiff repeats and re-alleges each of the foregoing allegations with the same force and effect as if more fully set forth herein.

89. The plaintiff, and each member of the proposed plaintiff class, has received numerous robocalls which, upon information and belief, were carried, processed, connected, placed, routed, and/or facilitated by the defendants and/or the agents, servants, employees, and related entities.

90. By their conduct, Defendants have violated the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227.

91. The depth and breadth of Defendants' violation of the TCPA is astonishing, as it continued for years, involved hundreds of millions of calls, and continued despite multiple complaints, inquiries, and warnings, and thus could only have been deliberate conduct.

92. Defendants disregarded all laws and regulations, ignored do-not-call lists, and acted with complete lawlessness.

93. Pursuant to the TCPA, Plaintiff, and each member of the plaintiff class, may recover the greater of actual damages or $500, and the Court may, in its discretion, increase the amount of the award up to three times that amount.

94. The defendants are jointly and severally liable.

95. By reason of the foregoing, Plaintiff, and each member of the plaintiff class, is entitled to recover the full extent of his damages, in an amount to be determined by the jury at trial.

JURY TRIAL DEMANDED

96. Plaintiff demands a trial by jury of all issues triable to a jury.

WHEREFORE, the plaintiff demands judgment against the defendants in the amounts and for the relief requested herein, plus attorney's fees to the extent permitted by law.

Dated: Brooklyn, New York
January 29, 2020

Yours,

THE BERKMAN LAW OFFICE, LLC
Attorneys for the plaintiff

by: _____
Robert J. Tolchin

111 Livingston Street, Suite 1928
Brooklyn, New York 11201
(718) 855-3627