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

Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices	))))	WC Docket No. 20-324

Reply Comments of ZipDX LLC

BACKGROUND

This proceeding was launched in response to the TRACED Act directive to the FCC to issue "*best* practices that providers of voice service may use as part of the implementation of effective call authentication frameworks *under paragraph (1)* to take steps to ensure the calling party is accurately identified." (emphasis added)

We note here two important aspects of this Congressional directive. First, Congress asked for BEST practices – not good practices or adequate practices, but BEST. Thus, in reviewing the NANC recommendations, we should all be striving to make sure they are truly the very best practices we can imagine.

A second aspect of the directive is the reference to paragraph (1) of section 4(b) of the Act. This paragraph mandates not only implementation of STIR/SHAKEN (section 4(b)(1)(a)) but also implementation of "an effective call authentication framework in the non-internet protocol networks of the provider of voice service." (Section 4(b)(1)(b)) Thus, the scope from Congress goes beyond STIR/SHAKEN (until STIR/SHAKEN addresses voice calls that are not IP end-to-end).

With this background in mind, we offer this Reply to some of the comments submitted to date.

Regarding USTelecom's Comments

As we (and they) have previously, USTelecom advocates that a Robocall Mitigation Program be mandated even when STIR/SHAKEN is deployed. USTelecom cites a reference in

the NANC report (p. 18). We wish to emphasize this recommendation, and also note that NANC in their Executive Summary (p. 5) says: "Service providers, whether IP- or non-IP-based should have ongoing robocall mitigation programs in addition to implementing call authentication protocols."

With these statements, industry experts are saying that an effective call authentication FRAMEWORK must include not just implementation of a protocol (STIR/SHAKEN) but an adoption of a thoughtful program that incorporates that protocol in a way that will best meet the overall objective. STIR/SHAKEN alone does not make for a comprehensive call authentication framework.

Regarding Inteliquent's Comments

We are sympathetic to Inteliquent's concern regarding NANC's recommendation that "Originating Service Providers should authenticate calls with attestation level A only when they can confidently attest that the End-User initiating the call is authorized to use the TN-based caller identity associated directly with the calling line or account of the End-User." (NANC at p. 5)

As we read NANC's sentence, it seems to conflate a *direct association* between the TN-based caller identity and the end-user placing the call (suggesting that the end-user is the owner of the number), versus an *authorization* from the TN owner granting that end-user permission to use the number. Inteliquent further expresses consternation about the definition of "customer" and "end-user." The sentence should be rewritten.

What is critical is that when a particular TN is used as the caller identity, it must be used only by the end-user to which that number is assigned, or by a caller to whom that end-user has granted explicit permission. Ideally, when that end-user-assignee grants such permission, it takes responsibility for all calls placed by the grantee using that number.

In attesting to level A, is the OSP's responsibility, as part of a BEST practice, to ensure that the actual usage is per the above. The BEST practice should not be relaxed just because this may, in some cases, be inconvenient or resource-intensive.

This seems clearer in NANC's paragraph 3.4 and is discussed in 3.6.1 without (apparently) drawing any conclusions. We believe that the BEST practice is for OSPs to limit, by default, the scope of caller-identity values that each caller customer is permitted to use. The default today, for most OSPs, is to allow callers to use any value they wish, which should be reserved only for the most reputable callers and even then only with an established understanding of the circumstances under which any given value will be used, and a monitoring program that alarms on potential non-compliance so that it can be investigated.

Inteliquent suggests that an overly rigorous BEST practice may force calls to lower levels of attestation (or to be rejected). Given that the congressional mandate is for best practices that providers "MAY use" (emphasis added), an OSP has flexibility to deviate from such practice. At the same time, the OSP must have the utmost confidence that its alternative practice delivers the same degree of assurance to the call recipient that the call has been placed with the full authorization of the number owner. Thus, the BEST practice sets the bar for the expected outcome, even if achieved in some alternate way.

Regarding Noble Systems' Comments

We generally agree with how Noble Systems walks through various scenarios in the context of the best practices. They point out that providers will need to be thoughtful and creative in their implementations, including consideration of who their callers are and what risks are involved. Different solutions will be appropriate in different circumstances, but always consistent with meeting the same objective as the best practice.

Noble points out (section IV) that when a TN cannot be validated, it should be attested at levels B or C. We want to emphasize that at the same time, an OSP that is unable (or too lazy) to validate and assign A-level attestation should not be able to wash their hands of an obligation to mitigate illegal calling.

And this is where we disagree with Noble and their section V, which states that a Robocall Mitigation Program is out of scope. We argue just the opposite. Noble says "While call authentication can be broadly described as a tool for mitigating robocalls, the phrase 'robocall mitigation' is now understood to be separate and distinct from STIR/SHAKEN implementation." Our collective objective is (illegal) robocall mitigation and STIR/SHAKEN is one tool in the

toolbox. The FRAMEWORK should be all-encompassing. Considering each piece separately when they are so intertwined just perpetrates ineffectiveness.

Noble writes: "Knowing the traffic patterns of such calls does not aid (nor hinder) the service provider with knowing the identity of the end-user or customer. In summary, it is not readily clear how monitoring the traffic patterns of such calls facilitates a service provider identifying the calling party." Monitoring traffic patterns gives a service provider insight into potential breaches of calling party integrity and informs further investigation. Monitoring DOES aid the service provider in identifying likely abuses of caller identity, the elimination of which is certainly an obvious goal of STIR/SHAKEN. Elimination of those cases where the caller is not who he says he is raises the value of caller identity for the remainder of calls.

General Items

Each of the entities submitting Comments are members of the Good Guys in the fight against illegal robocalls. We must remember that there is a cadre of others that are placing and enabling illegal robocalls by the millions. Fundamentally they are engaged in the business of fraud and are not respectful of rules, let alone what it means to be a contributing member of society. By their nature they are deceptive and misleading and looking for any avenue that will allow them to carry on their misdeeds.

Thus, those trying to operate legitimately need to raise the bar ever higher to screen out these misfits. That means going beyond an entry in the 499A database or cursory satisfaction of State AG vetting principles. BEST practices must embody the notion that service providers, especially when onboarding new customers or investigating those with suspicious traffic, must be necessarily suspicious when granting those customers access to services that are readily and frequently abused (such as high-volume calling and wide-open spoofing capability).

The NANC recommendations devote specific attention to foreign callers, and rightly so. Illegal robocalls include campaigns that violate various regulations but the most egregious are calls perpetrating fraud, and those calls largely originate from outside the USA. The BEST practices should set the highest bar for foreign-originated calls. US-based providers must be cognizant that fraudsters are adept at papering themselves as US entities when in fact they are

owned and controlled from elsewhere. The fraudsters do this specifically to avoid the scrutiny that they deserve, and we mjust not let them deceive us.

Whatever the Commission chooses to adopt in this initial action, it must include a methodology for periodically (and perhaps frequently) revising the practices so that they are indeed always BEST and benefit from collective learning as the illegal robocalling ecosystem evolves.

Respectfully submitted on behalf of ZipDX LLC,

DATED: October 26, 2020

/s/ David Frankel

dfrankel@zipdx.com

Tel: 800-372-6535