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

In the Matters of	)	
	)	
Implementing Section 503 of RAY BAUM's ACT	)	WC Docket No. 18-335
	)	
Rules and Regulation Implementing the Truth in Caller ID Act of 2009	)	WC Docket No. 11-39
	)	
	)	
To: The Commission	)	

JANUARY 2019 WRITTEN EX PARTE COMMENTS OF ZipDX LLC
RE ANTI-SPOOFING NPRM

Submitted to the Record

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

Filed: January 22, 2019

This document is submitted to the record, and also e-mailed to:

Zenji Nakazawa, Advisor to Chairman Pai

Travis Litman, Advisor to Commissioner Rosenworcel

Jamie Susskind, Advisor to Commissioner Carr

Arielle Roth, Advisor to Commissioner O'Rielly

Commissioner Starks

Eric Burger, CTO

On January 30, 2019 the Commission is scheduled to consider an NPRM to implement changes to its Truth in Caller-ID regulations reflecting recent legislation.

When the Commission adopted the 2011 Report and Order implementing the original Truth in Caller-ID act, it promised: "Once the Commission's rules are in force, we will have the opportunity to determine whether the current rules are sufficient to deter malicious caller ID spoofing. If they are not, we can revisit the issue." The rules are not sufficient. Now is the time to make good on this promise.

In the ten years that have elapsed since passage of the original Caller-ID Act, nefarious uses of the public telephone network have proliferated. Countermeasures have evolved, but the scammers move at an even faster pace. The FCC plays a critical role in implementing regulations that provide explicit direction and guidance to fulfill legislative intent. American consumers and all other stakeholders expect the FCC to apply its expertise and assume leadership.

Given how infrequently the Caller-ID rules are revised, this NRPM must go beyond the minor adjustments driven by the RAY BAUM's act. It needs to reflect what we now know, and anything we can anticipate, about how Caller-ID can be misused to public detriment.

Specifically, the Commission should direct the Bureau to revise the NPRM to include the following objective points prior to publication in the Federal Register:

1) A calling number must be one that is assigned to the caller or is used with the explicit permission of the party to which the number is assigned.
2) An entity that accepts a call for onward connection must have in place an effective practice limiting improper use of calling number or share in culpability for such misuse. Compliance will protect service providers from overzealous enforcement.

Incorporating these critical revisions (which are consistent with other Commission initiatives including STIR/SHAKEN) into the NPRM will reflect the Commission's stated commitment to addressing the scourge of illegal robocalling and other telephony abuses. Doing this now will maximize the opportunity for public comments relating to improvements and refinements.

The sections that follow provide additional detail.

Brief History of Caller Identification Service, Technology and Spoofing

Contrary to what many believe, Caller-ID spoofing – that is, placing a call using an originating telephone number other than that assigned by the telephone company to the calling customer – was not uniquely enabled by VoIP telephone services, and it is not inherently unstoppable in VoIP or legacy calling environments.

The Commission's Caller-ID Report from eight years ago (DA 11-1089, June 2011, page 5) does a good job of explaining the history of caller identification services. The report explains that it started in the 1980's with the deployment of Signaling System 7 (SS7) and has evolved as VoIP and SIP have emerged as complimentary and interworked services.

The Report explains that in SS7 and subsequently VoIP, the originating provider can screen, validate or substitute the caller identification value. Some VoIP implementations do not permit spoofing. Others do no validation or screening and simply pass whatever the customer supplies. The Report at page 8 cites examples of providers that restrict or validate the calling number and others that do not.

As the Report explained in 2011, and still true today, the ability to spoof a calling number is not, primarily, a function of the technology used. It is a function of policy and configuration on the part of the originating provider.

The Report (page 13) also explains how the Calling NAME function was originally implemented, and how it can be abused (page 14). Similar abuse is possible in some end-to-end SIP calling scenarios where it is possible for a Display Name chosen by the originator on a call-by-call basis to appear as the Calling Name to the recipient.

The protocols used for Text Messaging are distinct from those used for Voice, but the issues with caller identification are in many ways analogous.

What is Spoofing?

The Draft NPRM uses the terms "spoof" or "spoofing" without definition. The 2011 Report at footnote 3 says: "We use the term 'spoofing' in the popular sense of knowingly using identification information to masquerade as a different person or entity."

At paragraph 4, the 2011 Report says: "The accompanying growth of *caller ID manipulation, or spoofing*, has brought with it increased concerns about security, privacy, and other consumer harms." (Emphasis added)

The FCC website at https://www.fcc.gov/consumers/guides/spoofing-and-caller-id says: "Caller ID spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity."

SpoofCard, a commercial caller-ID manipulation service offered to the public, has a detailed discussion of spoofing at https://www.spoofcard.com/blog/caller-id-spoofing/. They explain: "Caller ID spoofing is the technology that allows you to alter the information forwarded to your caller ID in order to hide the true origin ID of the phone call. In simpler terms, caller ID spoofing allows you to display a phone number different than the actual number from which the call was

placed. Caller ID spoofing technology works for both phone calls and text messages on your smartphone."

Verizon, at https://www.verizonwireless.com/support/knowledge-base-218765/, says: "Caller ID spoofing is the process of changing the Caller ID to any number other than the actual calling number. Caller ID spoofing happens when a caller knowingly falsifies the info transmitted to disguise the number they're calling from."

Of all the definitions listed, Verizon's is closest to a "technical" explanation – but it highlights a further technical complication: What is "the actual calling number"? For cases like VoIP Termination (used by businesses) and Skype Out (used by consumers), there is no obvious "actual calling number" because these services by themselves do not enable the customer to receive calls and thus do not dedicate an assigned number to the service.

While these definitions vary in their scope and technical precision, this is the common thread: Spoofing is the use of a calling number not assigned to the caller.

Allowed Spoofing – Number Used with Permission

The Draft NPRM at paragraph 4 explains that spoofing may be legitimate in some situations. Here are three examples:

1) Outbound calls from a domestic violence shelter can't disclose the shelter's location. The shelter gets permission to use instead the number of the county social services department in another part of town.
2) A physician doesn't want his mobile number disclosed when he contacts patients after hours about their test results. He arranges for the calls to appear as if they came from his main clinic number.

3) A nationwide drugstore chain uses a business process outsourcer to make prescription reminders from a call center in Alabama. Knowing that customers won't recognize that number or location, the chain wants the calls to appear to come from the nearest local store. They give a list of store telephone numbers to their BPO, along with an express grant of permission to use the numbers for this purpose.

Each of these scenarios is allowable because the spoofed number is being used with the explicit permission of the party to which it is assigned. There is no intent to defraud or cause harm, and nothing is being done wrongfully to obtain something of value.

Critical in all of these cases is that the spoofed number is used with permission. This is an objective standard. The number cannot belong to some unwitting third party; that would likely cause harm to that party (in the form of brand defamation, or unwanted and misdirected callbacks – as so often happens in the case of neighbor spoofing by robocallers).

Regulatory History with respect to Service Providers

In accordance with the statute, the Draft NPRM proposes on page 15 a revised §64.1604(a): "No person or entity … shall, with the intent to … wrongfully obtain anything of value, knowingly cause, directly, or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information in connection with any voice service or text messaging service."

By its wording, the scope of this prohibition includes the service providers that carry the call from its point of origination to the call recipient.

When a caller places a call via Originating Provider A, who passes the call to Transit Provider B who delivers the call to Terminating Provider C who delivers the call to the

Recipient, each of providers A, B and C is somehow being compensated for their service ("obtaining anything of value").

If any of those providers is aware that the caller identification information is misleading or inaccurate, then they are acting knowingly and operating wrongfully.

The Draft NPRM at footnote 9 references the Truth in Caller ID Act of 2010, Report of the H. Comm. on Energy & Commerce, H.R. Rep. No. 111-461. At the bottom of page 7, that report states:

> *The Committee intends that the Commission's authority to promulgate rules under subsection (e)(3) includes the authority to specify exemptions from the prohibition where the requisite intent of the statute is not met, for example where the carrier or provider is merely transmitting the information it receives from another carrier, provider, or customer. Furthermore, the prohibition is not intended to stifle innovative new services such as pick your own area code, location, or call back number services.*
>
> *In the rulemaking conducted pursuant to subsection (e)(3)(A), the Committee anticipates that the Commission will consider imposing obligations on entities that provide caller ID spoofing services to the public. The widespread availability of caller ID spoofing services presents a significant potential for abuse and hinders law enforcement's ability to investigate crime. The prohibition in this bill of the use of such services with the intent to defraud or deceive could be of limited value if entities continue to provide these services without making any effort to verify their users' ownership of the phone number being substituted.*

In contemplating the original legislation, Congress intended that the FCC would make clear, with respect to service providers, what is permissible and what is not. Specifically, providers are allowed to pass onward information that is sent to them, but they have an obligation to make sure that their customers own the numbers they use.

The Draft NPRM at paragraphs 8-9 discusses four recommendations made by the FCC in its 2011 Report. The third was: "[G]iving the Commission appropriate authority to regulate spoofing services offered by third parties." Congress took no action on this recommendation; none was required. The Commission already has the necessary authority. It its 2011 Report and Order implementing the original Truth in Caller-ID Act of 2009 (available at https://www.fcc.gov/document/rules-and-regulation-implementing-truth-caller-id-act-2009) at paragraph 20, the Commission stated: "The person or entity that knowingly causes caller ID services to transmit or display misleading or inaccurate information may, in some cases, be a carrier, spoofing provider or other service provider, and we do not exempt such conduct from the purview of our rules."

The 2011 Report and Order includes a lengthy discussion of what obligations with respect to spoofing should be imposed on service providers. At Paragraph 40, it states:

> *We are very concerned about the harmful effects of caller ID spoofing done with malicious intent. We also recognize that requiring caller ID spoofing services to verify that users have the authority to use the substitute number would likely reduce the use of caller ID spoofing to further criminal schemes, and could simplify law enforcement efforts to determine who is behind a caller ID spoofing scheme. Likewise, the public would benefit from having third-party caller ID spoofing providers clearly and conspicuously notify their users about the practices prohibited by the Truth in Caller ID Act. However, we are not*

convinced that it is appropriate for the Commission to impose such obligations on third-party caller ID spoofing service providers ***at this time****. In crafting the Truth in Caller ID Act, we believe that Congress intended to balance carefully the drawbacks of malicious caller ID spoofing against the benefits provided by legitimate caller ID spoofing. The Act prohibits spoofing providers, like all other persons and entities in the United States, from knowingly spoofing caller ID with malicious intent. However, the Act does not expressly impose additional obligations on providers of caller ID spoofing services. Following Congress' lead, we decline to impose additional obligations on third-party spoofing providers* ***at this time****.* [Emphasis added]

At Paragraph 41, the 2011 Report and Order states: "Once the Commission's rules are in force, we will have the opportunity to determine whether the current rules are sufficient to deter malicious caller ID spoofing. If they are not, we can revisit the issue."

Much has been learned about caller-ID in the almost eight years since the Report and Order was released. The time is now to revisit the issue to address the explosion in unauthorized harmful spoofing.

Obligations and Protections for Service Providers

Service Providers that enable caller-ID manipulation play a key role in mitigating its abuse. Some providers hold themselves out specifically as spoofing services. Others offer simple outbound calling ("VoIP termination" in the world of internet calling) where the calling number is supplied by the customer and is merely passed onward by the provider without any validation – implicitly enabling spoofing.

A provider that merely passes along caller identification information that it receives from an upstream partner should not be forced to be culpable for caller-ID malfeasance. In fact, FCC regulations (§ 64.1601(a)) stipulate that intermediate providers "must pass unaltered to subsequent providers in the call path signaling information identifying the telephone number, or billing number, if different, of the calling party that is received with a call."

However, each provider must earn that immunity by having in place practices sufficient to mitigate the use of their platform as a conduit for improperly spoofed calls. That means they must not accept traffic from others that are known to be sourcing calls with wrongful caller identification. This prohibition must be carried all the way up the call chain. A provider claiming intermediate (rather than originating) status must cooperate fully and immediately with Commission and industry inquiries regarding any problematic traffic.

Immunity also requires cooperation with industry traceback efforts including promptly sharing the source of problematic calls under § 64.2005(d). A non-cooperating provider will be deemed the call originator subject to Truth in Caller-ID enforcement penalties. The Commission expects the industry to work together to preserve the integrity of the network, through traceback, sharing of best practices, naming of bad actors, and cooperation with enforcement authorities.

The onus is even greater on Originating Providers. They must take whatever steps are necessary to prevent their customers from originating calls with a caller-ID not assigned to the customer or used with the permission of the party to which the number is assigned; use of invalid or unassigned numbers is prohibited. Those steps could include, without limitation: validating and screening the number(s) the customer can use; substituting a known valid number (traceable by the provider to the customer and used instead of the value included by the customer, if any); call detail analysis to proactively identify suspicious calling patterns; vetting the customer prior

to enabling volume calling; contractual stipulations and sufficient monetary recourse to effectively prohibit abuse. Recognizing that abuse vectors are constantly evolving, each provider employs the measures appropriate for its business. The key requirement is that the provider prevents recurring patterns of abuse.

Where a provider's customer (be it retail, reseller, provider or otherwise) is outside the jurisdiction of the United States, that provider must be even more vigilant. Intermediate provider status cannot be claimed in this situation.

These provisions will give providers the objective guidance they need to earn necessary protection, while still obligating them to be proper stewards of the telephone network.

STIR/SHAKEN

Caller authentication via new STIR/SHAKEN protocols are being developed and rolled out by industry with encouragement from the Commission. Ultimately these new technologies will mechanize some of the concepts embodied here. The assignee of a telephone number will be able to electronically grant permission to another party to use their number, by transmitting a security certificate to the designee.

As we step into this new regime, service providers will still be responsible for vouching for the caller identification associated with calls originating or transiting their platforms.

Establishing a baseline for acceptable number sharing and associated service provider responsibilities and protections with today's relatively primitive caller-ID technology will inform future actions as STIR/SHAKEN is deployed in the years ahead.

Conclusion

Telephony abuse facilitated by caller-ID manipulation has been growing non-stop since the Commission first promulgated rules eight years ago. At that time, you promised that you would revisit the rules if they proved insufficient. They have and you must.

A new NPRM must not only address the statutory mandate from Congress, but it must also incorporate learnings since the original rules were adopted. The FCC must muster all its wisdom, insight and legal prowess to turn the tide on nefarious calling.

Acceptable spoofing must be objectively defined (number assigned to the caller or used with permission of the assignee). There must be an onus on all providers in the call path to prevent abuse, especially when they have been made aware of problematic calls. Providers need to know what they have to do to avoid ensnarement as a violator of the regulations.

Even with the changes highlighted herein, the proposed rules will not deter all abuse. There will still be burner phones and other avenues that render caller-ID useless. Revised Truth in Caller-ID rules cannot solve all the world's problems, but they must play the biggest possible role as one element in restoring credibility and utility in the United States telephone network.

Respectfully submitted,

DATED: 22 January 2019

/s/ David Frankel

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