Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the matter of:	)	
	)	
SECOND REPORT AND ORDER AND SECOND FURTHER NOTICE OF PROPOSED RULEMAKING:	)	WC Docket No. 20-67
	)	
Implementation of TRACED Act Section 6(a) —Knowledge of Customers by Entities with Access to Numbering Resources	)	

REPLY COMMENTS OF THE
SECOND REPORT AND ORDER AND SECOND
FURTHER NOTICE OF PROPOSED RULEMAKING

Marlene H. Dortch,
Secretary, Federal Communications Commission
Office of the Secretary
45 L Street NE, Room TW-A325
Washington, DC 20554

These comments to FCC-CIR202309-03 are respectfully submitted for the FCC's and the Public's consideration. The comments, herein, is a combination of feedback and suggestions in support of *Bandwidth.com's* response cited on page 11, FN 63*:* "the bulk of the proposed rules are reasonable and appropriately targeted toward preventing potential abuses that harm the public interest while simultaneously continuing to encourage innovative and wanted services", which is specifically related to *WC Docket No. 20-67* ("Implementation of TRACED Act Section 6(a) —Knowledge of Customers by Entities with Access to Numbering Resources").

***

We appreciate the Commission's hard work toward ensuring that important numbering resources are appropriately and properly made available to companies and consumers in a manner that fosters further advancements toward economic and technological benefits. The summary of the suggestions to further encourage good stewardship of those resources are found on paragraph thirty-four (34).

***

I, Aaron Woolfson, state and declare as follows:

1. My name is Aaron Woolfson. I am the founder of TelSwitch, Inc.[1] which was established in 1994. Over the last twenty-nine (29) years, TelSwitch, Inc. has operated as a Provider of Telecommunications Related Service ("PTRS"), as both a carrier and a provider of billing and switching services[2]. TelSwitch, Inc. respectfully submits this response to the FCC's planned rulemaking related to whether further restrictions upon the assignment of numbering resources, or telephone numbers("DID's") by VOIP carriers is necessary.

2. Our response, or comments, is directed specifically toward the FCC's inquiry on those DID's that serve as "virtual phone numbers" and are those that are offered for incorporation into products or services, such as Google Voice. Such products, especially those that offers a second line that is mutually exclusive of the phone number that may have otherwise been assigned to it, are essential in the advancement of work-at-home flexibility, and responsiveness to customer inquiries.

3. Typically, those companies that offer second-number products obtain their DID's, or telephone numbers, from companies such as *Bandwidth.com*, *Peerless*, etc. While there are hundreds of products and services that depend upon the incorporation of DID's built into software and services, there is one common denominator – the DID. And those DID's must be obtained

---

[1] California C-type Corporation (C1888360).

[2] Certificate of Public Convenience and Necessity ("CPCN") U-5410-C was granted on June 10, 1994 (Decision 94-06-022). U-7327-C (Decision 17-07-009) was granted on July 13, 2017. Tel-One Network Services now operates as a stand-alone company headquartered in San Francisco.

from *somewhere*. Colloquially known as Software as a Service ("SAAS"), companies that offer these "second line" and "consolidated or virtual communications" products, companies such as *Twilio*, *Salesforce*, *Talkdesk*, *Dialpad*, *Five9's*, etc. rely upon readily available DID's for incorporation into their products. The DID's are essential to the fabric of commerce and the continuity of business.

4. Unfortunately, other uses of the DID's – the use cases that generate the most annoyances, unsurprisingly involve high volumes of junk calls that are placed in quick succession by spammers[3], scammers, and robo-callers. And they result in *lots* of short duration calls, or calls that result in the delivery of pre-recorded message. Calls that, is answered, often are intended to impersonate those companies or organizations with which consumers would typically interface with, such as Social Security, Banks etc. This is done in order to entice those unsuspecting consumers to provide the caller with personal information.

BACKGROUND:

5. DID's have traditionally been used in connection with services ordered from "Phone Companies" for the purposes of making calls into, or receiving calls from the Public Switched Telephone Network ("PSTN"). However, those days are long gone. Now, anyone can order a DID from any vendor. And for any purpose. Those DID's, once assigned by phone companies and provided for use with landline phones purposed with making calls to or accepting calls from customers (or prospective customers), or cellphones, were a lifeline between companies and their customers, or individuals and other individuals. In sum, the DID's were used for legitimate purposes, and the telephone numbers from which the calls were made could be trusted.

6. Now while DID's can be used for many other purposes, including work-at-home offices, second lines, and AI driven help-bots such as those offered by *TalkDesk*, they can also be used by scam farms creating massive quantities of calls into the public switched telephone

---

[3] SPAM is the trademarked name of a canned meat product ("spicy meat and ham") that was first produced by Hormel Foods Corp. ☺

network in the hopes that an unsuspecting member of the public answers that call and provides personal or financial information. Essential services are being drowned out by a the continuous annoyance of unwanted calls involving scams and schemes to defraud us.

DID's ARE AGNOSTIC AND CAN BE USED FOR ANY PURPOSE.

7. At one time DID's were the sole and exclusive domain of the "Telephone Company". They were assigned to a customer, by the telephone company, and the DID's were associated with all calls that the customer made from those lines to which they were assigned. Calls were expensive so that unnecessary (or junk) calls were just simply not made. Besides, they could be easily traced, by the telephone company, to their source.

8. Now, however, DID's are agnostic and are not differentiated from one another based upon, the different types of services for which they are being used. Simply observing a DID on a handset is meaningless because there is really no way to determine whether the call is being received from a doctor's office, a school, or a scammer. They traverse different networks, and can originate *from* literally anywhere.

9. Making matters worse, bad actors can commandeer a number and use it for any purpose they want, even if the number belongs to a legitimate customer and that customer has no relationship with the DID vendor. Nothing can be done. For instance, there are no technical hindrances to commandeering Delta Airlines' number, and calling everyone in America to tell them that they may upgrade their flight to first class for $50.00, with the only purpose of obtaining financial information from those who have answered the phone[4].

10. And since it is neither the DID vendor's fault nor that of Delta Airlines, there is not a lot that can be done to prevent it.

//

//

---

[4] If this made you uncomfortable reading, it made me uncomfortable writing it. That's why it is imperative to stop these types of scams.

SCAMS HAVE PROLIFERATED BECAUSE OF CHEAP INTERNET AND EASY TO OBTAIN DID'S.

11. With the prolific availability of quality internet, DIDs, can be used for any purpose, by anyone, anywhere. And accordingly, the use of DID's has proliferated, turning the telecommunications landscape into a homogenization of not just legitimate calls, but also side-hustle scammers and wide scale organized crime schemes involving impersonation. The American public has been left with an eroded sense of trust in the PSTN.

12. With trust eviscerated, Americans are less likely to answer a call than ever. As described, a few bad actors have complete disregard for the TCPA and have commandeered the phone network for use with scams and schemes, all the meanwhile catalyzing the entire country into not picking up the phone. And there can be huge customer impacts of not answering a call from your doctor or your child's school in an emergency situation.

THE ORIGINAL PROVIDER OF DID's – THE TELEPHONE COMPANIES:

13. In the past, there were four types of telephone companies that offered DID's for use by consumers. These were Local Exchange Carriers ("LEC"), Independent Local Exchange Carrier ("ILEC"), Competitive Local Exchange Carriers ("CLEC"), and later on, wireless carriers. Businesses who wanted telephone lines had either twisted copper pair, typically referred to as a "1MB" line, where each pair of copper serviced one telephone device, or a Centrex service, by which multiple telephone lines were associated with one DID that allowed multiple phones to make calls and accept calls at the same times. Larger users, such as call centers, generally used more sophisticated digital services, so that they could maintain far greater number of simultaneous telephone calls over the same "multiplexed" facilities.

14. The facilities, usually T1's (or multiples of T1's, bundled together in a digital transmission format called a DS3's which carried twenty-eight T1's) were provided by the phone companies and were tied to an actual DID (or DID's) that were *hard wired* to a particular "Trunk Group".

15. As calls were initiated by call centers. stock brokerages, banks, and collection agencies, those digital facilities would carry the call into the phone network, and along with the

call, would assign the DID that was associated with the T1 upon which the call was conveyed.

16. As the call entered the phone network, the Class-4 switches that supported the trunks would attach that DID to the telephone number, and the call would be routed to the destination through a network of "access tandems" by which the calls would traverse. This made tracing the calls back to the source of the call, or the company making it, very simple. In fact, as easy as looking at the telephone number, determine which phone company handled the area code and prefix ("NPA/NXX") associated with that DID. And if you needed to know that the name of the company making that call, you could call the phone company or go to the library. And the information, published in phone directories and online resources, was readily available and easily accessible.

DID's ENTER THE AGE OF THE INTERNET AND PACKET BASED SWITCHING.

17. Once the internet became fast and reliable enough to support the quality of connection necessary to handle voice telephony traffic, providers started using packet switching mechanisms to transmit calls between one another. But not to end-users.

18. This efficiency allowed the telephone companies to save enormously. Rather than telephone companies being required to maintain facilities sufficient to support a N+1 usage scenario by having no less than *one more* telephone circuit available than the *maximum* number of calls that could traverse that route, packet based switching allowed telephone companies to apply *statistical* multiplexing to the packets of voice, and to send those packets of voice between one another using simple "IP" network routers with links between one another[5].

19. Eventually some clever companies recognized that they could install IP routers, such as the Cisco 2620, inside of telephone companies' central offices, and obtain DID's from the phone companies directly using zero-mile T1's[6], and then convert those DID's to packet, or VOIP,

---

[5] What we called VOIP now really was, a long time ago, simply called "packet switching of voice" and was commonly referred to as packet-based-voice.

[6] A zero mile T1 is basically an intra-central office telephone connection with a zero-mileage cost component

and extend them out to their customers via standard internet connections. It was an instant hit, and a cottage industry of VOIP gateways was born, including Asterisk and FreeSwitch, which allowed DID's to be obtained from the phone company using T1's, and extended to the customer premises using VOIP[7].

20. Not to be left behind in the transition, the big phone carriers also recognized that they too could simply offer the same solutions. In doing so, the "phone companies" could maintain the telephony in its' packetized form and transmit it directly in that form to the end-users, and could solve all sorts of technical challenges, and enjoy a heightened set of cost efficiencies in the process.

21. By pushing the packet-based voice traffic all the way to customers' premise using the public internet, PBX applications running on Asterisk, or Cisco Call Managers were able to handle the expanded business needs of companies that could previously only be delivered on high capacity digital facilities, some of which took weeks or months to install. And telephone companies were happy too. Telephone companies were able to depart from the capacity constraints that were, for nearly forty years, limiting the volume of calls that they could support, and companies were elated. By removing the T1's, which were originally configured as 23B+D and allowed only 23 voice channels (and one data, or control channel, per T1), and placing that traffic over VOIP, the transition empowered customers with an immediate and unlimited expansion capability. Customers could quickly adapt to their growing communications needs with elasticity, and well, phone companies would experience more traffic. Not only could call centers and other high volume users, such as airlines, instantaneously ramp up to meet the higher demands, they could drop expensive T1's. But there was an even larger benefit.

AN UNINTENTIONAL CONSEQUENCE OF PUSHING DID's OVER VOIP.

22. As a consequence of the transition to VOIP, one of the largest advancements in

---

[7] Telephone companies pushed back on the new VOIP "cottage industry", stating that among other problems that would occur, 911 would not be able to reliably identify from where a call was originating. As with many other concerns, these too would pass.

communications technology in the last twenty years occurred. The telephone numbers from which a company made or received their calls was no longer connected to the geographical area in which the companies were located. Because of VOIP, a company in Des Moines, Iowa could accept a call from a customer in California who dialed a local number in Palo Alto. Conversely, that same company in Des Moines, Iowa, could place a call to a customer in San Jose using the DID that was hosted our of Palo Alto

23. Phone companies were delighted because they could service more customer traffic, and dramatically improve their models of network efficiency. Similarly, companies were elated because they could maintain a higher level of control over communication costs by dropping T1's (and DS3's), while responding to more customer client interactions from less locations. It was a panacea of technology meets expectation meets practical, real world applications meets cost savings and efficiencies.

24. Unfortunately, call scammers also recognized that they could use these internet enabled platforms with VOIP delivered DID's to be make a lot of calls. And traffic blew up on the network and eroded the trust of the American consumer.

25. When the big phone companies had control over the services and were responsible for attaching the DID on outbound calls on behalf of the customer customers, there was a presumption that a displaying a number from the calling party was actually the person who was calling.

26. And there was accountability. Companies whose numbers appeared in the outbound telephone number portion of the caller ID display had to maintain equipment that was capable of also accepting call-backs to those DID's. But with the advent of VOIP, outbound calls could then be made using the DID from one vendor using the outbound trunks or network facilities from another vendor. And with a combination of traditional T1 and VOIP connecting the outbound calls to individuals using one route while accepting the inbound calls (or not accepting them) from the DID vendor in another, the causation between an outgoing call and an incoming call was lost.

PROLIFERATION OF DID'S HAS LED TO A CRISIS OF CONFIDENCE.

27. The use of, and wide consumer acceptance of telephony services that are portable, such as those offered by Google Voice for a second line on a cell phone, has become a part of the collective societal experience. The use of VOIP carriers, and easily obtainable DID's from *any* city anywhere being used to engage with us has become main-stream. We generally accept that, if we are *expecting* a call, but don't quite precisely know from where that call is arriving, that we will accept that call.– especially those who are expecting calls from doctors' offices, employment agencies, airlines etc. And scammers know that the psychology behind this.

28. And despite the fact that DID's are not guaranteed, or even assured to be associated with the individuals or companies in which we have placed our trust, we still continue to answer the phone. And while chances that any particular person will answer, and respond to, any particular call from any particular scammer are relatively small, quantities of calls do matter. And a lot of them are being made. And being made by those who understand that the TCPA generally doesn't apply to them – because they won't get caught.

29. But if DID Providers take a few measurable steps, and I think that most will be willing to undertake them, a significant step in toward the further abatement of the fraudulent calls can be accomplished. In sum, I do not believe that the DID vendors should be punished for the activities of those who commandeer their numbers.

30. The summary of recommended enhancements, which are discussed in further detail within this submission, are intended as suggestions as to how to further advance the effectiveness of the FCC's and the FTC's TCPA abatement efforts, while minimally impacting DID vendors.

NONE OF THIS IS THE FAULT OF THE DID VENDORS.

31. The FCC's proposed desire to attribute more accountability to the DID Providers for the DID's that they provide to their end users is a welcome advancement in policy, but it is does not solve the problem that DID's will be spoofed, or that bad actors will obtain numbering resources. Simply, the VOIP providers should not be punished for the actions of the scammers who have commandeered their DID's in order to engage in fraud – the FCC should give more capabilities to consumers and telephone companies and providers of services to fight scam calls.

SUGGESTED IMPLEMENTATIONS THAT WOULD BE MINIMALLY IMPACTFUL ON DID PROVIDERS, AND WOULD SOLVE MUCH OF THE FRAUD PROBLEMS.

32. The DID Providers are masterful facilitators of communication. There are so many great solutions to industry challenges that have been facilitated because of VOIP and readily available DID's. Those companies who are providing essential network elements have brought forth some of the most recognizable technological improvements in modern history – literally equalizing the cost and efficiency of communication, fostering business relationships through enhanced methods of communications, and engaging in further human contentment. If we didn't have DID Providers, for example, we would not be able to take business calls from home without installing a separate line. We would not have programs that allowed us to answer our calls away from the office on secondary lines on our cell phone. Politicians could not quickly ramp up for campaigns. Radio stations could not temporarily increase capacity for contents. Reverse 911 systems, that quickly sent massive amounts of emergency notifications, simply would not be possible.

33. In sum, DID Providers are an essential part of the telecommunications infrastructure, and as a matter of public utility should not be punished for the actions of a few bad actors. These DID providers should be encouraged to continue to offer their services in the *same* manner that they are now – with a few enhancements that will provide additional emphasis on the *existing* mechanisms, which should result in a further reduction in TCPA violative calls, while allowing DID vendors to continue to service their customers without further restrictions or encumbrances.

//

//

//

//

//

//

***

34. TelSwitch, Inc. respectfully submits these comments for consideration related to the inquires, or points of discussion, that appear on page thirty-six (36) of the Commission's proposed rulemaking:

> (1) how interconnected VoIP providers that obtain direct access to numbers are using those numbering resources today, including, for example, the extent to which they use numbers obtained in a state to serve the customers of that state, the extent to which they use numbers obtained via direct access to provide non-interconnected VoIP service, and the extent to which numbers obtained via direct access are resold to other providers;
>
> (2) those uses in terms of compliance with the Commission's robocalling, Access Stimulation and other rules, area code exhaustion, and other public interest concerns, including potential consumer benefits or competitive harms of increasing the availability of direct access to numbers or placing more limits on the use of numbers obtained via direct access; and
>
> (3) possible options for mitigating any identified adverse impacts on consumers of number disuse, misuse, and resale, and how any Commission-imposed requirements for, or limits on, number use or resale would impact consumers, providers, and competition.

<u>Publicly available contact information for consumer reporting of fraud.</u>

(a) DID providers should be required to publish an email address or other contact information that is readily available and accessible on the DID Providers' websites so that consumers who receive calls from those DID's can lodge complaints to those vendors. Companies such as *bandwidth.com* and *Peerless Networks* already have been doing this for years, and are extraordinarily responsive to reports of fraud.

<u>DID Providers should be able to tag DID's as fraud while investigating.</u>

(b) DID Providers who receive reports of fraud should be explicitly allowed to investigate and suspend (or shut down) those DID's that are originating suspect traffic. This means tagging the CNAM with "potential scam", and details of those fraud reports should be immediately reported to the US Telecom Traceback Group, who has the ability to cross-reconcile outbound calls using those particular DID's with the VoIP providers who are enabling those calls.

<u>DID Providers should further engage the Do-Not-Originate database.</u>

(c) DID Providers should be encouraged to place those DID's that are under investigation on the Do-Not-Originate list while investigations are ongoing by the US Telecom Traceback Group,

without any repercussions to the DID Provider.

Networks need to expedite data to US Telecom's Traceback Group:

(d) Too much fraud is due to DID's being used for outbound calls on one network which is disparate from the network related to the DID itself. Any network that experiences more than 25,000 outbound calls in a day that are traversing its network from a particular DID should be reporting that activity to the US Telecom Traceback Group.

CNAM Databases should report high-volume CNAM lookup numbers to the US Telecom Traceback Group.

(e) CNAM Database Vendors should be encouraged to provide the US Telecom Traceback Group with notification of any DID that resulted in either (a) 25,000 CNAM look-ups per day, or (b) 100,000 or more lookups in that month. That DID should be immediately flagged for investigation[8].

This will allow for quick identification of those DID's that are generating lots of traffic, and should be useful in cross-comparing telephone numbers to the lists of fraud reports and shutting down the calls.

Establish thresholds for excessive CNAM dips. DID's that are deemed by the US Telecom Traceback Group as being used to generate fraudulent calls should not be allowed to receive any type of compensation based on call volumes.

(f) DID vendors that exceed certain thresholders should receive NO revenue from the CNAM providers, and those monies should be forfeited to the USAC to be tagged with further advancement of TCPA abatement effort.

Reduce the cost of the FTC's DNC database.

(g) As identified by the esteemed attorney Eric Troutman, the DNC database should not cost $26,000 a year – to make it truly useful for everyone, make it free. Or so low cost, that companies would find it unreasonable to not subscribe and use.

I would be surprised if the cost of operating the entire DNC database would cost more than $280,000 a year and I hope that

[8] There are also ways that the CNAM vendors can tag calls, for instance, that incur more than 10 CNAM lookups per second, etc.

TelSwitch, Inc. will have the opportunity to bid on it at some point.

Assist consumers in reporting illegal use of DID's to Providers by creating an access portal for consumers to access the DID database in the same manner as it was available to consumers prior to Local Number Portability[9], [10]

(h) DID vendors are generally unaware that their numbers have been commandeered because those calls traverse different outbound networks than those that are maintained by the DID vendors. Consumers should be able to easily identify the DID vendor, so that the consumer can reach out to them, and in turn, the DID vendor could notify the US Telecom Traceback Group[11].

This would allow the quick identification of the providers of the DID's that are being used to generate fraudulent traffic and/or calls that are violative of the TCPA, so that consumers can easily and readily lodge complaints to those respective providers.

---

[9] FCC order FCC-15-35A1 (03/27/2015) explicitly mandated *continued* availability of iConnectiv's data for purposes of compliance with the TCPA. (¶.142). The historical information *does not* contain subscriber information, only carrier of record and line type. Before number portability, this would have been a simple task of looking at the Local Exchange Routing Guide ("LERG"), or absent access to the LERG, finding the area codes and prefixes from an online collection of national phone books.

[10] In *Perrong v Call Identified as Connor* (Case No. 1:22-cv-04479-CPO-EAP, DC, New Jersey, Camden Vicinage), "plaintiff has queried the database of iconectiv [sic], the company charged by the Federal Communications Commission to administer the Number Portability Administration Center, which is the master database which lists which telephone provider services a particular number, among other information required to route telephone calls to the proper provider" (ECF 3)

[11] If unopposed by the FCC, TelSwitch, Inc. desires to support this effort by making a publicly-available *free* DID provider look-up website that should be as easy as looking up an ISP by IP address. The website would be subject to the same availability restrictions as the FTC's website (*www.telemarketing.donotcall.gov*) which allows individuals to check whether particular numbers are on the DNC list. While being *free* for non- commercial users, any commercial users would be subject to the terms and conditions of TelSwitch, Inc.'s resale agreement with iConnectiv. Note: TelSwitch, Inc. maintains PCI-DSS compliance, and follows best practices surrounding the data security TelSwitch, Inc. does not maintain information related to routing, nor does it maintain any customer information, nor any information that would pose any risk to the core or peripheral routing of phone calls.

***

35. The next section contains, following my signature block, contains background on the fraudulent call problem, how we got here, and where we go from here. Having a unique vantage point after being in business for nearly thirty years, variously as a carrier, and now as a Provider of Telecommunication Related Services (e.g. billing, rating, and network analysis), we would like to respectfully advance our thoughts, and share our perspectives, with the Commission and the general public. Or, alternatively you may save time and depart from the document at this point – the important items have been stated.

***

TELSWITCH, INC. OFFERS THIS FEEDBACK AS A PTRS WITH ALMOST THIRTY (30) YEARS OF EXPERIENCE IN THE INDUSTRY.

36. From 1994 through 2001, TelSwitch Inc. offered retail and wholesale telecommunications services to residents and businesses in California through 950- and 10XXX casual dialing access scenarios, as well as 1+ dialing via PIC designations to our CIC code of 0626[12] and pre-paid and post-paid calling cards and wholesale carrier clients via branded-toll-free numbers. TelSwitch, Inc. also manufactured an IVR-based platform called Canvas, a module of which maintained internal-DNC (iDNC) functionality. The iDNC functionality was used by approximately ninety (90) telemarketing organizations.

37. After 2001, TelSwitch, Inc. focused almost exclusively on offering Airnet AMS, a comprehensive billing, provisioning, and network management platform to other telephone companies, including resellers and interconnected VOIP carriers. Contained within Airnet is also a real-time TCPA-compliance module that integrates into Kamailio, a platform used by call centers, to flag those calls that may be subject to restrictions under the TCPA, and as well as calls

[12] TelSwitch, Inc. d/b/a Tel-One Network Services was assigned Carrier Identification Code ("CIC") of 0626 and Access Carrier Name Abbreviation ("ACNA") of DLL by Bellcore.

that may be subject to more specific restrictions under the various states' mini-TPCA's.

38. The Kamailio platform provides real time functionality to identify and tag calls that are violative, or could be violative, of the TCPA[13], using DNC data from the FTC and WDNC data from iConnectiv. Similar to other organizations, that investigates, analyzes, and audit calls records related to allegations of violations of the TCPA, TelSwitch, Inc. also provides assistance in auditing the Call Detail Records ("CDR's") and assists companies in responding to allegations of violations of the TCPA.

TELSWITCH, INC. HAS BEEN INTEGRALLY INVOLVED IN INVESTIGATIONS OF FRAUD, INCLUDING LARGE CNAM FRAUD SCHEMES.

39. In addition to offering Airnet for Billing and Provisioning and real-time network lookups for determining which calls are potentially violative of the TCPA, via Kamailio, TelSwitch, Inc. also maintains a particular feature within Airnet that was used as either a stand-alone, or integrated module for interfacing with the a Caller Name ("CNAM") database provider for the provision, maintenance, and accounting of CNAM assignments.

40. For instance, when DID Provider-clients of ours decided to assign a telephone number, colloquially known as a DID to a customer, Airnet interfaced with an Application Programming Interface ("API") to provision the CNAM data and to load various switches with routing information on how to route, or convey, calls back to the customers' premises, so that those individuals who are who are calling the DID's that appear in their handsets are routed to the correct end-points associated with the customer of the DID.

41. We also included specific instructions related to the transcoding of the calls, so that as the calls traversed the Metaswitches and other facilities that are involved in the conveyance of the call, the switches know whether to use g.711 or g.729[14], or to conduct transcoding between

---

[13] Based upon the type of call, the call is flagged for specific call handling (such as manual dial, no pre-record, or simply no-call). Our data comes from the FTC's DNC database, and from iConnectiv – which TelSwitch, Inc. is a reseller of.

[14] G.711 and G.729 are two popular Session-Initiation-Protocol ("SIP") protocols used in the transmission and delivery of VOIP calls.

the two.

42. In connection with the CNAM module, TelSwitch, Inc. also manufactures an IVR platform called Canvas, of which one of the modules assists DID Providers and call centers with the collection of internal Do-Not-Call ("iDNC") requests. During a particularly heavy usage timeframe of several weeks in 2015, and again in 2016, some of the telemarketing companies that were using the Canvas iDNC module received a combined 250,000 iDNC requests per day.

43. TelSwitch, Inc. was asked to assist in the investigation of what appeared to be a massive scheme involving "CNAM fraud". Apparently, a particular DID reseller was obtaining their DID's from their wholesale vendor, which was in turn offering those DID's to telemarketers for free, in exchange for those telemarketers using the DID's as part of the outbound dialing process.

44. Asked by the DID reseller to make as *many* calls as possible, the telemarketers were encouraged to generate a huge quantity of dips into the CNAM database, so that a massive number of CNAM dips would generate massive amounts of CNAM revenue. Since CNAM dips occur regardless of the call being answered by the called party, even the calls that did not result in an answer incurred a CNAM dip. The scheme was also the subject of an investigative report that was contained in the Wall Street Journal.[15]

FRAUDSTERS USE DIFFERENT OUTGOING NETWORKS THAN THE NETWORKS FOR INBOUND TRAFFIC THAT IS ASSOCIATED DIDS IN AN ATTEMPT TO OBFUSCATE OUTBOUND TRAFFIC.

45. The reason why the alleged fraud persisted so long was that the telemarketers were using (and still use) different outbound networks to place the calls than the networks that were responsible for carrying the inbound calls to which DID's were assigned to. This clever way to obfuscate the actual origin of the calls that were initiated into the network from the carriers made

---

[15] As described in the article titled "Why Robocallers Win Even if You Don't Answer." (Wall Street Journal, June 4, 2018), each dip incurs a small fee that is shared with the carrier of record for that DID's, regardless of whether the individual who is called answers the phone. The money that was generated from this scheme was then shared with the telemarketers.

it difficult to identify. Without the help from consumers and the esteemed individuals at the US Telecom Traceback Group, carriers have almost no chance to terminate it. That is why it is essential that DID providers' interface with, and provide assistance to the US Telecom Traceback Group.

THE EFFORTS OF THE US TELECOM TRACEBACK GROUP AND THE FCC's INCORPORATION OF THEIR RECOMMENDATIONS ARE THE BEST TOOL AVAILABLE TO ABATE FRAUD.

46. In speaking with various individuals involved in the telecommunications, as well as those involved in the abatement of fraud, I learned that the most difficult part of identifying fraud was associating the calls that were outbound over one network, with the inbound calls over another.

47. It turned out that the calls were extremely difficult to trace despite the volume and frequency of calls, because the outbound calls were initiated from the scammers using DID's of one network, while the receipt of calls *from* those who were returning calls *to* those DID's were occurring entirely over a different network. By using multiple different call paths for the outbound calls while engaging a totally different network path for receiving the dial-backs to the DID's that were displayed in the handsets of the call recipients, the perpetrators of fraud had created an almost impossible-to-decipher scenario. The intentional obfuscation made it nearly impossible for investigators to identify the calling parties.

48. The ensuing civil litigation[16], as well as the investigations that were conducted by the CNAM vendor and various other entities, resulted in significant changes in the manner that DID's were assigned to companies with respect to pay-for-CNAM dips. I was told that, as a result of the investigation, there were many changes to CNAM revenue relationships.

49. A few things were excessively evident to me during the investigation. The challenges that I experienced, even with every piece of information at my avail, made it abundantly clear that the public had almost insurmountable challenges in identifying the

[16] *Marshall Spiegel et al v. EngageTel et al.* (Case No. 1:15-cv-01809, N.D. Il, Eastern Div.)

perpetrators of fraudulent and TCPA-violative activity. Even those companies who were seeking information on how the calls were being routed couldn't identify certain elements. And even once various players were identified, it didn't matter – the landscape of fraud kept shifting while the technologies that were used to identify the fraud couldn't keep up.

50. While many of the challenges have now been remedied with the passage of the TRACED act, which led to increased engagement between carriers and he coordinated efforts of US Telecom Traceback Group, there are still challenges. And even though the FCC has engaged in significant efforts to expedite the shut-down of carriers that offered safe harbor for fraudsters, there are still issues that need to be resolved.

***

51. Every client that I speak with states the same thing. The DNC list is too expensive, and cumbersome[17], and irrationally, does not provide historical information to users[18]. iConnectiv's WDNC[19] data (and number assignment data), while being reasonably priced, is may be too difficult for most individuals and companies to obtain access to, despite it containing *publicly available* information. It is also simply too difficult for most people to implement[20].

***

52. Although STIR/SHAKEN, DNC, WDNC and Do-Not-Originate databases are wonderful tools that have been wildly successful when used in connection with one another, it still requires the tools to be made available, and an overarching organization to actuate the ultimate

---

[17] The cumulative number of records contained in the FTC's daily DNC files between 01/01/2023 and 09/30/2023 is 62,847,325,609 records.

[18] Because of the idiosyncratic manner of how the DNC list is published, no historical data is available. A company must download the DNC list for at least thirty days to determine whether numbers that they are calling have been on the DNC list for more than thirty (30) days.

[19] Wireless Do-Not-Call data available from iConnectiv.

[20] iConnectiv's has been extremely helpful and has meaningfully engaged in every interaction that we have experienced, and I hope that more companies interface with them to implement their affordable WDNC product in order to mitigate calling activities that could potentially violate the TCPA.

shutdowns. And while the efforts of individual citizens in determining the bad actors and bringing attention to the DID Providers are certainly an important part of this, the US Telecom Traceback group, with its unique vantage point, and the brilliant technologists who work there and are working tirelessly to fix these problems, is the star of the show. Simply, not enough information makes it there, however, to mitigate fraud.

53. It is my belief that the US Telecom Traceback group is the most important tool in the FCC's arsenal, because the Traceback group has the ability to determine which outbound calls are associated with which DID's and subsequently which carriers, through the analysis of call detail records that are generated across different, disparate call networks. But they need more information from the carriers, DID Providers, CNAM databases, and from private individuals.

THE TCPA WORKS – AND THE SUPREME COURT FIXED THOSE PARTS OF IT THAT DID NOT WORK.

54. Another important point of contribution has been the private right of action that has been afforded under the TCPA[21]. Together, the framework for the TCPA, together with the TRACED act, have significantly curtailed fraud while allowing those who are legitimate callers – such as collection agencies, doctors' offices, airlines, and so on and so forth, to continue to engage in beneficial calling activities. And in sum, fraud ends when trust is restored and individuals who are being called can trust the number that is being displayed on the caller ID handset.

55. The landscape is moving toward one of consumers being able to once again trust the calls, and in specific, the caller-ID that appears on the phone before accepting the calls. In other words, consumers are once again able to trust that which appears on the caller ID display of their phone and accept the calls that they want. But it is because of the significant efforts that are being made by the trades, working together to bring best-of-breed practices and technologies to undermine scammers' abilities to initiate calls. These include esteemed individuals and clever products provided iConnectiv, the Network Operators and DID providers who, working together

[21] I have always been mystified as to why there is no private right-of-action under the Truth-in-Caller-ID act.

along with the FCC and the FTC and US Telecom Traceback group, are able to start to rebuild that foundation of trust.

TRADE ORGANIZATIONS, SUCH AS PACE AND R.E.A.C.H. PLAY IMPORTANT ROLES IN THE ABATEMENT OF FRAUD.

56. Additionally, there are several trade organizations that are deeply involved in solving the challenges of trust in the phone network. ACA International and PACE are on the forefront of these efforts, and along with R.E.A.C.H., and appear unified in their approach toward restoring trust and faith in the sanctity of what is displayed on the handset when calls are received. The cohesive and cooperative efforts by those organizations, and the recommended best-practices that have resulted, especially by R.E.A.C.H., serve as models of how the trade associations can guide constituency toward being as compliant as possible, while still affording members with the most impactful technology that is appropriate with which to make calls. The entire industry, from what I can tell, is interested in shutting down bad actors. And I believe that significant strides toward re-establishing good stewardship of telephonic communications is being achieved, without the need to chastise the DID Providers who are clearly not involved in the actual calling.

57. Thanks to PACE and R.E.A.C.H. and ACA International, and the efforts of the FCC and FTC, iConnectiv, NeuStar, the DID Providers, the carriers, and the CNAM vendors, and especially (I cannot over-emphasize this) the US Telecom Traceback Group, this problem can and will be solved.

58. The distinguished carriers and DID Providers, who have a vested interest in maintaining integrity of the telecommunications infrastructure by combatting bad actors will, in my opinion, apply solutions that will lead to a quantifiable and measurable reduction of bad traffic. In sum, legitimate callers want to hold themselves accountable – and those who are not, will simply be disallowed from participation in the conveyance of telephone calls across the P.S.T.N.

THERE SHOULD BE NO NEED FOR CALL BLOCKING APPLICATIONS, BUT THEY ARE NOW PERCEIVED AS THE ONLY OPTION BY CONSUMERS AMIDST THE EROSION IN CONFIDENCE OF PHONE NETWORKS AND REGULATORY AGENCIES' PERCEIVED INACTIVITY.

59. Unfortunately, the largest contributor toward the reduction of fraudulent calls reaching the handsets may actually come from the enhanced integrations of call blocking applications into the handsets. Originally developed as stand-along programs that incorporated into the phone's software (for example, using Apple's CallKit), call blocking applications YouMail and First Orion implement a scoring for mechanism that is based upon crowd-sourcing. Most likely because the perceived lack of ability of regulatory agencies to act, and the need to experience the satisfaction of a cessation of calls. Now, it is being implemented within the cell phone networks themselves.

IN SUM, THIS IS NOT A PROBLEM CREATED BY THE DID PROVIDERS. PLACING ADDITIONAL RESTRICTIONS ON DID VENDORS WILL NOT SOLVE THIS PROBLEM.

60. This predicament is a result of industry itself – not the DID Providers. But until industry steps up to the plate and implements some changes, the call blocking apps that are blocking those important calls, the will continue to win, and are the only choice.

61. To make qualified decisions, people must be given reliable information so that they can report spam to the DID Providers, so that DID Providers can report this information to the US Telecom Traceback Group, and place those DID's in the DO-NOT-ORIGINATE database while spam and scam investigations are completed.

62. But while people do want to do the right thing, they aren't. They are captured within an entire system that does everything possible to disengage with the consumer – the same consumers that they desperately want to connect with. There should not be one DNC list that costs $26,000 a year. Parroting the well loved and respected attorney Eric Troutman, the DNC list should be a free.

63. And there should not be extreme and extensive weird restrictions that are artificially placed on the information that relates a telephone number back to a particular DID Provider. This information should be free, and there should be dozens of websites offering it, not ZERO.

FINAL CONCLUSIONS

64. While the information as to which telecommunications vendor was associated with what number had been readily available from phone books and libraries in identifying the carrier of record and lodging complaints, barring this information, downloading a call blocking application is the only viable option. And with each increase in price of the DNC list, and with each increased difficulty of being able to get information as to which carrier is associated with which DID, and the lack of *immediate* cessation of robocalls, the challenge for companies increases, and the trust in the phone network erodes.

65. And although carriers are now experiencing expanded participation in the Do-Not-Originate ("DNO") database, there is still a long way to go. Until the industry comes up with unified solutions, including giving consumers additional tools necessary to report fraud, there will not be a diminished importance of these applications. Had industry addressed challenges related to fraud and scams, especially with CNAM, the call blocking apps would have never proliferated. If the FCC implemented a trusted CNAM scenario, and Congress fixed the Truth in Caller ID act to allow private right of action against companies that were providing misinformation related to the delivery of caller ID and Name information, would clean up bad behavior, and quickly.

***

66. While, I firmly believe that consumers are finally achieving some relief from the onslaught of scams and spam, they are still hesitant to accept calls based upon the telephone number alone which isn't necessarily the call source. Having limited ability to control who is calling them, they continue to download call blocking applications. There should be other options for consumers, such as allowing consumers to be able to identify the name of the carrier to whom a DID belongs to, such as what *Perrong* did when calls were being made to him by *unknown* caller.

67. And those consumers reports that are made to the DID vendors, should in turn send those complaints, along with call records, to the US Telecom Traceback group.

68. But most consumers aren't as *Perrong*, who obtained the carrier information from iConnectiv, and then sent a subpoena to the hosting carrier.

69. So with limited choices, and a lack of *perceived* interest from carriers and regulatory agencies in approaching TCPA violative activities, businesses may have to live with the choices *of industry itself* – which is that consumers won't answer the phone. Important calls, like calls from doctors' offices.

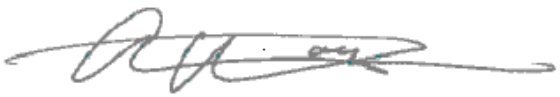
70. But be deprived of doctors' calls, car dealership recall notices, calls from airlines, and other types of necessary calls - that is a better choice to consumers than answering calls that are from scammers who are masquerading to be from the Internal Revenue Service, or agents from the Social Security administration, or Rachel from Card Services, or auto warranty calls, or so on and so forth.

71. But until the suggestions in this document are implemented, I will continue to place my trust and faith in the call blocking apps, which at least let me block those calls that are simply blocked by crowd-sourcing. Sure, I may miss a few calls from doctors or maybe an airline here and there, but who cares. They'll leave a message.

Thank you for taking time to read this response, I am appreciative of everyone's time and expertise at all of the aforementioned organizations, and thank you for your continued, tireless efforts in addressing robocalls and scams and other potentially TCPA-violative activity. We thank the Commission for their tireless efforts in working with private and public partners in chaperoning the industry through the myriad of challenges in a constructive and meaningful way.

declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct. Executed this 14th day of September, 2023 in Pleasant Hill, California.

Respectfully Submitted,



Aaron Woolfson

woolfson@telswitch.com