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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

REPLY COMMENTS OF ZipDX LLC[1]

5th/4th FURTHER NOTICES OF PROPOSED RULEMAKING
Re: Gateway Providers & Foreign-Originated Calls

[1] ZipDX LLC is a provider of phone- and web-based collaboration tools. Since 2013, we have devoted resources to the fight against illegal robocalls. In 2013, our entry in the FTC's Robocall Challenge outlined the traceback approach that is in use today, with participation mandated by the TRACED Act (passed by Congress in 2019) and the Commission's rules (adopted in 2020). Starting in late 2018, ZipDX developed (without compensation) and ran the first Secure Traceback Portal, responsible for thousands of successful tracebacks by USTelecom's Industry Traceback Group. Reports from this Portal, as well as correspondence and affidavits of ZipDX's CEO, appear in numerous enforcement actions by federal and state agencies, including the FCC's largest-ever fine for robocalling issued in a 2021 Forfeiture Order. ZipDX continues to work with enforcers and industry battling illegal robocalls.

The FNPRM and Comments responsive thereto have set the stage for a shift in the FCC's fight against illegal robocalls. Rather than sweeping rules that touch every provider and every telephone call, the focus must be on the much smaller subset of providers and call flows that are at the root of the problem. Allocating resources to specifically target the sources of these illegal calls will provide the best return on investment.

By definition[2], robocalls are machine-initiated and/or invoke a pre-recorded or artificial voice; these are the fundamental mechanisms that have allowed the calls to scale to billions per month. This is in contrast to the original purpose of the telephone network: conversational calls, where one human dials a telephone number and sticks with that call exclusively until it ends. The logical place to look for illegal robocalls is in streams of rapid-fire computer-driven calling; there will not be any significant number in conversational traffic.

In the following pages we articulate rules for how this needs to happen, consistent with many of the comments already filed in this proceeding. Our approach is to keep things as simple as possible. Briefly, our proposal:

- Obligates those providers that choose to accept non-conversational traffic to apply appropriate controls and scrutiny
- Eliminates some distinctions between originating and intermediate providers,
- Leverages the huge investment in STIR/SHAKEN already made by industry and regulators to protect legal robocalls while further shielding us from illegal calls

The steps we put forward could, and should, be taken by every provider in the industry that wants to contribute to combatting illegal robocalls; they do not need Commission permission to move forward.

[2] There is, in fact, no regulatory definition of "robocall" but we seem to all think we know it when we see it.

TABLE OF CONTENTS

SOURCES AND FACILITATORS OF ILLEGAL CALLING

The most prolific illegal robocallers currently operate in a fairly consistent fashion. The US Department of Justice wrote this in January 2020[3]:

In the cases announced today, the United States alleges that the defendants operated voice over internet protocol (VoIP) carriers, which use an internet connection rather than traditional copper phone lines to carry telephone calls. Numerous foreign-based criminal organizations are alleged to have used the defendants' VoIP carrier services to pass fraudulent government- and business-imposter fraud robocalls to American victims. The complaints filed in the cases specifically allege that defendants served as "gateway carriers," making them the entry point for foreign-initiated calls into the U.S. telecommunications system. The defendants carried astronomical numbers of robocalls. For example, the complaint against the owners/operators of Ecommerce National d/b/a TollFreeDeals.com alleges that the defendants carried 720 million calls during a sample 23-day period, and that more than 425 million of those calls lasted less than one second, indicating that they were robocalls. The complaint further alleges that many of the 720 million calls were fraudulent and used spoofed (i.e., fake) caller ID numbers. The calls facilitated by the defendants falsely threatened victims with a variety of catastrophic government actions, including termination of social security benefits, imminent arrest for alleged tax fraud and deportation for supposed failure to fill out immigration forms correctly.

In its March 17, 2021 Forfeiture Order[4], the FCC's Enforcement Bureau wrote:

The Rising Eagle Notice asserted that Rising Eagle admitted to the Traceback Group that Rising Eagle did not stop using spoofed caller ID until September 10, 2019. In its response, Rising Eagle admits to knowingly using unassigned numbers as caller ID, because its main client, Health Advisors, "prescribed that all of the calls made during the course of its telemarketing campaigns would be made from unassigned, inactive caller ID numbers." Rising Eagle also admits to providing services for 525,500,000 Health Advisors calls. Rising Eagle does not contest that it spoofed more than 500 million calls. Rising Eagle argues instead that it was acting according to its client's wishes in choosing which numbers to spoof.

Our extensive work investigating illegal robocalls is consistent with these findings and suggests that the following are descriptive of illegal robocall schemes:

- Each caller sends hundreds of thousands or millions of calls each day.

[3] https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions

[4] https://docs.fcc.gov/public/attachments/FCC-21-35A1.pdf

- An illegal robocaller's calls, on average, last less than a minute – typically 15 to 30 seconds.
- Only a tiny fraction of the calls – typically less than 1% -- last more than two minutes.
- The callers often use a huge number of different caller-ID values – the most common technique is to make up a different caller-ID for every call they make. Sometimes they acquire (or rent) enormous banks of numbers. Either way, they are trying to deceive analytics engines and deceive the called party.

Many of these calls with random caller-ID values have been captured in voice messaging platforms, matching the bad behavior to the scam call content. And in those cases where callers were using the same caller-ID values repeatedly (as opposed to making just one or a few calls per caller-ID), we can readily correlate those values to scams (including government imposter, baseless credit card interest rate reduction offers, utility cutoff threats, and fake Amazon charge alerts) identified in those messaging databases and to submissions to the FTC's Do-Not-Call complaint database.

These call duration metrics (low Average Call Duration, abbreviated ACD, and few calls of any substantial length) are in sharp contrast to conversational calling, where analysis consistently shows ACD of three minutes or more and 25% or more of calls lasting at least two minutes. If these automated (non-conversational) calls were legitimate, they would use a small, consistent set of caller-ID values (also referred to as Automatic Number Identification or ANI), not the millions of different values that we have observed.

The metrics we describe above were available to the facilitating providers on the days the calls were placed had those providers bothered to undertake a similar analysis. Calculating the metrics for several million CDRs can be accomplished in a few minutes or less when the records

are stored in a relational database. Providers that truly want to address illegal robocalling need to refuse all calls from sources whose traffic meets the profile described here. That is the shortest path to solving the illegal robocall problem.

REGULATORY FOCUS ON HIGH-VOLUME TRAFFIC

We believe that introducing explicit treatment of high-volume traffic into the existing rules framework is the quickest and most cost-effective way to make a measurable impact on the illegal robocalling scourge. Our approach finds support in many of the comments submitted in this docket.[5]

Illegal robocallers by definition do not follow the rules. Many of them are fraudsters; they are liars at their core. Those that facilitate these activities are often of similar disposition. These characters think nothing of clicking a checkbox that says "under penalty of perjury" such as those seen in the filing forms for 499A, Intermediate Provider Registry, FRN sign-up, and Robocall Mitigation Database. To the extent that they are outside the United States, they are well aware that they are not going to be extradited by Pakistan or India or the Philippines or Hong Kong or the UAE for clicking such a checkbox. Those in the United States likely are using a fake name and/or address and/or will relocate and change their identity before they get tracked down. Such self-certification, combined with no vetting or enforcement, is entirely ineffective.[6]

[5] As an initial example, i3Forum says (p. 10): "'Know your customer' in the gateway context should instead be 'know your traffic,' so to speak."

[6] USTelecom highlights these concerns as well (p. 7, "[R]ules that apply to providers only when they act as gateway providers, but not in other contexts, threatens to add new opportunities for gamesmanship. For instance, some providers may claim to be based in the United States – and even may be legal U.S. corporate entities – but have little or no U.S. presence, operations, or principals. The threat of enforcement may not have a significant deterrence effect against such entities. In addition, some gateway providers may be fly-by-night entities that, in effect, rely on another provider's (including potentially downstream transit provider's) platform to accept and route calls. These providers very well could disappear upon any significant scrutiny, only for one or more gateway providers to pop up in place. These facts obfuscate which provider – whether the gateway provider or the provider one or two hops downstream – is most responsible and can best be held accountable by the Commission for bringing foreign-originated illegal traffic to U.S. subscribers. In some cases, this obfuscation may very well be by design.")

Of course, we know illegal robocallers lie about all sorts of things. They hijack phone numbers that belong to others, or just make up numbers on the fly. They file garbage as their Robocall Mitigation Plan, or file a legitimate-looking plan that they do not follow.

The traffic they send, on the other hand, tells a story that is much harder to manipulate. Rather than looking at each call in isolation, we need to look at the set of calls that a given source sends to a provider willing to take their traffic in exchange for payment. We know from decades of experience that over the course of a day, traditional conversational traffic – where a human initiates a call and sticks with it exclusively while it is answered and then ultimately terminated by the called or calling party – has a fairly predictable profile. Average call duration (ACD), calculated as the sum of the durations of each call after it is answered, divided by the count of all answered calls, will be in the range of three to five minutes. And while many connections will be very brief (for example, many calls end up in voicemail and some callers hang up as soon as they discover they haven't reached a live person), typically there will be 25% or more of the calls that last at least two minutes.

Robocalling, however, has much different characteristics. These rapid-fire machine-generated calls are typically very short (most recipients hang up when they realize who's calling), and the only calls that last more than two minutes are those where a target responds to the initial automated message and engages with a human.[7],[8]

[7] Several commenters highlighted concerns with high-volume calling, including i3forum (p. 12, referencing high call volumes and short durations); iBasis (p. 2, has implemented internal analytics to identify very high volume and/or very short duration calls that trigger internal alerts); YouMail (p. 9, "High volumes of short duration calls are not indicia of bona fide, high value communication attempts. Rather, they are indicia of robocalls that plague consumers and degrade the overall phone network."). Twilio (p. 6) suggests "the Commission would benefit from gathering additional metrics on how to improve reasonable analytics"; that is what we do here.

[8] SipNav advocates the monitoring and blocking of media IP addresses as an alternative mitigation mechanism. We are not enthusiastic. Media IP addresses are often not preserved end-to-end; many providers purposefully proxy or re-initiate the media stream in a process called topology hiding, to cloak the identity of their customer. Additionally, while obtaining a fresh IP address after being blocked is an additional hurdle for a fraudster, it is a low one. IP addresses are readily available; Amazon's compute cloud makes them available for a few dollars a month.

Providers that want to be part of the robocalling solution need to focus their energies on non-conversational traffic, as that is where the illegal calls will be found. Regulations need to mandate that focus.

Our best first step is to separate conversational and non-conversational traffic. Blending of the two types makes it harder to distinguish each; thus, we want to encourage the traffic types to stay separated as far along the call path as possible.

Conversational traffic should flow unimpeded. Providers handling this traffic need not be burdened with new requirements, because this is not where the problematic robocall traffic will be found.[9] Because conversational traffic is relatively safe, we need not worry about whether it is domestic or foreign-sourced, or whether it has a USA caller-ID, or whether it comes from a provider registered in the RMD. It is even not critical that it be SHAKEN-signed.[10]

Our challenge with non-conversational traffic is to make sure that the legal calls are reliably delivered, and the illegal calls are rejected. We do this by establishing safe handling for the legal calls and fencing off the others, via the steps described in each section below.

A. Providers Opt-In to taking Non-Conversational Traffic

Each provider must make a deliberate decision as to whether they will or will not accept non-conversational traffic. Those that elect to take payment for this type of traffic must have the resources and expertise to deal with it appropriately. They must know that they will be held liable for illegal calls that move via their platform.

---

[9] Certainly there can be other nefarious activity in conversational traffic, but that is not the focus or mandate of this robocall effort and, to the extent it is to be addressed, needs to be dealt with in its own distinct context.

[10] CTIA, for example, expresses concerns about overly-burdensome rules (p. 14): "While providers in industry standards bodies are focused on how to promote the use of call authentication with foreign partners, this work is in its nascent stages, and it would be premature for the Commission to adopt authentication requirements here. For these reasons, the Commission should maintain its flexible approach to allow gateway providers to determine whether attestation is appropriate for unauthenticated foreign originated calls." We agree, as long as the calls are part of conversational traffic.

B. Providers Must Have Appropriate, Effective Safeguards

The industry routinely argues that it does not want the FCC to mandate specific best practices.[11] Consistent with this philosophy, each provider that elects to take payment to carry non-conversational traffic can implement whatever methodology they wish – it just MUST be effective. Each provider has many options. Non-conversational traffic is so dangerous that they SHOULD have a complete understanding of what each of their customers is doing – who are they, who do they work for, whom are they calling, what message(s) are they playing, what calling number(s) are they using. Providers can put in place contract provisions that constrain how their service is used and allow them to audit and even record calls[12]; they can ask for bonds and indemnification if rules are broken; they can definitely put limits on the numbers of calls placed and the caller-ID values permitted.[13] Any provider that is uncomfortable or incapable of implementing an effective process to ensure the legality of the calls must not accept non-conversational traffic; similarly, if their current or prospective customer finds the conditions onerous, that customer should find another route for their traffic.[14]

---

[11] T-Mobile, for example, says (p. 9): "imposing an obligation to include particular contract terms in carrier agreements is contrary to the Commission's flexible approach to imposing customer-related requirements and mitigating illegal traffic."

[12] YouMail (p. 10): "YouMail believes that auditing and analysis of calling patterns needs to be supplemented by research of both public and private information providing evidence that specific call sources are committing harm to the public. This can be done through periodic 'content sampling' of robocalls and 'complaint boards.'"

[13] YouMail suggests (p. 3): "the Commission could propose new rules that would require the NANP administrator to designate a new Area Code for exclusive use in foreign locations. Over time, consumers would learn to recognize the Area Code and its purpose. To stimulate consumers to answer calls from these numbers, VSPs, most especially gateway providers, would have an even stronger incentive to stop robocalling from these numbers." A similar but more effective approach would be to designate a specific area code for ALL robocalls (not just foreign). ZipDX suggested this in our 20-Oct 2021 comments regarding Access to Numbering (Docket 13-97, https://ecfsapi.fcc.gov/file/10212332527789/ZipDXComments_AccessToNumberingFCC-21-94r20.pdf, p. 9). This, however, is a long-term approach; we prioritize instead what we describe in these Reply Comments.

[14] We recognize this may result in somewhat increased costs for legal robocallers. These callers are already enjoying tremendous cost REDUCTIONS thanks to VoIP technology, access charge reforms, and other changes. i3Forum explicitly suggests new fees on robocall traffic: "[C]reating a cost for call attempts that share characteristics of illegal robocalls would significantly increase the overall cost of fraudulent activities." It is appropriate that incremental costs associated with automated calling be borne by those placing the calls.

C. Providers Must Know What Role They Play

Commenters have pointed out that they often do not know what role they play in a given call, nor might they know what role their source plays.[15] While this may not be an issue for conversational traffic, providers DO need to know their role when dealing with non-conversational traffic. The fight against illegal robocalls dictates that we de-mystify this traffic; part of that is insisting that each party understand where they fit in the call path.

D. Non-Conversational Traffic Must Reach The Destination in Two Hops Max

We learned a terrific lesson several years ago in (largely) solving the Rural Call Completion problem. Calls to rural areas were inexplicably not reaching the called party in extraordinarily high numbers. The FCC put in place a safe harbor, absolving providers of extensive reporting requirements if each call was sent to the rural destination via no more than two intermediate providers. Case closed.

An identical approach is appropriate for non-conversational traffic. Today, these calls follow circuitous paths that obfuscate responsibility.[16] The two-hop limit will dramatically improve transparency for these calls and make it much easier for those facilitating the calls to implement the appropriate safeguards. Perhaps more importantly, those making LEGAL robocalls will see improved delivery rates and will have a much easier time resolving improper

[15] For example, BICS explains (p. 2): "Applying a 'call-by-call' classification for gateway providers seems unfair as gateway providers are unable, in most cases, to determine the origin and nature of each and every calls (as explained above). Gateway providers will not be able to cascade and apply different processes and controls per call." Precisely, which is why BICS and other similarly-situated providers should steer completely clear of non-conversational traffic, including demanding that their upstream sources do the same.

[16] Comcast notes (p. 9): "While some gateway providers may have direct relationships to callers or their originating voice service providers, that is often not the role that gateway providers play. Indeed, in many cases the gateway provider is multiple hops from the originating caller or originating network."

blocking and labeling issues. Providers choosing to carry non-conversational traffic must collaborate to ensure each call transits no more than two intermediate providers.[17]

E. Non-Conversational Calls Must Be Authenticated With A-Level Attestation

Industry and regulators have made an enormous investment in STIR/SHAKEN, which was prompted and justified by robocalling concerns. We must tie this investment back to robocalling by mandating that providers choosing to accept and originate non-conversational traffic do so only when they can and do properly authenticate that traffic with A-level attestation[18] using their own SHAKEN certificate.

Further, we need to use the OrigID field to identify the source of each call clearly and transparently. Knowing with certainty the caller and originating provider will further help the LEGAL calls flow smoothly.

F. Non-Conversational Calls Must Be Sent Onward via S/S Capable Routes

Today's Call Authentication Framework suffers because it only works when the call is end-to-end SIP, or to the extent that the emerging out-of-band authentication standards are deployed. It likely will be a long time before our entire network is STIR/SHAKEN capable.

---

[17] YouMail says (p. 3): "Indeed, there is a large market for delivering lawful, legitimate, and yes, even desirable, robocalls (autodialed) from overseas to the United States." We disagree. While some US businesses make legal robocalls that ultimately connect to overseas human agents, we believe the bulk of those calls are initiated stateside. Regardless, for those legal robocalls (be the number large or small) that do originate overseas, they can be sent directly (via the Internet, as virtually all such calls travel today) to a provider that can ensure that they reach their final destination via two or fewer intermediaries – not via a long chain of aggregators that add little or no value.

[18] i3Forum says (p. 5): "Despite the Commission's assertion that gateway providers would not be limited to assigning a C-level attestation to all calls, gateway providers, in almost all situations, could only confirm that the provider is a gateway provider with no relationship to the call originator (i.e., a C-level attestation). This lowest level attestation under STIR/SHAKEN fails to provide any useful or meaningful assistance for blocking illegal robocalls. It would be wasteful and unfair to require gateway providers to invest their resources in attempting to comply with STIR/SHAKEN when the outcome does not facilitate the identification or elimination of illegal robocalls." We agree. Maximum utility, especially with respect to potentially problematic non-conversational traffic, comes from A-level attestation.

But there are plenty of pathways today that support S/S. So that S/S can be as effective as possible with respect to the traffic it was intended to target, all non-conversational calls must be sent onward via such a route.[19] Only with respect to final delivery to the terminating provider should an exception be allowed if there is no alternative.

Again, multiple benefits accrue to LEGAL robocallers. Their A-level attested calls will arrive fully authenticated. And if for some reason one of their calls is blocked, having a reverse path that is SIP-capable is tremendously helpful per the separate, simmering 602/607/608 debate.

G. RMD Should Reflect Non-Conversational Treatment

The Robocall Mitigation Database promises to be a useful and perhaps critical tool in managing what will likely be an on-going challenge. Today there are almost 7,000 entries in the RMD, including over 4,000 that have Robocall Mitigation Plan documents and more than 800 indicated as Foreign. Trying to audit all of these entries is a monumental task; we know because we have tried. And a complete audit is not the best use of resources, because most of these providers are not part of the robocall problem.

By augmenting the RMD with a checkbox[20] whereby a provider indicates that it accepts non-conversational traffic, we will all be able to better focus our attention in the right place. Those providers that have opted into this business can be given 120 days to update their RMD entry by checking the box, uploading an appropriate RMP that details how they ensure that their

[19] TransNexus points out illegal robocallers will (and perhaps already are) working to avoid STIR/SHAKEN (p. 2): "Furthermore, gateway providers that use non-IP network technology or interconnections, and that might be inclined to look the other way while transiting illegal robocall traffic, would become a preferred route for illegal robocalls." We agree. Non-conversational traffic must go via a STIR/SHAKEN route, be that an IP network or via a non-IP extension when and where available.

[20] USTelecom (p. 6) advocates new checkboxes for different provider types. We prefer to eliminate the provider type distinction. Differentiating those that do (and do not) accept non-conversational traffic is more relevant.

non-conversational traffic is legal (see B, above), and affirming compliance with everything here.[21]

Having that in place will provide additional tools for industry and enforcement. Providers obviously should not accept non-conversational traffic from other providers that claim not to carry it. Providers can review each other's RMPs to build best practices (RMP redaction should not be an option). Robocall tracebacks that implicate providers not checking the box can raise automatic alarms that trigger swift delisting from the RMD after a brief investigation. Enforcers can proactively review the entries and RMPs of those providers opting into non-conversational traffic and will have better context when enforcement actions are taken.[22]

H. Adapting the Regulations

ZipDX claims little expertise at writing formal regulations. We note that today, 47 CFR § 64.1200 (n) (3) says that "Every voice service provider must take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic." We propose eliminating the references to new and renewing customers and the "originating" notion (because providers often don't know). "Every provider must proactively and effectively mitigate illegal robocalls regardless of their role in the call

[21] USTelecom writes (p. 4): "the Commission should require that all providers implement a robocall mitigation plan, and that they do so regardless of the role in the call path they play and their STIR/SHAKEN implementation status." This must be mandated for providers carrying non-conversational traffic; it may be unnecessary for others.

[22] USTelecom writes (p. 8): "A key to unlocking the promise of the RMD of a chain of trust in all U.S.-destined traffic is aggressive and rapid enforcement. The Commission today already has a significant set of tools to ensure that providers are held accountable, which will be enhanced with the changes to the RMD proposed herein. The Commission can and should take action to ensure that RMD filings are proper and valid, and take action when they are not." We agree that the Commission must step up to its crucial obligations with respect to aggressive and rapid enforcement. We also believe that the "chain of trust" notion is flawed not only because of the "intermediate provider loophole" identified in USTelecom's comments, but because (as we noted elsewhere) the RMD is being seriously gamed. Nonetheless, the ability of the Commission to quickly delist a noncompliant provider is a key tool that can be effectively leveraged when the focus is placed on non-conversational traffic.

without waiting for notification from the Commission or otherwise (such as a traceback notification from the registered consortium)."

Given that this is a broader mandate, we would suggest a safe harbor: "A Provider will not be liable for illegal calls from a given source on any day for which the Provider has Call Detail Records demonstrating that the entirety of traffic from that source on that day met Conversational Metrics (average call duration exceeding two minutes, and more than twenty percent of calls exceeding two minutes in duration)[23],[24]. This exception does not apply if the Provider has within the previous six months been notified about one or more illegal calls from that source. A terminating provider that is not also the originating provider will not be liable for an illegal call unless the Commission can show that the provider acted carelessly in accepting or continuing to accept calls from the source."

The elements (A-G) we have outlined above would then frame rules for non-conversational traffic.[25] We note (again) that illegal robocallers are clever and nimble. In crafting our approach, we have tried to "think like a robocaller" but we know that whatever actions the Commission takes, the fraudsters and their facilitators will react to work around and defeat them. Thus, Commission and the industry should anticipate routine revisions to keep current.

CONCLUSIONS

The FNPRM was prompted by the observation that many illegal robocalls appear to originate outside the United States. An obvious potential solution would be to identify the

[23] Specifically, we suggest ACD = SUM(all answered call durations, in seconds) / COUNT(answered calls), and % > 120 secs = 100 X COUNT(call duration > 120) / COUNT(answered calls). For both metrics, calls to toll-free numbers are excluded from the numerator but not the denominator, since some may try to game the system using lengthy toll-free calls. We focus on answered calls today, but suspect more attention will need to be given to cancelled calls (where the caller hangs up after the call starts ringing, but before it is answered) in the future.

[24] The Commission could consider phasing in the thresholds to give providers more time to clean up their traffic. For example, we could start quickly with an ACD of 90 seconds and later move to 120.

[25] We recognize that there could be rare exceptional legitimate cases that require deviation from these rules; the FCC should be prepared to grant narrow exemptions in such cases upon review of an appropriate application.

Gateway Providers that bring those calls onto the USA network and impose upon them additional operational constraints.

Commenters, including ZipDX, expressed misgivings about various aspects of this approach. Callers and providers lie about their whereabouts. There is a reluctance to introducing another provider category when we already have difficulty knowing who is an originator vs. an intermediate provider vs. a caller. Commenters oppose placing additional requirements on those that are not part of the problem.

We have put forward a constructive alternative that focuses the collective energy on the places where the illegal calls lurk. Our approach leverages many of the tools that have been put in place over the last several years.

The message to providers that want to avoid burdens associated with illegal robocalls, both foreign and domestic, is simple: Do not deal in anything but conversational traffic. Do not pollute your call streams with dialer, call center, high-volume, short-duration, or whatever other labels might apply. Leave that to those providers that have the necessary resources.

Those that do elect to play in this space must proceed with extreme caution. Our belief is that very few legal robocalls originate overseas, but to the extent that they do, they need to come directly to a provider that is equipped to handle them.

As always, we stand ready to engage in further dialog as the Commission and stakeholders work to enhance and optimize the constructive ideas put forward here and elsewhere in this docket.

Respectfully submitted,

DATED: 9 January 2022

/s/ David Frankel
dfrankel@zipdx.com
Tel: 800-372-6535