TRIENNIAL REPORT ON THE EFFICACY OF THE TECHNOLOGIES USED IN THE STIR/SHAKEN CALLER ID AUTHENTICATION FRAMEWORK

Prepared by the:

Wireline Competition Bureau

Submitted to the:

Senate Committee on Commerce, Science, and Transportation
House of Representatives Committee on Energy and Commerce

December 30, 2022

I. INTRODUCTION

Combatting illegal robocalls continues to be one of the Federal Communications Commission's (FCC or Commission) top consumer protection priorities. Illegal caller ID spoofing is a particularly noxious practice whereby bad actors falsify caller ID information to deceive call recipients into believing the caller is someone they trust,[1] exposing consumers to fraudulent and malicious activity.[2] In 2019, recognizing the scope of the problem posed by illegal robocalls and caller ID spoofing,[3] Congress passed the TRACED Act.[4] Among other provisions, the TRACED Act directed the Commission to require voice service providers to implement the STIR/SHAKEN caller ID authentication framework.[5] Caller ID authentication combats illegally spoofed robocalls by allowing providers to verify that the caller ID information transmitted with a call matches the caller's number.[6] The Commission's rules implementing the TRACED Act required voice service providers to fully implement STIR/SHAKEN in the Internet protocol (IP) portions of their networks by June 30, 2021,[7] subject to certain extensions,[8] and the

[1] FCC, *Caller ID Spoofing*, https://www.fcc.gov/spoofing (last updated Mar. 7, 2022).

[2] *See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263, para. 48 (2020) (*First Caller ID Authentication Report and Order and Further Notice*) (noting that fraudulent robocall schemes cost Americans an estimated $10.5 billion annually).

[3] 165 Cong. Rec S7176-01, S7177 (Dec. 19, 2019) ("While their telephones were once a reliable means of communications, they have been turned against us. They are now mechanisms for scammers and fraudsters who wish to cheat and to defraud. The numbers are staggering. In 2019, consumers have received an estimated 54 billion robocalls. That is 6 billion more than 2018, and we still have 2 more weeks to go."); FTC, Consumer Sentinel Network Data Book 2021 at 12 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf ("American consumers reported a total of $692 million lost to fraud via phone call, with a median loss of $1,200."); NCLC Comments, WC Docket No. 17-97, GN Docket No. 17-59, at 4 (filed Aug. 17, 2022) ("Truecaller, the entity whose survey data the FCC cited to in 2020, released its estimate of nearly $40 billion in consumer monetary losses over the previous twelve months. As with the FCC's 2020 estimate, this updated estimate does not include nonquantifiable harms such as less reliable access to emergency healthcare communications and (continued and further) diminished trust in the U.S. telephone network caused by illegal robocalls.").

[4] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (TRACED Act).

[5] TRACED Act § 4(b)(1). In this proceeding, a "voice service provider" refers to a provider of "voice service," which is defined in relevant part in the TRACED Act as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan" and includes "without limitation, any service that enables real-time, two-way voice communications, including any service that requires internet protocol-compatible customer premises equipment . . . and permits out-bound calling, whether or not the service is one-way or two-way voice over internet protocol." *Id.* § 4(a)(2); *see also* 47 CFR § 64.6300(n). Commission rules define an intermediate provider, by contrast, as "any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic." 47 CFR § 64.6300(g).

[6] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1861, para. 3 (2020) (*Second Caller ID Authentication Report and Order*).

[7] 47 CFR § 64.6301; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3252, para. 24. The Commission also required intermediate providers to either authenticate any unauthenticated calls received on the IP portions of its networks that it will exchange with another provider as a SIP call, or both (1) cooperatively participate with the industry traceback consortium and (2) respond fully and in a timely manner to all traceback request is receives from the Commission, law enforcement, and the industry traceback consortium. 47 CFR § 64.6302(b).

[8] 47 CFR § 64.6304; *see also Second Caller ID Authentication Report and Order* 36 FCC Rcd at 1876-83, paras. 36- (continued….)

Commission has continued to work toward ubiquitous implementation of STIR/SHAKEN by all providers in the potential chain of a call.[9]

As directed by Congress in section 4(b)(4) of the TRACED Act, the FCC's Wireline Competition Bureau (Bureau) submits this report to "assess the efficacy of the technologies used for call authentication" in the STIR/SHAKEN framework.[10] Based on the record developed for this first triennial assessment, the Bureau concludes that, when the technical standards and protocols that comprise the STIR/SHAKEN framework are correctly applied, the framework effectively authenticates caller ID information as required to identify illegal spoofing.

II. BACKGROUND

A. The STIR/SHAKEN Framework

The STIR/SHAKEN framework[11] is a set of technical standards and protocols that enable providers to authenticate and verify caller ID information transmitted with Session Initiation Protocol (SIP) calls.[12] The framework involves two components. The first is the technical process of

(Continued from previous page)

51. These include an extension until June 30, 2022 for "non-facilities-based" small voice service providers and June 30, 2023 for "facilities-based" small voice service providers. The Commission shortened the extension for non-facilities-based small voice providers because it determined that they were at a heightened risk for originating illegal robocalls. *Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, FCC 21-122, at 12, para. 23 (rel. Dec. 10, 2021) (*Fourth Caller ID Authentication Report and Order*). As used herein, the term "non-facilities-based small voice service provider" means "a small voice service provider that is offering voice service to end-users solely using connections that are not sold by the provider or its affiliates." *Id.* at 9, para. 19; 47 CFR § 64.6300(h).

[9] *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order, Fifth Report and Order, Order on Reconsideration, Order, Seventh Further Notice of Proposed Rulemaking, Fifth Further Notice of Proposed Rulemaking, FCC 22-37, at 22-30, paras. 51-63 (May 20, 2022) (*Gateway Provider Order and Further Notice*) (expanding STIR/SHAKEN implementation obligations to gateway providers). "Gateway providers" are the domestic intermediate providers that serve as the point of entry for foreign calls into the United States. *Id.* at 12, para. 25. Rules adopted by the Commission in May 2022 require gateway providers to implement and begin using the STIR/SHAKEN framework by June 30, 2023. *Id.* at 28, para. 59; 47 CFR § 64.6302(c).

[10] TRACED Act § 4(b)(4)(A), (C) (directing the Commission to "assess the efficacy of the technologies used for call authentication under this section" not later than three years after December 30, 2019 and every three years thereafter, and to submit a report to Congress).

[11] A working group of the Internet Engineering Task Force (IETF) called the Secure Telephony Identity Revisited (STIR) developed several protocols for authenticating caller ID information. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7. Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *Id.*

[12] *Id.* at 1861-62, paras. 3, 6-7. The Session Initiation Protocol (SIP) is "an application-layer control protocol" "for creating, modifying, and terminating sessions" such as Internet Protocol (IP) telephony calls. IETF, *SIP: Session Initiation Protocol*, RFC 3261, at 1 (2002), https://tools.ietf.org/html/rfc3261. The STIR/SHAKEN caller ID authentication framework only works on IP networks—that is, those networks with technology that is able to initiate, maintain, and terminate SIP calls. *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3245, para. 7. Because the Commission has not yet mandated that providers implement any particular non-IP caller ID authentication technology, there is no implemented technology to assess for this triennial evaluation of the caller ID authentication framework and the Bureau did not seek comment on the subject. *Wireline Competition Bureau Seeks Comment on Two Periodic TRACED Act Obligations Regarding Caller ID Authentication*, WC Docket No. 17-97, Public Notice, DA 22-831, at 5 n.35 (WCB Aug. 5, 2022) (*Triennial Review Notice* or *Notice*).

authenticating and verifying caller ID information. This process relies on public-key cryptography to securely transmit the information that an authenticating provider knows about the caller and its relationship to the phone number it is using along with the call itself, allowing the terminating voice service provider to verify the information on the other end.[13] This encrypted information is contained in a unique part of the SIP message known as the "Identity header field,"[14] and includes an "attestation level" to signify what the authenticating provider knows about the calling party and its right to use the number in the caller ID.[15] Once added to the Identity header field, this information travels with the call to the terminating voice service provider.[16] When the terminating voice service provider receives the call with the Identity header attached, it can decrypt it, verify the caller ID information, and then use that information to protect its subscribers from unwanted and illegally spoofed calls.[17]

The second component of the STIR/SHAKEN framework is a certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call.[18] When an authenticating provider adds information to the Identity header, it must also include a digital "certificate," which essentially states that the provider is the entity it claims to be, the provider is authorized to authenticate the caller ID information, and the caller ID information transmitted by the provider is trustworthy.[19] To maintain trust and accountability in the providers that vouch for the caller ID information, a neutral governance system issues these certificates.[20] The STIR/SHAKEN governance system requires several roles in order to operate: (1) a Governance Authority, which defines the policies and procedures for which entities can issue or acquire certificates;[21] (2) a Policy Administrator, which applies the rules set by the Governance Authority, confirms that Certification Authorities are authorized to issue certificates, and confirms that providers are authorized to request and receive certificates;[22] (3) Certification Authorities, which issue the certificates used to authenticate and verify calls;[23] and (4) the

[13] *See First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6.

[14] *See Id.*; IETF, *Authenticated Identity Management in the Session Initiation Protocol*, RFC 8224, at 4, (2018), https://datatracker.ietf.org/doc/rfc8224/.

[15] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1863-64, para. 10. The current STIR/SHAKEN standards allow for three attestation levels. The highest level of attestation—called "full" or "A-level"—asserts that the authenticating provider can confirm the identity of the subscriber making the call and that it is using its associated telephone number. The next-highest level of attestation—called "partial" or "B-level"—asserts that the authenticating provider can confirm the identity of the subscriber but not the telephone number. The lowest level of attestation—called "gateway" or "C-level"—asserts only that the provider is the point of entry to the IP network for a call that originated elsewhere and has no relationship to the call initiator. *See id.*

[16] *Id.* at 1863, para. 8.

[17] *See First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6.

[18] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7.

[19] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 9.

[20] *Id.* at 3246, paras. 9-10.

[21] *Id.* at 3246, para. 10. The role of Governance Authority is currently held by the Secure Telephone Identity Governance Authority. Secure Telephone Identity Governance Authority, *STI Governance Authority*, https://sti-ga.atis.org (last visited Dec. 12, 2022).

[22] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 10. The role of Policy Administrator is currently held by iconectiv. *See* iconectiv, *Industry Players*, https://authenticate.iconectiv.com/industry-players (last visited Dec. 12, 2022).

[23] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 10. At the time of this Report, the Policy Administrator, has approved 9 certification authorities. *See* iconectiv, *Approved Certification Authorities*, https://authenticate.iconectiv.com/approved-certification-authorities (last visited Dec. 12, 2022).

authenticating providers themselves, which select an approved Certification Authority from which to request a certificate.[24] Under the current Governance Authority rules, a provider must meet certain requirements to receive a certificate.[25]

B. Use of STIR/SHAKEN to Authenticate Caller ID Information and Certifications

Most voice service providers are required to implement STIR/SHAKEN technology for SIP calls[26] and, with limited exceptions, all will be required to do so by June 30, 2023.[27] Under the Commission's rules, that means that voice service providers must: (1) authenticate and verify caller ID for all SIP calls that exclusively transit their own networks; (2) authenticate caller ID information for all SIP calls that they originate and will transmit to another voice service provider or an intermediate provider and, to the extent technically feasible,[28] transmit such calls with authenticated caller ID information to the next provider in the call path; and (3) verify caller ID information for all SIP calls they receive from another provider and will terminate that include authenticated caller ID information.[29]

---

[24] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864-65, para. 11.

[25] In order to receive a digital certificate, a provider must obtain a token issued by the Policy Administrator. *See* STI-Governance Authority (GA), Policy Decision Binder, Policy Decision 001: SPC Token Access Policy Version 1.2, at 5 (May 18, 2021) (*SPC Token Access Policy*), https://sti-ga.atis.org/wp-content/uploads/sites/14/2022/07/220728-STIGA-Board-Policy-Decision-Binder-v4-0-Final.pdf; *Call Authentication Trust Anchor, Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions*, WC Docket Nos. 17-97 and 21-291, Third Report and Order, 36 FCC Rcd 12878, 12879-81, paras. 4-6 (2021). The Governance Authority's current SPC token access policy requires providers to: (1) have a current form 499A on file with the Commission, (2) have been assigned an Operating Company Number (OCN) or a Resp Org ID, and (3) have certified with the Commission that they have implemented STIR/SHAKEN or comply with the Robocall Mitigation Program requirements and are listed in the FCC Robocall Mitigation Database or is a non-service provider Resp Org that has direct access to numbering resources. *SPC Token Access Policy* at 5. The SPC token is a prerequisite for providers to apply to an approved Certification Authority to obtain the digital certificate needed to sign calls in the STIR/SHAKEN framework. STI-Governance Authority (GA), Policy Decision Binder, Policy Decision 002: Certificate Policy Version 1.3, at 12 (Aug. 17, 2021).

[26] *See* 47 CFR §§ 64.6301(a), 64.6304(a)-(d). For purposes of complying with the requirement to authenticate calls, it is sufficient for a provider to adhere to the three ATIS standards that are the foundation of STIR/SHAKEN. Specifically, ATIS-1000074, ATIS-1000080, and ATIS-1000084—and all documents referenced therein. *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258, para. 36; *Gateway Provider Order and Further Notice* at 23-24, paras. 53-54.

[27] After June 30, 2023, all voice service providers with control over the network infrastructure necessary to implement STIR/SHAKEN will be required to do so unless they are one of the limited number of providers unable to obtain an SPC token. *See Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, DA 22-1342, at 1 (WCB Dec. 16, 2022) (*Second Reevaluation of STIR/SHAKEN Extensions Public Notice*). Providers that lack control over the facilities necessary to implement STIR/SHAKEN do not have an implementation obligation. *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40. Further, pursuant to section 4(b)(5)(B) of the TRACED Act, voice service providers have an ongoing extension for the parts their networks that rely on technology that cannot initiate, maintain, and terminate SIP calls. *See* TRACED Act § 4(b)(5)(B); *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1892-96, paras. 66-70; 47 CFR § 64.6304(d).

[28] In adopting this requirement, the Commission noted that, "the transmission of STIR/SHAKEN authentication information over a non-IP interconnection point" was not technically feasible at that time. *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3258, n.135.

[29] 47 CFR § 64.6301(a). Gateway providers will have substantially similar obligations after their June 30, 2023 deadline to implement and begin using STIR/SHAKEN. *See id.* § 64.6302(c) (requiring gateway provides to "authenticate caller identification for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that gateway provider is subject to an applicable extension in § 64.6304").

Intermediate providers are required to pass any authenticated caller ID information they receive with a SIP call to the next intermediate provider or voice service provider unaltered, subject to limited exceptions.[30]

Voice service providers are required to certify the status of their implementation and use of the STIR/SHAKEN framework.[31] These certifications are submitted to the Commission through the Robocall Mitigation Database, a public portal accessible via the Commission's website.[32] Among other data points, certifications must indicate whether the voice service provider has fully, partially, or not implemented STIR/SHAKEN in its network for the calls they originate.[33] With limited exceptions for public safety, intermediate providers and voice service providers are prohibited from accepting calls from domestic voice service providers that have not filed the required certifications in the Robocall Mitigation Database or have been delisted pursuant to an enforcement action by the Commission.[34] Stated differently, if a voice service provider does not implement and use the STIR/SHAKEN framework to authenticate caller ID information on its IP network as required by the Commission's rules (absent an applicable extension) and does not manifest its compliance with those rules through accurate certifications in the Robocall Mitigation Database, the Commission may remove that provider from the Robocall Mitigation Database, thereby prohibiting downstream providers from doing business with that provider.[35] The Commission has done so when necessary.[36]

C. Triennial Review Notice

When Congress mandated that the Commission require voice service providers to implement STIR/SHAKEN in the TRACED Act, it also directed the Commission to "assess the efficacy of the technologies used for [the] call authentication frameworks" no later than three years after the December

[30] *Id.* § 64.6302(a). Intermediate providers must also use STIR/SHAKEN to authenticate any unauthenticated calls that they receive and will be exchanged with another provider as a SIP call or both (1) cooperatively participate with the industry traceback consortium and (2) respond fully and in a timely manner to all traceback request is receives from the Commission, law enforcement, and the industry traceback consortium. *Id.* § 64.6302(b). The *Gateway Provider Order and Further Notice* proposed eliminating this choice by requiring intermediate providers to authenticate all calls they receive and that will be exchanged with another provider as a SIP call. *See Gateway Provider Order and Further Notice* at 63-68, paras. 160-73.

[31] *See* 47 CFR § 64.6305(c)(1) (requiring certification of implementation status).

[32] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902, para 83.

[33] 47 CFR § 64.6305(c)(1). Voice service providers that have not certified that they completely implemented STIR/SHAKEN must submit a robocall mitigation plan. *Id.* Gateway providers must submit a robocall mitigation plan regardless of their STIR/SHAKEN implementation status by January 11, 2023. *See Wireline Competition Bureau Announces Deadlines for Gateway Provider Robocall Mitigation Requirements and Additional Compliance Dates and Filing Instructions*, WC Docket No. 17-97, Public Notice, DA 22-1303, at 2 (WCB Dec. 12, 2022) (*Gateway Provider Public Notice*). 47 CFR § 64.6305(d)(2)(ii)-(iii). The Commission recently proposed requiring all providers, including intermediate providers, to submit a robocall mitigation plan regardless of their STIR/SHAKEN implementation status. *See Gateway Provider Order and Further Notice* at 75, para. 195. Voice service providers are required to update any information in their certifications within 10 business days of any changes to information previously submitted. 47 CFR § 64.6305(c)(5). Gateway providers are subject to the same obligation. *Id.* § 64.6305(d)(5); *see also Gateway Provider Public Notice* at 4.

[34] 47 CFR § 64.6305(e).

[35] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1903, para. 83 (authorizing removal of voice service providers from the Robocall Mitigation Database under certain circumstances); *Gateway Provider Order and Further Notice* at 18. para. 40 (authorizing removal of gateway providers under the same circumstances).

[36] *See Global UC Inc.*, Removal Order, DA 22-1219, at 3-4, paras. 6-8 (EB Nov. 22, 2022) (removing Global UC Inc. from the Robocall Mitigation Database for filing a deficient certification).

30, 2019 enactment date of the Act.[37] The Commission was also directed to "revise or replace the call authentication frameworks" if the Commission determines it is in the public interest to do so based on this assessment[38] and to submit a report to Congress "on the findings of the assessment . . . and on any actions to revise or replace the call authentication frameworks."[39]

On August 5, 2022, the Bureau issued a Public Notice seeking comment to inform this first triennial assessment of the efficacy of the STIR/SHAKEN caller ID authentication framework, as directed by the TRACED Act.[40] In the *Notice*, we proposed to assess STIR/SHAKEN based on how well it effectuates the authentication of caller ID information.[41] The *Notice* next sought comment on the efficacy of STIR/SHAKEN under this standard and whether the Commission should consider if it would be in the public interest to revise or replace the STIR/SHAKEN framework, or whether doing so would be premature.[42] The Bureau received nine comments and five reply comments in response to the *Notice*.[43]

III. DISCUSSION

STIR/SHAKEN implementation is in its early stages. Voice service providers were just required to implement and begin using STIR/SHAKEN 18 months ago,[44] with the exceptions of non-facilities-based voice service providers, which were not required to implement STIR/SHAKEN until six months ago,[45] and facilities-based small voice service providers, which will not be required to implement STIR/SHAKEN for another six months.[46] Accordingly, the data available to evaluate the efficacy of the STIR/SHAKEN caller ID authentication framework is currently limited, but will increase as voice service providers' experience with the technology and the providers using it expands. The comments filed for this first triennial assessment of the framework indicate, however, that STIR/SHAKEN technology is effective at authenticating caller ID information. No commenter submitted substantive comments suggesting that the technology is itself deficient for that purpose,[47] but some express concern that providers may be applying its technical requirements inconsistently. There is general agreement in the

[37] TRACED Act § 4(b)(4)(A).

[38] *Id.* § 4(b)(4)(B).

[39] *Id.* § 4(b)(4)(C).

[40] *See id.* § 4; *Triennial Review Notice* at 5-6.

[41] *Triennial Review Notice* at 5. The Bureau also sought comment on alternative approaches to our evaluation. *Id.*

[42] *Id.* at 6.

[43] A list of commenters is contained in the Appendix hereto.

[44] 47 CFR § 64.6301; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3252, para. 24.

[45] *See* 47 CFR § 64.6304(a)(1)(i) (providing an extension of the implementation deadline for non-facilities-based small voice service providers until June 30, 2022); *see also Fourth Caller ID Authentication Report and Order* at 12, para. 23. The extension for voice service providers with services scheduled for section 214 discontinuance also lapsed on June 30, 2022. *See* 47 CFR § 64.6304(c).

[46] *See* 47 CFR § 64.6304(a)(1) (providing an extension of the implementation deadline for facilities-based small service providers until June 30, 2023). Providers that cannot obtain an SPC token or operate non-IP networks are not required to implement STIR/SHAKEN until it is feasible to obtain a token or an effective non-IP caller ID authentication framework emerges. *See id.* § 64.6304(b), (d); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, 1882-83, paras. 32, 50.

[47] The only commenter in the record seemingly supporting replacement of STIR/SHAKEN offered only conclusory arguments that STIR/SHAKEN "fails to have met the moment" and should be replaced by "self-sovereign identity" and blockchain technologies. *See* Rafalko Comment. This comment lacked sufficient detail for the Bureau to evaluate, however.

record, however, that when applied as designed, the technology used in the STIR/SHAKEN framework effectively allows providers to identify calls with illegally spoofed caller ID information.

A. Standard Used to Assess the Efficacy of the STIR/SHAKEN Framework

After reviewing the record developed in response to the *Notice*, the Bureau assesses the efficacy of the STIR/SHAKEN framework herein based on the proposed standard of how well it effectuates the authentication of caller ID information. We conclude that evaluating the STIR/SHAKEN framework based on this standard will best assess how well it performs the purpose of the framework that Congress mandated under section 4 of the TRACED Act, i.e., performing caller ID authentication.[48] The majority of commenters support this approach.[49] Indeed, most commenters addressing this issue oppose applying an alternative standard.[50] For instance, in the *Notice*, the Bureau sought comment on whether we should assess the efficacy of STIR/SHAKEN based on its impact on preventing illegally spoofed robocalls, or preventing all illegal robocalls.[51] We agree with the majority of commenters that evaluating the efficacy of STIR/SHAKEN on this basis would fail to account for the fact that, while a critical tool in protecting consumers from illegal spoofing, the STIR/SHAKEN framework is only one facet of the larger campaign by the Commission and industry to combat illegal robocalls.[52]

[48] TRACED Act § 4(b)(4)(A).

[49] NCTA Comments at 2 (stating that "[s]ection 4 of the TRACED Act envisions STIR/SHAKEN as a tool for performing caller ID authentication, and it is therefore appropriate that a report mandated by Section 4 evaluate how well STIR/SHAKEN carries out that function"); Neustar Comments at 2 ("Neustar agrees with the Bureau's proposal to assess the efficacy of STIR/SHAKEN based on how well it effectuates the authentication of caller ID information—its original purpose."); Numeracle Comments at 3; TransNexus Comments at 3; INCOMPAS Reply Comments at 1.

[50] *See* NCTA Comments at 2-3; TransNexus Comments at 3; Neustar Comments at 2; Numeracle Comments at 3. Some commenters agreed with our approach while also suggesting that we supplement our review with additional considerations, such as the effectiveness of STIR/SHAKEN in preventing all illegal robocalls, or the progress of the IP transition. *See* ZipDX Reply Comments at 2; *see also* NCTA Comments at 2-3; VON Comments at 3 (discussing the IP transition). As previously noted, the Bureau did not seek comment on caller ID authentication for non-IP networks for this triennial assessment of technologies used for caller ID authentication because the Commission has not yet mandated that providers implement any particular non-IP caller ID authentication technology. *Triennial Review Notice* at 5, n.35. We note, however, that the Commission has launched an inquiry to examine potential call authentication solutions for non-IP networks, including the nexus between non-IP caller ID authentication and the IP transition generally. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, FCC 22-81, at 17-21, paras. 37-42 (rel. Oct. 28, 2022) (*Non-IP Authentication Notice of Inquiry*).

[51] *Triennial Review Notice* at 5.

[52] *See supra* note 50; Verizon Reply Comments at 1 ("Implementation of the STIR/SHAKEN framework has become a critical cornerstone of the foundational progress that industry, together with the Commission's leadership, has made in the fight against illegal and unwanted robocalls."); Numeracle Comments at 12 ("Numeracle believes that the Commission's leadership and collaboration with service providers to implement STIR/SHAKEN represents a foundational achievement in the effort to combat illegal phone calls."); TransNexus Comments at 3 ("Call authentication is an important and necessary component of measures to prevent illegal robocalls. However, it is not sufficient to prevent illegal robocalls by itself. Call authentication is intended to be used in concert with robocall prevention measures."); CTIA Reply Comments at 5 ("STIR/SHAKEN was never intended to be a 'silver bullet' to solve the illegal robocall problem—STIR/SHAKEN's role is to 'reduce the effectiveness of illegal spoofing . . . and help voice service providers identify calls with illegally spoofed caller ID information before those calls reach their subscribers.") (quoting *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3243, para. 2). *But see* ZipDX, LLC Comments at 2 (arguing that our assessment of the efficacy of the STIR/SHAKEN framework should be based, at least in part, on how effective the framework is at "preventing all illegal robocalls"); VON Comments at 3-4.

B. Assessment of the Efficacy of STIR/SHAKEN Technology

Applying the standard above, the Bureau finds that the technology used in the STIR/SHAKEN framework is effective at authenticating caller ID information. Our conclusion is based on the record developed for this triennial assessment, which strongly supports a finding that the technical standards and practices that comprise the STIR/SHAKEN framework have "proven tremendously successful at authenticating caller ID information for providers that have implemented the technology in their networks."[53] Indeed, Neustar states that, in its experience, in the networks where STIR/SHAKEN has been deployed, it is "establishing the authenticity of the caller number, securely transporting this information through the network, and verifying it at the receiving end of the call . . . signing and validating calls at a nearly 100% rate."[54] USTelecom and Transaction Network Services, Inc. (TNS) also indicate that STIR/SHAKEN's effectiveness in authenticating caller ID information may be responsible for some bad actors feeling the need to shift tactics since it is harder for them to get away with illegal spoofing.[55]

The Bureau's finding is predicated, however, on STIR/SHAKEN technical standards and protocols being executed as required by the three ATIS standards that establish them—ATIS-1000074, ATIS-1000080, and ATIS-1000084—and all documents referenced therein.[56] Those commenters that express concern about the STIR/SHAKEN reaching its full potential as a tool to combat illegal spoofing generally do so on the basis that providers may be applying the standards inconsistently or incorrectly.[57] Incorrect application of the ATIS standards by some providers does not mean that the technology used in the STIR/SHAKEN framework is ineffective when correctly applied, however. Although enforcement matters are beyond the scope of this triennial assessment,[58] we note that the Commission's rules require voice service providers to comply with the ATIS standards as a *minimum* requirement for satisfying their

[53] NCTA Comment at 2; *see also* INCOMPAS Reply Comments at 1-2 (stating that "STIR/SHAKEN, where implemented, is effectuating the authentication of caller ID information as intended"); Numeracle Reply Comments at 3 (stating that "STIR/SHAKEN has represented an important leap forward in establishing a carrier to carrier framework . . . for verification and transmission of critical information over the pathway of a call"); Neustar Comments at 2.

[54] Neustar Comments at 2; *see also* NCTA Comments at 2 ("[STIR/SHAKEN] has proven tremendously successful at authenticating caller ID information for providers that have implemented the technology on their networks.").

[55] USTelecom Comments at 1-2 ("[I]mplementation of the [STIR/SHAKEN] framework may already be responsible for some bad actors shifting to acquire batches of real numbers instead of spoofing."); TNS Comments at 2 ("TNS sees scam robocallers shifting to networks that are the 'weakest link' against robocalling and avoiding those where STIR/SHAKEN has been deployed.").

[56] *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258, para. 36.

[57] TransNexus Comments at 3 (arguing that STIR/SHAKEN's effectiveness is impaired "because, in the U.S. telephone network, STIR/SHAKEN is not being used as intended, per the ATIS standards on STIR/SHAKEN."); Neustar Comments at 5 ("[T]he Commission should encourage all voice service providers to follow the ATIS specifications when determining the proper attestation level to assign a call."); CTIA Reply Comments at 2 (arguing that "to maximize the effectiveness of STIR/SHAKEN, all providers should apply the ATIS standard in a consistent and disciplined manner, as the Commission's rules direct and industry best practices guide"); TNS Comments at 2-3 (urging the Commission take appropriate action to address unsupported attestations); TNS Reply Comments at 4 (arguing that "[o]ver-attestation and other errors in attestation undermine the success of STIR/SHAKEN by devaluing the information that the attestation purports to present); Verizon Reply Comments at 1 (arguing that "the full promise of STIR/SHAKEN technology will not be realized unless the Commission ensures that call attestations are meaningful and accurate"); USTelecom Comments at 2.

[58] Congress directed the Commission to submit a report on "the efficacy of the technologies used for [the] call authentication framework" and "any actions to revise or replace the call authentication frameworks." TRACED Act § 4(b)(4)(A), (C). As such, our review is squarely focused on the efficacy of STIR/SHAKEN technology as a tool for the authentication of caller ID information. *See Triennial Review Notice* at 5-6.

caller ID authentication obligations.[59] Accordingly, specific instances of providers undermining the efficacy of the STIR/SHAKEN caller ID authentication framework by, for instance, failing to sign calls according to the ATIS standards[60] could result in an investigation for noncompliance with the Commission's rules.

The Commission has observed that "STIR/SHAKEN has beneficial network effects,"[61] and that increasing its use will "help voice service providers identify calls with illegally spoofed caller ID information before those calls reach their subscribers."[62] For this reason, the Commission has worked to expand the scope of providers subject to STIR/SHAKEN implementation requirements[63] and the Bureau has declined to extend implementation extensions previously granted by the Commission due to undue hardship.[64] Indeed, earlier this month, the Bureau declined to extend the implementation extension for facilities-based small voice service providers beyond June 30, 2023,[65] finding that doing so would promote the Commission's goal of achieving ubiquitous STIR/SHAKEN implementation without placing additional burdens on providers.[66] Some commenters contend that a full assessment of STIR/SHAKEN's efficacy will be difficult to perform until further progress is made toward full STIR/SHAKEN implementation,[67] and most urge the Commission to continue its efforts to achieve that goal.[68] Numeracle

[59] *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258-59, para. 36. Gateway providers will have the same obligation. *Gateway Provider Order and Further Notice* at 23-24, para. 53.

[60] Neustar Comments at 4 ("Neustar has observed that A-level attestations are sometimes given to calls from numbers that do not merit that assignment. In the most egregious cases, originating providers are using A-level attestations for clearly spoofed calls . . . . This inconsistent application of the attestation framework impedes STIR/SHAKEN's ability to stop illegal robocalls."); TNS Comments at 2 ("TNS is concerned about instances where unsupportable attestation levels are introduced into the network, particularly where an "A" level attestation has been provided for calls that appear not to warrant such attestation level."); Verizon Reply Comments at 1-3; USTelecom Comments at 2.

[61] *Gateway Provider Order and Further Notice* at 27, para. 58.

[62] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1861, para. 3.

[63] *See Gateway Provider Order and Further Notice* at 22-29, paras. 51-60 (imposing gateway provider authentication obligation). The Commission has also sought comment on narrowing or eliminating an exception to the obligation of intermediate providers to use STIR/SHAKEN to authenticate any unauthenticated SIP calls that they receive. *Id.* at 63-68, paras. 160-173.

[64] *Wireline Competition Bureau Reevaluates STIR/SHAKEN Extensions Pursuant to Section 4(b)(5) of the TRACED Act*, WC Docket No. 17-97, Public Notice, DA 21-1593, at 2 (WCB Dec. 16, 2021) (declining to extend the small voice service provider STIR/SHAKEN implementation extension); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Order, DA-22-741, at 1, paras. 1-2 (WCB July 11, 2022) (denying requests for waivers from the Commission's requirement that non-facilities-based small voice service providers fully implement STIR/SHAKEN in the IP portions of their voice networks by June 30, 2022).

[65] *Second Reevaluation of STIR/SHAKEN Extensions Public Notice* at 4-5.

[66] *Id*.

[67] *See* Numeracle Comments at 3 (agreeing that "it is difficult to measure results when the adoption of STIR/SHAKEN is incomplete"); INCOMPAS Comments at 2-3.

[68] *Id.*; Neustar Comments at 3 ("STIR/SHAKEN's value and effectiveness increase as the industry approaches universal adoption, which should remain the Commission's ultimate goal."); NCTA Comments at 1 ("STIR/SHAKEN has proven very effective for those providers that have implemented the framework, and it will become more effective as it is implemented by more carriers."). In particular, some commenters urge the Commission to address the fact that STIR/SHAKEN does not work on networks or portions of networks that lack the technology to initiate, maintain, and terminate SIP calls (i.e., non-IP networks). *See* NCTA Comments at 1-3; VON Comments at 2-3; TransNexus Comments at 6-7; INCOMPAS Reply at 3. As noted above, the Commission has launched an inquiry into this issue. *See Non-IP Authentication Notice of Inquiry*.

and Verizon argue that the efficacy of STIR/SHAKEN would also increase if the Commission required providers to pair their implementation of the framework with other tools.[69] Notably, however, no commenter submitted substantive arguments suggesting that the Commission replace the STIR/SHAKEN framework with different technology.[70] The record indicates that providers have embraced STIR/SHAKEN as the industry standard for authenticating caller ID information.[71]

C. Conclusion

The technology used in the framework is effective at authenticating caller ID information and identifying illegally spoofed calls, and we anticipate its effectiveness will increase as STIR/SHAKEN implementation becomes more widespread.[72] The framework has significant support among stakeholders, including voice service providers that have invested substantial resources into STIR/SHAKEN implementation over the course of the past three years,[73] and are continuing to do so as additional implementation deadlines approach. For this reason, we conclude that it would be premature to consider revising or replacing the STIR/SHAKEN framework at this time.[74]

- FCC -

[69] *See* Numeracle Comments at 4-5; Verizon Reply Comments at 3 (arguing that the Commission should adopt rules encouraging providers to implement know-your-caller and customer due diligence programs). We note that the Commission has adopted "know-your-upstream provider" requirements for gateway providers, and sought comment on requiring all domestic providers to describe their "know-your-upstream provider" processes in submissions to the Robocall Mitigation Database. *See Gateway Provider Order and Further Notice* at 41, 78, paras. 96, 203.

[70] *See supra* note 47.

[71] Neustar Comments at 2; CTIA Reply Comments at 3; INCOMPAS Reply Comments at 3; Numeracle Comments at 3; Verizon Reply Comments at 1.

[72] *See* TNS Comments at 1-2 ("[T]he true potential of STIR/SHAKEN is only realized when all or virtually all voice service providers utilize the call authentication framework.").

[73] *See* Neustar Comments at 1.

[74] *See* INCOMPAS Reply Comments at 3.

Appendix

Entities That Filed Comments in Response to the *Triennial Review Notice**

Commenter	Date Filed	Short Cite
NCTA—The Internet & Television Association	10/3/22	NCTA Comments
Neustar, Inc.	10/3/22	Neustar Comments
Noah Rafalko	9/19/22	Rafalko Comments
Numeracle	10/3/22	Numeracle Comments
Transaction Network Services, Inc.	10/3/22	TNS Comments
TransNexus	10/3/22	TransNexus Comments
USTelecom—The Broadband Association	10/3/22	USTelecom Comments
The Voice on the Net Coalition	10/3/22	VON Comments
WetWork, LLC	10/2/22	WetWork Comments
CTIA—The Wireless Association	10/21/22	CTIA Reply Comments
INCOMPAS	10/21/22	INCOMPAS Reply Comments
Transaction Network Services, Inc.	10/21/22	TNS Reply Comments
Verizon	10/21/22	Verizon Reply Comments
ZipDX LLC	10/22/22	ZipDx Reply Comments

* All comments are publicly available in WC Docket 17-97.