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
	)	FCC 20-96
To: The Commission	)	

FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING
Comments of ZipDX LLC

SUMMARY

In this fourth FNPRM, the Commission has solicited input regarding the affirmative and effective measures that voice service providers will be obligated to take to prevent origination of illegal calls. The FNPRM notes that stopping calls at the source is the most effective mitigation.

We explain that illegal robocalls generally fall into two distinct (but sometimes overlapping) categories: fraud and telemarketing. We propose that calling platforms and voice service providers (the companies that place these calls onto the USA network) incur legal responsibility for these calls.

Fraud calls are most often originated by foreign sources. We propose, as part of a safe harbor for providers, that foreign-sourced calls be prohibited from using USA Caller-ID values. This removes a level of credibility and makes it easier for potential victims and their service providers to recognize the calls.

For telemarketing calls, we propose restrictions on web-based consent since this form of consent is at the heart of many calling campaigns and is fraught with abuse. We note that

obligating providers to be liable for the calls incents them to be more vigilant about the customers they take on and the ways their platform is used (or abused).

BACKGROUND

At ¶80, the 4th FNPRM states: "We propose to establish an affirmative obligation for voice service providers to … take affirmative measures to prevent customers from originating illegal calls, and we propose to make clear that failure to comply with any of these affirmative obligations is unjust and unreasonable under section 201(b) of the Communications Act."

At ¶101, the FNPRM states: "We propose to require voice service providers to take affirmative, effective measures to prevent new and renewing customers from using their networks to originate illegal calls."

We address these points herein. The last half of ¶101 is crucial: "The most effective way of preventing illegal calls from reaching American consumers is by ensuring that those calls never originate on or enter the network. Only originating voice service providers and gateway providers can prevent this from happening." Anything we can do to eliminate these calls at the source lessens the burdens addressed elsewhere in the FNPRM: fewer calls to block, fewer calls mistakenly blocked or mislabeled. The worst enemy for everybody dealing with any aspect of this problem, including legitimate callers and regulators and network operators and of course consumers, is the originator of the illegal robocall.

In setting strategy for this war, it is crucial to understand the enemy. We are fighting against two distinct threats, although at first glance their missiles may seem similar:

- FRAUD callers use any ruse they can imagine to extort money from their victims.

- TELEMARKETERS are promoting some product or service or cause as part of a process known as lead generation.

In both cases, the strategy is to make a huge number of automated, low-cost calls, attempting to find a handful of individuals that will engage with a human working on behalf of the caller attempting to consummate the sponsor's transaction.

Most consumers do not distinguish between the two types of calls; each is just another unwanted robocall. Those of us engaged in the fight, however, must attack them quite differently. But the strategies converge as noted above: The most effective way to address these calls is to engage voice service providers to keep them out of our network to begin with.

FRAUD CALLS

A discerning listener can recognize a fraud call immediately from the message delivered. When the caller announces that they are from the Social Security Administration or Visa/MasterCard, we know that is false and that the call has nefarious intent. Most often, these calls originate outside the United States. They will usually use a caller-ID value chosen to look like it is geographically proximate to the called party, or a legitimate number belonging to a recognized institution (such as a Social Security office or a real issuer of credit cards).

To reach recipients, these calls must enter the US telephone network through a US-based Voice Service Provider – the "Gateway Provider." Gateway Providers accept these calls because they are paid to do so. (Some have argued that they are "compelled" to connect all calls; that is a fallacy. They accept calls per the terms of the Service Agreements and Acceptable Use Policies that they author and have wide latitude regarding the content.) Only an offsetting financial disincentive will compel them to be more judicious in the traffic they solicit and carry.

Establishing such a disincentive is the simplest, most practical, and effective way to disrupt these fraud calls. Specifically, we must discourage gateway providers from accepting calls from foreign sources that purport, via their Caller-ID, to originate in the United States.

We propose that the Commission accomplish this by stipulating that a provider will be deemed an "initiator" under the TCPA and any other applicable regulations (including Truth-in-Caller-ID) for calls not in compliance. Given that burden, the provider would likely contractually obligate his customer to indemnify that provider against any such claims and would perform sufficient diligence to be confident that the customer would make good on the indemnification.

Some providers might find that onerous, so we propose a safe harbor. A provider would be relieved of said responsibility, on a customer-by-customer basis, if it has:

1. Determined the domicile of their customer
    - For a publicly-traded company listed on a US stock exchange, via public records
    - Otherwise, by (a) confirming entity registration with the applicable Secretary of State per the customer's physical address in the USA and (b) verifying payment coming from an account in the customer's name at a US financial institution and (c) securing an image of a valid, current driver's license or identification card issued by a US state or territory matching an entity officer per the Secretary of State filing; records of which must be retained by the provider.
2. Treats as non-qualified:
    - any individual
    - any entity that has not been verified as US-based per (1) above

3. Prohibits by contract non-qualified customers from using automated calling technology (including a recorded voice), and proactively monitors for and mitigates such traffic.
4. Accepts a call from a non-qualified customer only if the Caller-ID value is:
    - Not in the North American Numbering Plan; or
    - An NANP number provided by and serviced by the provider, with outbound and inbound traffic for each number technically restricted to a uniquely-identified endpoint (e.g., handset or SIM) and to a level (concurrent calls and call attempts per minute) commensurate with conversational calling; or
    - Within the NANP but only if the NPA (Numbering Plan Area, or Area Code) is valid, corresponds to the domicile of the customer (without extension to the customer's customer), and is not a USA NPA nor an 8YY (toll-free) NPA.

No doubt there are other approaches that could accomplish the same objectives; hopefully others will be forthcoming with their specific counterproposals. Putting millions of daily calls onto the US telephone network is a powerful capability. With great power comes great responsibility. Providers that choose to go into this business must do so only when they have the wherewithal, including technical, operational and administrative resources to handle that responsibility; otherwise, they should limit their activities to functionality that does not invite abuse.

All stakeholders must recognize that this is an evolving space. Those perpetrating fraud are intrinsic liars. There is every reason to believe that they will fabricate responses to know-your-customer inquiries and will even forge state and federal forms and documents. The Commission (and providers) should anticipate revising rules periodically in response. Regarding legal authority, what is described above appears to be consistent with 47 USC § 201 and § 227.

TELEMARKETING

Generally, telemarketers have convinced themselves, and would like us to believe, that they are making their calls legally. Certainly there are some that are. But millions of daily calls are made with a fast and loose interpretation of the law which needs to be reined in.

The fringe telemarketers rely on a big exception to certain TCPA rules: calling with consent. It is well-documented that this arena, which includes a small industry called lead generation, is fraught with disputes. See, for example, this recent filing in CG Docket 02-278 regarding a Petition for Declaratory Ruling: https://ecfsapi.fcc.gov/file/1081372806755/sostrin%20ex%20parte%20letter.pdf.

Most problematic are callers that claim to have obtained consent via a web form – they insist that the called party visited a web site, asked to be called, and clicked on an acknowledgement specifically permitting automated dialing and pre-recorded or artificial voice announcements. Such claims are implausible when the caller is making millions of calls.

The most effective yet simple change the Commission can make is to refine its definition of "prior express written consent." Consent via web form must only be acceptable if it:

- Stipulates precisely one named seller to which authority to call is granted (a separate explicit web form submission would be required for each additional named seller), and
- Expires after three call attempts or fourteen days, whichever comes first.

This is consistent with the purported intent of such consents: the web visitor is interested in an insurance quote or to learn more about solar energy or for help with student loans. To the extent that a caller wants something less restrictive, they have several options:

- Communicate with the prospect via another channel (e.g., email)
- Have a human (rather than an automated system with a recorded voice) make the call
- Invite the prospect (via the web) to initiate a call towards the seller
- Obtain (and record and retain), as part of an initial call, an explicit consent to extension of time for future automated calls.

Further, we propose that any calling platform provider that delivers artificial or pre-recorded voice messages on behalf of a customer must bear responsibility for such calls under the TCPA, and must deliver proof of consent within 72 hours upon demand from the called party, law enforcement and regulators, or an authorized investigatory body. As noted earlier in our fraud discussion, this will motivate the platform provider to require its customer to indemnify it for such liability, and to know its customer sufficiently that it can comfortably rely on that indemnification. It will also motivate the provider to pre-screen the messages or scripts used by its client to ensure compliance with regulations.

A platform provider that is nervous about the liability it could incur due to abuse of its platform is in the best position to decide how to limit that exposure. It can modify the operation of its platform; it can be more selective about the customers with which it engages and the terms under which it does so; and it can be more diligent in screening and monitoring its customers' activities. All of these are fully under the control of the platform provider.

TECHNICAL REFINEMENTS

The Commission should take this opportunity to make two technical refinements to existing regulations, given that the existing language has proven problematic.

With respect to Truth-in-Caller-ID: Append to 47 CFR § 64.1604 (a): "A call containing caller identification information that is not assigned to the calling party, or is used without the express permission of the owner or assignee of that information, is presumed to be in violation."

With respect to automated message content, at 47 CFR § 64.1200 (b)(1), change the words "At the beginning" to "Within 15 seconds of the start". Change "State Corporation Commission (or comparable regulatory authority) must be stated" to "State Corporation Commission (or comparable state-level authority) and the city and state where the entity is located must be stated with cadence and clarity comparable to the rest of the message."

ANTICIPATED CONSEQUENCES AND REACTIONS

We expect providers to bristle at being asked to: take on new liabilities; deploy additional resources on diligence and risk mitigation; revise contractual language; and turn away potential new customers. Any business would. Illegal robocalling is a persistent, massive problem that requires attention on several fronts; there will be associated costs. SHAKEN/STIR is a massive industry undertaking costing huge sums. What is proposed here complements (but does not duplicate) that effort at a fraction of the cost. All these efforts contribute to restoring trust in our telephone network, which ultimately benefits the entire ecosystem. The cost is worth the reward.

We have proposed essentially that any call using a USA caller-ID must have an American sponsor. Some mobile operators will complain that this impedes Americans roaming in a foreign country, but this is likely overstated. Calls from roamers using WiFi calling or Voice-over-LTE will be sent back in data form to their US-based provider, who will validate and originate the calls as if the subscriber were at home – so not impacted. Some effort will have to be put into accommodating foreign roamers using legacy foreign networks; this is, we contend, manageable.

US entities operating foreign call centers may complain that those centers will not be able to display valid US caller-ID. But that is not the case. If, for example, Wells Fargo Bank has a call center in Ireland, that Irish center can place their calls over a VPN or other secure route to a US provider that has agreed to accept the calls on Wells' behalf. Or the call center could send the calls to Wells in the US, who would then send the calls onward. The crux of the proposal here is that Wells takes responsibility for calls purporting to come from Wells; Wells is the US provider's customer (not the foreign-based call center).

These are relatively small prices to pay if the overall proposal can put a major dent in fraudulent calling.

We are concerned about the ease with which fraudsters may be able to instantiate themselves as US-based when in fact they are not. Our Safe Harbor may be too lenient, discouraging providers from doing sufficient vetting on new customers. A probationary period with call volume limitations and traffic monitoring may be appropriate, or some other refinements.

All providers would still be subject to existing regulations, including the Commission's recent Third Report and Order in this docket, whereby origination of illegal calls can cost a provider their ability to send traffic downstream. Our explicit goal with the proposal here is to prevent that traffic from getting on the network to begin with.

Respectfully submitted on behalf of ZipDX LLC,

DATED: August 30, 2020

/s/ David Frankel

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