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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
	)	
To: The Commission	)	

OCTOBER 2017 WRITTEN EX PARTE COMMENTS OF ZipDX LLC

Submitted to the Record

David Frankel
dfrankel@zipdx.com
17554 Via Sereno
Monte Sereno, CA 95030
Tel: 800-372-6535

Filed: October 26, 2017

Illegal robocalls and related unwanted calls have been the biggest source of complaints at the FCC and the FTC for several years. The rate at which complaints are filed (in excess of ten thousand per day) continues to trend upward at an alarming pace. While there are several regulatory, industry and legislative efforts underway in various stages, none will have sufficient impact, even if fully implemented, to reverse this trend in the near term (before the end of the decade).

In further response to NOI FCC 17-24, ZipDX submits this proposal. We advocate engaging Originating Providers – those closest to the robocallers – to use existing technology and standards to constrain the mass calling and spoofing that has made this problem so intractable.

BACKGROUND AND CONTEXT

It has been repeatedly stated that illegal robocalling is facilitated by the proliferation of voice-over-internet-protocol services, which enable cheap, high-volume calling using any caller-ID of the caller's choosing. When a call arrives at the destination, it is impossible to know if the calling number is spoofed and very difficult to trace the call back to its origin.[1]

We know that the number of *robocallers* is tiny compared to the number of robocall recipients. This becomes intuitively obvious when we learn, from enforcement actions, that some robocallers are placing more than a million calls per day.[2] It would be far more efficient to stop

[1] "[P]art [of the solution] is identifying the bad actors who use robocalls to take advantage of unsuspecting consumers by using numbers assigned to others (spoofing). They use cheap and accessible technologies to spoof their caller identity and scam victims with threats from the IRS, offers of loans, or free travel. The Strike Force is committed to protecting customers, but these disguised calls have put investigators and enforcers at a disadvantage." October 2016 Robocall Strike Force Report, p. 1, available at https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

[2] Citation and Order, In the matter of Adrian Abramovich, Marketing Strategy Leaders Inc., and Marketing Leaders Inc., FCC DA 17-593, para. 10, available at https://apps.fcc.gov/edocs_public/attachmatch/DA-17-593A1.pdf.

robocallers at their sources, if we could, just as it is easier to stop a dandelion at its flower rather than chasing all of its wind-scattered seeds.

Illegal robocallers come in many shapes and sizes, just as dandelions may appear individually while in other cases they fill an entire field. The top priority should be the most egregious violators.

One recent study by Pindrop Security noted: "Our results show that 51% of the robocalls recorded can be attributed to only 38 distinct telephony infrastructures…."[3] The FCC quotes this statistic: "U.S. consumers receive an estimated 2.4 billion robocalls per month in 2016."[4] Extrapolating from those numbers, we can calculate that, on average, each of those 38 robocallers is placing about 32 million calls per month or about a million calls per day – consistent with the FCC's finding in the recent Enforcement Bureau action.

These are *volume callers*, and a focus on volume callers is a cornerstone of this proposal. To be sure, some volume callers are operating legally. But if you consider the hundreds of millions of individuals and institutions that place USA phone calls each day, only tiny fraction of them are placing massive numbers of calls and they are the ones we should spend some of our energy scrutinizing. How do we achieve that focus, especially when the illegal robocallers appear hidden and in some cases offshore? Every phone call that terminates to a subscriber on the United States Public Switched Telephone Network enters the network via an originating carrier regulated by the FCC. This is shown in Figures 1 and 2 below.

[3] The Pindrop paper is available at https://www.blackhat.com/docs/us-16/materials/us-16-Marzuoli-Call-Me-Gathering-Threat-Intelligence-On-Telephony-Scams-To-Detect-Fraud-wp.pdf

[4] From FCC 17-89, Call Authentication Trust Anchor NOI, page 1, quoting from the YouMail Robocall Index, available at https://ecfsapi.fcc.gov/file/07141096201120/FCC-17-89A1_Rcd.pdf.

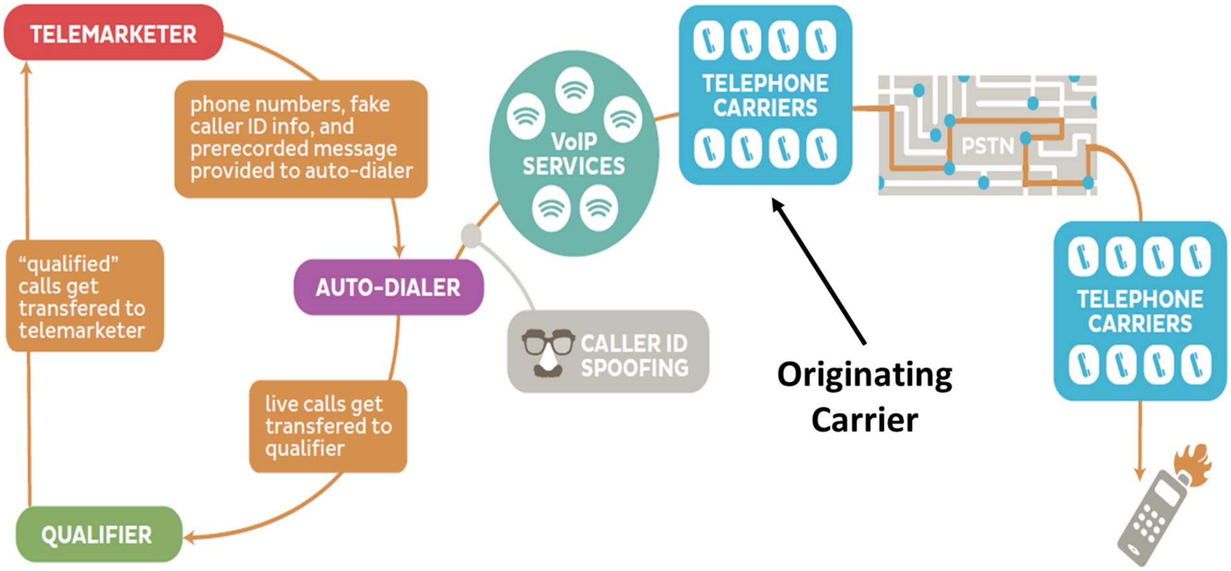
TELEMARKETER
phone numbers, fake caller ID info, and prerecorded message provided to auto-dialer
"qualified" calls get transfered to telemarketer
AUTO-DIALER
VoIP SERVICES
CALLER ID SPOOFING
TELEPHONE CARRIERS
PSTN
TELEPHONE CARRIERS
Originating Carrier
live calls get transfered to qualifier
QUALIFIER

Figure 1: Robocaller Call Flow[5]

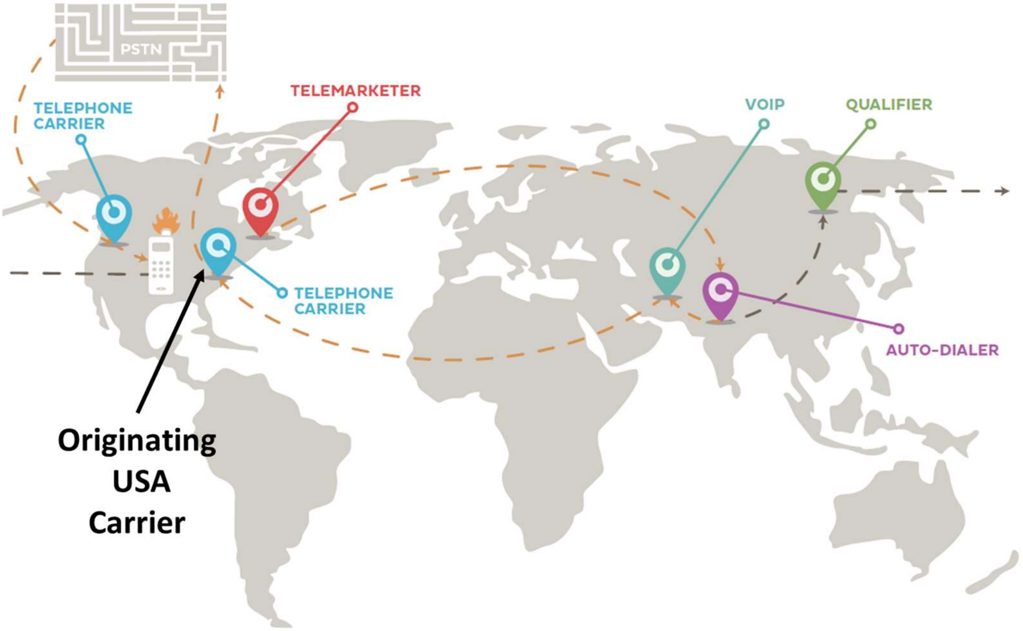

Figure 2: International Call Flow[6]

[5] From Federal Trade Commission "How Does a Robocall Work", available at https://www.consumer.ftc.gov/articles/pdf-0113-robocalls-infographic.pdf. "Originating Carrier" indication added.

[6] From Federal Trade Commission "The path of a robocall can span the entire globe", available at https://www.consumer.ftc.gov/articles/pdf-0113-robocalls-infographic.pdf. "Originating USA Carrier" indication added.

Even calls originating overseas still come through some USA PSTN gateway. Figure 2 above shows a telemarketer in the USA controlling an overseas auto-dialer that targets USA phone numbers.

Thus, originating carriers as shown in Figures 1 and 2 occupy a critical position in the robocall call path and they have the opportunity to play a pivotal role in sharpening our focus to mitigate this scourge. The "VoIP Services" provider shown in Figure 1 can also contribute; the closer we get to the actual robocaller, the better. As a complement to the other robocall mitigation efforts now underway, the FCC will have a huge impact on the problem if it works with these *Originating Providers* (carriers and VoIP providers) along the lines we present here.

The next section explains the actions that we propose Originating Providers take; Appendices A and B provide additional technical detail and some proposed values for the applicable thresholds and limits that will define and constrain volume callers and spoofers.

ORIGINATING PROVIDER ACTIONS

Here are the steps that we are asking Originating Providers to take with respect to volume callers:

1. Before an Originating Provider enables a customer to become a volume caller, that customer should undergo some level of vetting. This is one way to deflect a potential PSTN terrorist. Today, anybody can go on the web and sign up with a credit card to make large volumes of calls. Since very few people have a legitimate need to suddenly start making millions of phone calls, it would be prudent to collect some additional information before unlocking the telephony floodgates.

2. We noted at the outset that caller-ID spoofing is a key enabler for illegal robocallers, making downstream mitigation as well as identification and enforcement problematic or impossible. While spoofing is sometimes legal, Originating Providers need to set very high hurdles for *spoofing by volume callers*. The default should be that spoofing is not allowed; it should be enabled only with supporting documentation.
3. For calls that do make it onto the network, Originating Providers need to take advantage of all available signaling elements that would enhance the ability of downstream providers and enforcement officials, acting on behalf of illegal robocall recipients, to rapidly identify the sources of those calls and take appropriate action.
4. All Originating Providers need to proactively cooperate in industry traceback efforts and FCC investigations so that they can be quickly and efficiently resolved without suffering delays and expense associated with unnecessary legal maneuvering.
5. Since illegal robocalling remains somewhat clouded in mystery and is constantly evolving, we need to increase our data gathering and enable the deployment of more sophisticated analytics. This will allow for ongoing refinement of mitigation and enforcement efforts as robocallers change their tactics.

KEY ATTRIBUTES OF THE PROPOSAL

We can only ask Originating Providers to step up to this challenge if our proposal is pragmatic and if providers believe that their efforts will in fact be rewarded with a measurable reduction in illegal robocalls. We achieve this in several ways:

A. We are not inventing new technology. We are asking that providers use, to the fullest, targeted extent possible, technology already in place. We use call admission metrics that are already available in deployed switching systems, signaling elements that are already standardized and operational, and reports that leverage data already being gathered.

B. Recognizing that the PSTN is transitioning from legacy (SS7/TDM) signaling and transport to VoIP (SIP), our approach is designed to span both domains, offering end-user benefits regardless of technology and infrastructure. Illegal robocallers will have a difficult time hiding behind a technology façade.

C. We intend to set thresholds that will keep efforts focused on the most lucrative targets. Providers that serve smaller customers where the ability to make large numbers of calls is already constrained won't be burdened by this proposal.

D. We know that one size does not fit all. A system of exceptions is required; whether for technical limitations in provider systems and equipment, or special circumstances associated with a particular customer. Our proposal needs to accommodate these situations and it has to be structured to evolve as we learn more about the problem, shift our focus to smaller perpetrators once the big ones are knocked down, and adjust to their ever-changing tactics.

E. This is an urgent problem; consumers are at the breaking point. But change takes time. We recommend a phase-in approach, allowing some quick benefit with initial steps and more mitigation as the proposal is fully adopted.

F. We are not asking providers to determine if a call is legal. We are putting in place hurdles that will make it harder to place illegal robocalls. Legal robocallers and their providers will have to affirm their compliance with applicable laws and regulations.

FCC AUTHORITY AND PAST SUCCESSES

We know that the FCC needs specific authority for any regulation it enacts, and we also know that solutions that have worked in the past can foreshadow future success.

Several years ago, the FCC addressed the problem of Rural Call Completion, which to that point had been growing in scope and seemed otherwise intractable. The FCC imposed a set of reporting requirements which, it was hoped, would lead to better identification of the root cause(s) of the problem and allow appropriate correction(s). The RCC order also offered a safe harbor, exempting providers from the somewhat onerous reporting requirements if they adhered to a specific set of best practices in managing the path taken as they sent each call onward. Specifically, having discovered that employing multiple downstream providers in the call path was at least one significant cause of rural call failures, the safe harbor dictated a limit on the number of providers that could be used to reach the destination.

The RCC effort has been at least partially successful, less so for the utility of the reports that were generated, but because some providers opted into the safe harbor which resulted, as expected, in a lower rate of call failures to rural areas when those best practices were followed.[7]

One approach to implementing our proposal would be to mimic that used for RCC. We would like to see all providers embrace our actions 1 through 4 above. However, if it were not possible for the FCC to mandate all that, the reporting requirements (item 5) could be imposed on providers (as was the reporting requirement for RCC); that will give the FCC visibility to

[7] "Limiting the number of intermediate providers has proven to reduce the number of call failures. This 'best practice' is the bedrock of the 'safe harbor' and it, combined with the record keeping and reporting requirements, have mitigated call completion issues." Letter from NTCA/The Rural Broadband Association to Marlene H. Dortch, 12-October-2017, available at https://ecfsapi.fcc.gov/file/10120142507673/10.10.17%20FCC%20Ex%20Parte-Notice%20of%20NTCA%20meeting%20with%20WCB%20and%20EB%20staff%20on%20rural%20call%20completion%2C%20WC%2013-39.pdf

volume calling activity, highlighting points of origination that are indicative of caller-ID spoofing and indiscriminate dialing frequently associated with illegal robocalling. The other items could be part of a safe harbor; providers opting into that would be relieved of the reporting requirement. Participation in the safe harbor is more efficient – illegal calls get stopped before they propagate through the network so there's less need for traceback and enforcement. Providers get a choice and whichever path they choose, there is a significant public benefit.

We believe this approach will result in a measurable reduction in overall illegal robocalling and this will be reflected in the rate at which consumers file complaints. The proposal should be implemented expeditiously and, to the extent that certain aspects require a longer lead time, they should be phased in while the core of the proposal gets broadly activated. We'd like to see a rulemaking completed in six months and implementation complete in twelve. Notably, there is nothing that prevents a provider from adopting any or all of the practices herein prior to a formal rulemaking. The sooner they act, the more illegal robocalls get stopped.

As with RCC, the providers that are in the best position to address the robocall problem are the ones that accept originating calls from customers for termination to the USA PSTN. The "covered providers" from the RCC order "include LECs, interexchange carriers (IXCs), commercial mobile radio service (CMRS) providers, and VoIP service providers."[8] The order explains that "VoIP service providers" includes providers of both "interconnected VoIP service and one-way VoIP service".[9]

[8] In the Matter of Rural Call Completion, Report and Order and Further Notice of Proposed Rulemaking, FCC 13-135, para. 19.

[9] RCC Report and Order and FNPR, footnote 56.

With the engagement of these VoIP providers, we move closer to the source of the robocalls and greatly improve our ability to find and stop the illegal ones. As shown in Figure 1 above, the VoIP Services and Originating Carrier entities that funnel the calls onto the USA PSTN are in the best position to help mitigate these calls.

We hear often that there is no silver bullet for the illegal robocalling problem and that a combination of solutions is required. Our proposal complements other existing and pending efforts. Call blocking tools rely on Caller-ID and are defeated by random number spoofing; our proposal can greatly reduce illegal spoofing, making those blocking tools more effective and giving consumers more control over the calls they choose to receive. STIR/SHAKEN is a complex technology with several elements still being finalized. When that is done, it will take considerable time for originating providers to deploy the new technology. [10] It is initially applicable only for end-to-end SIP calls. Our proposal is a stepping stone for those providers. Providers can deploy our proposal now with existing technology and it is immediately applicable to both TDM- and VoIP-originated calls that terminate to wireline, mobile and VoIP subscribers.

DETAILS OF THE PROPOSAL

Robocalling has become a sophisticated and technically complex endeavor. The devil is in the details when it comes to finding and stopping illegal calls, while not interfering with the ability of legal callers to ply their trade. This section of the document, and the appendices, may

[10] In his 13-Oct 2017 ex parte filing, Richard Shockey, Chairman of the SIP Forum, states on slide 7 in his capacity as a consultant: “I repeat my personal belief outlined in my ex parte that STIR SHAKEN should be mandated” and “Nothing will deploy before 2019. It[‘]s just the way it works.” Available at https://ecfsapi.fcc.gov/file/1013653727266/Shockey%20Consulting%2017-97%20Call%20Authentication%20Trust%20Anchor%20exparte.pdf

challenge the patience of a lay reader. We welcome input from telecom technical professionals in refining this content.

Key to our proposal is that all USA PSTN calls enter through a regulated provider. It is virtually impossible to place a call to a CenturyLink landline or a T-Mobile wireless customer or a Comcast home phone user unless the caller (or their agent) has established a business relationship with a regulated provider that serves as a gateway to our PSTN. This is true regardless of how the call is originated – traditional TDM (legacy) calls, as well as VoIP-originated calls.

This is true even for calls originating from other countries. When a Vodafone subscriber in the UK places a call to a USA Sprint customer, Vodafone might hand that call off to Verizon, which would be their gateway to the USA network, and Verizon would pass the call to Sprint. Similarly, a business in the UK might subscribe to SIP trunking service from British Telecom; when one of their users calls a USA Frontier number, BT could send the call to AT&T, which is their gateway to the USA PSTN and sends the call on to Frontier. Or, because that business makes lots of calls to the USA, they might get a SIP trunk from USA-based Bandwidth.com; the business would send their calls via the internet to the USA, and then Bandwidth would be the gateway onto our PSTN.

Common Characteristics of Illegal Robocall Campaigns

The most prolific illegal robocallers are making tens of thousands or hundreds of thousands, or even millions of calls per day. The originating provider is best positioned to observe that concentration of calls, which will stand out for several or all of the following characteristics:

1) *High call rate.* Consumers and small businesses that are heavy phone users might make dozens of calls per hour, while a large business might make several hundred. Robocallers are making dozens or hundreds of calls per MINUTE, continuously throughout the day.
2) *Large fraction of short-duration calls.* Calls that are welcomed by the recipient typically last a few minutes or longer; some are shorter (including those from callers that abandon the call if they reach voice-mail). Unwanted robocalls are typically quickly terminated by the called party; most (but not all) robocallers try to detect voicemail and instantly disconnect. Thus, a robocaller will typically have a much higher fraction of short-duration (less than 30 seconds) calls compared to other callers.
3) *Large fraction of calls to invalid numbers.* Consumers and businesses are almost always calling memorized numbers or those stored in a validated electronic directory; few of their calls are rejected as being invalid. Many robocallers call random or sequential numbers or use outdated call lists, resulting in many calls to out-of-service numbers.
4) *Many different originating numbers.* Calls placed from homes and mobile phones carry the corresponding caller-ID; those from businesses originate from a small universe of numbers associated with the business. Legitimate robocallers will use one or a few numbers identifying their business. Illegal robocallers are increasingly resorting to neighbor spoofing and other randomization of their caller-ID; this can be recognized by a higher ratio of unique caller-IDs to total number of calls placed.

Reporting Requirements

Our reporting requirements, detailed in Appendix A, dictate that Originating Providers examine their call records, looking for customers whose calling patterns might fit the profile of an illegal robocaller. The reports we require will show, hour by hour, high volume callers and the associated metrics indicated above. We cast a wide net, meaning that we set low reporting thresholds. We do this for two reasons. First, we do not want robocallers to be aware of our limits and adjust their calling patterns to avoid appearing in the reports. Second, we want to learn from the reports and inform the future refinement of reporting requirements and mitigation best practices. We propose that these reports be filed confidentially with the FCC, and that the FCC use internal and contracted talent to mine the data for actionable follow-up. That follow-up could include going back to the reporting provider(s) for additional information, or releasing aggregated data to help providers and others pursue complementary mitigation efforts.

Even with our wide net, we expect that many providers will have little or nothing to report, because they have few or no volume callers.

Note that in many cases, a robocaller will blend their calls with other legitimate traffic, often purposefully so that the overall traffic pattern is not blatantly problematic. We also know that some robocallers split their traffic across several originating providers to further obfuscate their activities. Collecting sufficient detail will allow the reporting requirements (and our best practices, discussed next) to be adjusted with time to detect at least some of these efforts.

Our proposal requires that the reports be timely submitted monthly. Many robocalling campaigns start and end rapidly. Timeliness of reports will allow investment, mitigation and enforcement efforts to be undertaken reasonably quickly.

We realize that monthly reports with the level of detail shown in Appendix A sounds like a monumental reporting task. But these reports will be generated and filed automatically.

Once the reporting logic is implemented, the computer power to run it is tiny. Providers are already generating Call Detail Records with dozens of fields and presenting these to their customers nightly or even in real-time. We welcome feedback from providers regarding the effort to generate the reports versus the magnitude of the robocalling problem.

While our reports will not include identifying customers by name, the reports will give the FCC sufficient information to launch deeper investigations. Typically, an investigation would start by going back to the provider for additional information associated with suspicious entries in a report. Our proposal mandates that providers keep detail underlying the reports (including customer identification) for 24 months, in case it is needed to support those investigative (and enforcement) efforts.

Signaling Requirements, Controls, and Cooperation

The other key elements of the proposal are the signaling requirements, spoofing and volume calling controls, and investigative cooperation. In the RCC analogy, this is the safe harbor into which providers can opt. It is detailed in Appendix B. Providers implementing this set of best practices could be exempted from the reporting requirements just explained.

1) Limits on number of simultaneous calls and call initiation rates. As explained above, very few customers (besides robocallers) need to place large numbers of calls simultaneously; nor do they need to make calls at high rates (amounting to tens of thousands or more calls per day). Most modern switching systems allow setting call limits on a customer-by-customer (or trunk-by-trunk) basis. Providers should, by default, set the limits high enough that normal customer traffic is not impeded, but low enough that high-volume robocalling is prevented. Many providers already have

such limits and disclose them in their terms of service or individual customer agreements.

2) Screening of Caller-ID. The vast majority of callers do not need to spoof their caller-ID; they use the caller-ID assigned to them by their phone company. Originating Providers should screen the caller-ID supplied by the calling customer to ensure that it is on a list of numbers assigned by the provider to that customer.

3) Use of Charge Number. The legacy telephone signaling system (SS7) supports several numbers associated with the calling party. Caller-ID (technically, Calling Party Number) is discussed routinely in this proceeding. But Charge Number (also sometimes called Billing Telephone Number or Automatic Number Identification) is a standard element of the protocol.[11] Historically it was used for billing purposes; for single-party lines it would be identical to the Caller-ID. For businesses, Charge Number might be the main listed number while Caller-ID would be the dialable extension of the individual placing the call. Charge Number is now less often used, but it should be resurrected and populated by the Originating Provider with a telephone number tied (by that provider) to the calling customer. Caller-ID is what is displayed to the called party; Charge Number is captured internally by interexchange providers. This can facilitate the tracing of spoofed calls to their origin by providers in the call path. For calls that are propagated using VoIP, the SIP protocol provides the P-Charge-Info header, which is converted to and from the SS7 Charge Number information element when a call transitions between legacy SS7 and SIP.

[11] ANI and Charge Number were discussed in the context of Caller-ID privacy features in 1994-1995. See, for example, https://apps.fcc.gov/edocs_public/attachmatch/FCC-95-187A1.pdf.

4) Use of Redirecting Number. This SS7 information element is used when a call is forwarded. For example, if a call from 212-555-1234 is placed to 415-555-6000, and 415-555-6000 forwards that call on to 206-555-7788, the second leg of the call would have the original Caller-ID, 212-555-1234, but ALSO a Redirecting Number of 415-555-6000. The called party at 206-555-7788 will see the original calling number, 212-555-1234, on their caller-ID display, even though that original 212 caller did not directly dial the 206 number. If the call is reported as abusive, the terminating provider can use the Redirecting Number to know the source of the call to the 206 number. Originating Providers should insure that redirected calls carry a valid Redirecting Number. The SS7 Redirecting Number information element is interworked with the SIP Diversion header.

5) Exception to Call Rate Limit. The vast majority of customer traffic will be compliant with the default parameters we propose. For those few customers that need to place more calls per minute than we normally allow, an Originating Provider must: (a) obtain from the customer and retain on file an explanation of the calls being placed and an explicit affirmation that they are fully compliant with all applicable laws and regulations; (b) verify that the allowed Caller-ID values (see (2) above) are dialable and appropriately answered with the name of the calling entity; (c) ensure that the calls are placed with the Caller-ID privacy indicator set to "off" (number is NOT marked private). While many provider terms-of-service or customer agreements already carry prohibitions against illegal calls, best practices would include specific mention of prohibitions on automated calls to mobile phones, compliance with do-not-call lists, and other oft-violated requirements.

6) Exception to Caller-ID Screening. Caller-ID spoofing (that is, using a Calling Party ID other than one belonging to the originator) should only be allowed for low-volume calling, or if a Redirecting Number belonging to the originator is included. We know that some call centers and other businesses, as part of their legitimate business, use an interexchange carrier that is not the carrier of record for the number(s) they use as their outbound Caller-ID. In these cases, the IXC should vet and maintain a list of allowed Caller-IDs, and should also insert a Charge Number acquired by the IXC on behalf of the customer for this purpose.
7) Cooperation with traceback and investigation requests. The Originating Provider must agree to cooperate with FCC-sanctioned traceback efforts as well as inquiries directly from the FCC. This means timely response to valid inquiries without requiring a court order or other formalities. CPNI must be shared per the exception in the CPNI regulations.
8) Cooperating Provider. Our proposal allows Providers that are not regulated providers to voluntarily commit to the best practices documented here and document that to the FCC. We note that the RCC order included VoIP providers in their definition of "Covered Provider" so it may be that this extension is largely superfluous. An Originating Provider receiving traffic from a Cooperating Provider need not subject that traffic to the screens described here; instead, it is treated like traffic from a regulated provider and the upstream Cooperating Provider is responsible for making sure the traffic from each of their customers is compliant.

There will need to be exceptions to our rules and we've laid out criteria for documenting those when they occur. The process sounds cumbersome but our intent is that it be accommodated via secure on-line web forms that minimize the administrative burden for both providers and the FCC.

Our proposal here is applicable to calls that providers originate on behalf of their customers. Calls that are received by a provider from an upstream provider would not be covered by these requirements.

We also recommend that this proposal be extensible to allow cooperation with foreign regulators, widening the scope of coverage.

CONCLUSIONS

Some providers will complain that this proposal requires additional resources, and it does. Those resources are warranted given the scope of the problem – the most complained about issue at the FCC and the FTC. This proposal requires far less resource than STIR/SHAKEN, and yet no provider voicing an opinion has indicated that STIR/SHAKEN poses untenable resource requirements.

Some providers will lament that they do not want rules mandated upon them. By their failure to tackle this problem more effectively, they have demonstrated that they need regulatory persuasion to take reasonable, available steps. STIR/SHAKEN will also have to be mandated if it is to be effective, so this is just the initial part of the journey.

This document is lengthy because we have tried to provide detail sufficient for it to be scrutinized and discussed by industry experts. The engineers and regulatory professionals that must weigh in on this proposal should not be intimidated by the apparent complexity. The robocalling problem is complex and the devil is in the details. No doubt some of the details that we have provided will prove inefficient or unworkable and alternatives will be found.

This proposal does not require new equipment or technology or protocols. The FCC should expedite it through the rulemaking process and start a countdown clock ticking on implementation. Providers that are truly concerned about robocalling can implement the best practices documented here without waiting for regulations.

We invite constructive discussion from all stakeholders and recommend that the FCC convene a workshop to facilitate an interactive dialog.

Respectfully submitted,

DATED: October 26, 2017

/s/ David Frankel

dfrankel@zipdx.com
Tel: 800-372-6535

APPENDIX A
REPORTING REQUIREMENTS

Any Provider that accepts calls from a customer other than a provider covered by this Order for termination to a North American Numbering Plan number with an area code either assigned to a United States geography or designated as toll-free, must report with respect to those calls sent onward by the Provider, for each hour of each day of the calendar month, separately for each trunk:

A. The number of calls attempted; if less than 600 for that hour, no report is required

B. The number of calls answered

C. The number of calls reaching a busy user

D. The number of calls abandoned (disconnected from the originating end before being answered)

E. The number of calls failing (due to vacant number, out of service, congestion, or similar)

F. The number of unique values of Calling Party ID (or SIP From User) conforming to the NANP (ten digits, 1 followed by 10 digits, or +1 followed by ten digits)

G. The number of calls with a Calling Party ID not conforming to the NANP

H. The number of calls without a Calling Party ID

I. The number of calls with a Calling Party ID with the privacy indicator set

J. Total number of conversation minutes (after answer)

K. The number of answered calls disconnected after 30 seconds or less

L. The number of answered calls disconnected from the originating side

M. The number of answered calls disconnected from the terminating side

N. The number of simultaneous calls allowed on the trunk (or 0 if unlimited)

O. The number of call originations per minute allowed on the trunk (or 0 if unlimited)

P. The signaling used on the trunk (MF, SS7, ISDN, SIP, or other specified)

Q. Whether the trunk is bi-directional (one-way or two-way)

R. The transport layer for the trunk (physical: dedicated circuit (e.g., T-1 or optical); IP-private: private IP network; IP-public: public internet, wireless, or other specified)

S. Location of the originator customer (USA or international)

T. Nature of the originator (provider, end-user, other specified)

U. A unique identifier for the trunk

V. The date and hour (24-hour clock, UTC)

A trunk is defined as a physical or logical interface over which a customer signals calls and exchanges media. This could be a grouping of several physical circuits (for example, an ISDN Primary Rate Interface group comprised of four T-1's configured with two D-channels for signaling and 94 bearer channels). Another example would be a logical interface defined on the public internet that accepts SIP calls from two different remote IP addresses and exchanges media via RTP over the public internet. Trunk assignments should be consistent with the Provider's established practices and must not be altered to skew or evade the requirements here.

The report is due to the FCC by 10th day of each month (or the next business day if the 10th is a weekend or federal holiday) covering the preceding calendar month. Delivery is electronic in a format consistent with an example to be provided. Reports are confidential and available only to the FCC or its authorized agents.

APPENDIX B

CALL SCREENING AND SIGNALING REQUIREMENTS

A. Except as provided in (C) below, for each customer trunk provisioned for the termination of calls to NANP USA and toll-free locations:

1. Except as provided in (5) and (6) below, limit the number of simultaneous calls to no more than:

   a. For dedicated physical circuits, the bearer capacity of the circuit(s); that is, the number of calls that can coexist simultaneously on the circuit(s).

   b. For logical circuits, 24 for newly-provisioned customers; for established customers, the greater of 24 or the aggregate number of billed connection minutes over the trunk during the prior three months, divided by 25,000

2. Except as provided in (5) and (6) below, limit the number of call attempts per minute to a value not greater than the limit on simultaneous calls from (1) divided by 4.

3. Except as provided in (6) below, if the calls-per-minute limit in (2) is greater than 10, establish a set of one or more authorized originating numbers. Each number in the set must be allocated to the Provider in the Local Number Portability database, and assigned by the Provider to the customer serviced by the trunk; OR the Provider must verify that each number is assigned by another provider and assigned uniquely to the customer. Only send onward calls that include either a Calling Party Number or Redirecting Number or both, or the SIP equivalent, that is in this set.

4. Except as provided in (6) below, include in all calls sent onward a Charge Number allocated to the Provider in the Local Number Portability database. If the Provider does not have access to NANP numbers, then it will obtain from another provider number(s) for this purpose; when dialed, said number(s) will play a recording identifying the Provider and giving contact details.
5. If there is a business need to deviate, for a particular trunk, from the limitations set out in (1) or (2) above, the Provider will, prior to implementing the deviation:
    a. Document the rationale for the deviation
    b. Vet, using best commercial efforts, the legitimacy of the customer and their commitment to the legality of their calls
    c. Forward to the FCC a summary of the deviation and vetting process
    d. Retain the documentation in the Provider's file for 24 months
    e. Ensure that calls will not have the Calling Party Number marked private
6. If there are technical limitations that prevent implementation of the constraints in (1) through (4) above, the Provider must document same and submit it to the FCC, provided that it does not affect more than 100,000 call originations per month or 0.1% of the Provider's originated calls, whichever is greater. Otherwise, the Provider does not meet the Call Screening and Signaling Requirements. The Provider will update the documentation at least annually.

B. The Provider will establish a point of contact (office or individual) for fulfilling traceback and investigative requests regarding calls reported as abusive. The Provider will forward to the FCC an email address and telephone number to receive these requests. The Provider will respond to requests from the FCC and from FCC-designated industry groups (such as USTelecom) in no more than one business day for 90% of the requests presented in any calendar month, and within 3 business days for 100% of such requests, provided that if more than 3 requests are received in a single day, the fourth and beyond requests will not be included in the response time measurements. The Provider will be forthcoming with all available information without need for subpoena or civil investigative demand or other formality, and will release CPNI under 47 U.S. Code § 222 (d) (2).

C. The provisions in (A) apply to calls received by the Provider from a customer, but not to calls received from another provider independently subject to these rules. Further, a non-regulated service provider can voluntarily agree to be bound by these Screening and Signaling requirements via a filing to the FCC. The FCC will publish a list of these Cooperating Providers so that other providers can be aware of their status. A Cooperating Provider that revokes its filing must promptly notify the FCC and any providers through whom it places calls.