

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

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

**COMMENTS OF INTELIGENT, INC.**

Inteligent, Inc. (“Intelligent”), by counsel, files these Comments in response to the Commission’s Public Notice<sup>1</sup> seeking comment on the recommendations of the NANC Call Authentication Trust Anchor Working Group (“CATA Working Group”) in the Report on Best Practices for the Implementation of Call Authentication Frameworks (the “Best Practices” or “Report”).<sup>2</sup>

Intelligent’s comments concern the circumstances under which the Report proposes to allow a SHAKEN Originating Service Provider (“OSP”) to assert full attestation (also known as “A”-level attestation) for calls. The Report articulates the correct principles in this regard, namely, an OSP should assert full attestation only if the call passes a customer identification and vetting procedure, as well as what the Report calls a “TN Validation” procedure to ascertain that the calling telephone number (TN-based caller identity) is being used legitimately. Intelligent is concerned, however, that the recommended Best Practices would operationalize these principles

---

<sup>1</sup> Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices, WC Docket No. 20-324, Public Notice, DA 20-1154 (Oct. 1, 2020).

<sup>2</sup> See Call Authentication Trust Anchor Working Grp., N. Am. Numbering Council, Best Practices for the Implementation of Call Authentication Frameworks (2020), <http://nanc-chair.org/docs/CATAWGReport-August2020DRAFT.pdf> (“Best Practices”).

in ways that inappropriately exclude multiple categories of legitimate call scenarios from receiving full attestation.

In taking this unduly narrow approach to full attestation, the Report’s proposal deviates from ATIS Standard ATIS-1000074-E<sup>3</sup> and ATIS Technical Report ATIS-1000088,<sup>4</sup> which through agreed-upon terms and descriptions of calling scenarios, appropriately envisioned a broader application of full attestation to legitimate calls. Consistent with the ATIS standards, Inteliquent urges the Commission to recognize that there are many legitimate call flows where a TN is not “associated directly with the calling line or account of the End-User,”<sup>5</sup> and that SHAKEN attestation relates to the service provider’s Customer, not necessarily the “End-User.”

**I. The Best Practices Suggest Allowing “A” or “Full Attestation” Under More Narrow Circumstances Than the ATIS Standards.**

The Best Practices suggest allowing “A” or full attestation only when the OSP “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.”<sup>6</sup> But this is a more narrow scenario than anticipated by the ATIS standards. Section 3.1 of the Best Practices quotes the ATIS-1000088 definition of “TN-based caller identity” which states that “the caller identity

---

<sup>3</sup> Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000074-E, ATIS and SIP Forum (2019), [https://access.atis.org/apps/group\\_public/document.php?document\\_id=46536](https://access.atis.org/apps/group_public/document.php?document_id=46536) (“ATIS-1000074-E”).

<sup>4</sup> See A Framework for SHAKEN Attestation and Origination Identifier, ATIS-1000088, ATIS and SIP Forum (2020), [https://access.atis.org/apps/group\\_public/download.php/51435/ATIS-1000088,%20A%20Framework%20for%20SHAKEN%20Attestation%20and%20Origination%20Identifier.pdf](https://access.atis.org/apps/group_public/download.php/51435/ATIS-1000088,%20A%20Framework%20for%20SHAKEN%20Attestation%20and%20Origination%20Identifier.pdf) (“ATIS-1000088”).

<sup>5</sup> See, e.g., Best Practices at 5 (explaining, contrary to Inteliquent’s view, 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.”).

<sup>6</sup> *Id.*

may be set to an identity other than the caller's Calling Line Identification or Public User Identity."<sup>7</sup> This reference acknowledges that the calling TN is in many cases not an unambiguous identifier of the calling entity. The standards documents and other industry reports recognize that there are many legitimate cases where a calling TN is not "associated directly" with a "calling line or account" of the entity initiating the call.<sup>8</sup>

Thus, the Best Practices may needlessly limit the ability to enable full attestation, which is detrimental to a variety of legitimate calls. For example, the Best Practices may preclude full attestation where an enterprise uses an assigned TN through multiple service providers or where an enterprise contracts with call center operators who place calls on the enterprise's behalf (for instance delegating its own main number to be sent as the TN-based caller identity) through the call center's service providers. In an indirect origination scenario as described in the Best Practices as well as ATIS-1000088, a calling TN could also be associated with the account of the directly-connected Customer (e.g. a value-added service provider) and made available for an End-User's calls. With proper authentication, these call flows should be able to receive full attestation, but the Best Practices may not allow it.

Instead of defining legitimate calling TN usage narrowly, Inteliquent recommends that the Best Practices state that the OSP should validate the association of the calling TN to the calling entity regardless of the usage scenario. In some cases, the OSP will be able to determine

---

<sup>7</sup> Best Practices at 6.

<sup>8</sup> *See, e.g.*, ATIS-1000074-E at 9 7 n.1 (explaining, for example, that legitimacy of the use of the number can be determined using a variety of mechanisms, including "[t]he number was assigned to this customer by the signing service provider, [t]his number is one of a range of numbers assigned to an enterprise or wholesale customer, [t]he signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number), [and] [t]he number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe").

the association through locally available information, and in some cases it will need information from the Customer, TN providers, or outside vetting and information services to make that determination. Although certain call flows may require the OSP to take additional steps, industry should be encouraged to provide full attestation where appropriate, rather than excluding such calls because of a “Best Practice” that is too narrowly defined.

## **II. Defining Attestation Levels in Relation to the End-User, Which is Not Necessarily the OSP’s Customer, Will Needlessly Limit Full Attestation.**

SHAKEN defines the attestation levels based on the OSP’s relationship to its directly connected Customer or service provider because that is the entity with which the OSP has a direct commercial relationship.<sup>9</sup> This ensures that the Customer can be held accountable for calls they send (whether the Customer is the ultimate source of the call or not). The Best Practices, however, seem to redefine the attestation framework in relation to the End-User, whether or not the End-User is the OSP’s Customer.<sup>10</sup> The Best Practices therefore imply that each OSP must definitively identify each indirect calling entity and determine each entity’s calling TNs before asserting full attestation, even though the OSP and calling entity have no

---

<sup>9</sup> *See, e.g.*, ATIS-1000074-E at 9 (explaining that for full attestation, the signing provider shall satisfy, among other requirements, that it “[h]as a direct authenticated relationship with the customer and can identify the customer”).

<sup>10</sup> *See, e.g.*, Best Practices at 22 (explaining that “[t]wo essential qualifications of the A-level attestation listed in ATIS-1000074 are that the signing service provider: [c]an identify the End-User [and] [h]as established a verified association of the End-User with the telephone number used for the call”). ATIS-1000074, however, makes reference to the Customer and not the End-User. *See, e.g.*, ATIS-1000074-E at 9. In a footnote, the Best Practices explain that “[f]or alignment with terminology used in this document, some of the terms in this appendix have been modified from the original ATIS-1000074 text.”). Best Practices at 22, n.10. The terms “End-User” and “Customer,” however, are not necessarily synonymous as used in the industry. To avoid needless confusion, it is important that A-level attestation be available for authenticated “Customers,” not just “End-Users.”

direct business relationship. The Best Practices do not need to be so prescriptive to accomplish the goal of determining the legitimacy of the calling number and ensuring traceability of a call to an End-User.<sup>11</sup>

Under the existing SHAKEN definitions and framework guidelines,<sup>12</sup> an OSP can achieve the attestation goals through a variety of means, such as agreements that the Customer will perform TN Validation or use TNs assigned to the Customer, and agreements that the Customer will provide indirect call-originator identities when needed for enforcement. Alternatively, the OSP and Customer can jointly rely on trusted third-party services that vet caller identities and TN associations and may provide that information openly or on an anonymized basis for use in databases and/or in secondary authentication transactions (*e.g.* caller-signed PASSporT tokens). In these cases, the OSP may not directly have access to necessary information on entities with which it does not have a direct relationship, but the information is available from other parties. When the information necessary to enable full attestation is available, this should be sufficient to allow such attestation, even though the OSP does not necessarily have a relationship with the End-User.

---

<sup>11</sup> We also note that there is an outstanding question in the industry as to whether or not STI-GA-sanctioned SHAKEN service provider authority is going to be granted to many thousands of small entities who are not currently considered “service providers” but who resell voice services as an adjunct to other products such as cloud-based communications platforms. Where these entities continue to be excluded from receiving SHAKEN service provider credentials, they will still be considered “Customers” of one or more OSPs but not “End-Users.”

<sup>12</sup> *See, e.g.* ATIS-1000088 at 13 § 5.4.1.

## Conclusion

The CATA Working Group Best Practices in many respects provide a workable framework for caller ID authentication, but as drafted, the Best Practices risk inappropriately narrowing the scope of legitimate calls eligible for A-level, or full, attestation. The Best Practices do not need to narrowly define the conditions for full attestation in order to accomplish the goals of reducing caller ID spoofing and increasing traceability of calls to their source. Instead, any best practices should recognize the broader variety of legitimate call flows and the additional flexibility of the ATIS standards. This more pragmatic approach to attestation will advance the Commission's goals of reducing fraudulent calls by providing full attestation under more circumstances where it is warranted.

Respectfully submitted,

**INTELIQUENT, INC.**

By:  \_\_\_\_\_

Matthew S. DeNero  
Thomas G. Parisi  
COVINGTON & BURLING LLP  
One CityCenter  
850 Tenth Street, NW  
Washington, DC 20001  
*Counsel for Inteliquent, Inc.*

October 16, 2020