Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

NOTICE OF INQUIRY

Comment Date: August 14, 2017
Reply Comment Date: September 13, 2017

Adopted: July 13, 2017 **Released: July 14, 2017**

By the Commission: Chairman Pai and Commissioners Clyburn and O'Rielly issuing separate statements.

I. INTRODUCTION

1. Year after year, Caller ID spoofing and the robocalling it enables generate the largest number of consumer complaints to this Commission and to the Federal Trade Commission.[1] U.S. consumers receive an estimated 2.4 billion robocalls per month in 2016.[2] With this Notice of Inquiry (NOI), we take another step towards the goals of better protecting American consumers from unwanted and oftentimes fraudulent robocalls. Specifically, we explore how we can further secure our telephone networks against these activities by facilitating use of methods to authenticate telephone calls and thus deter illegal robocallers. Authenticating calls aims to make it possible for subscribers and carriers to know that callers are who they say they are, reducing the risk of fraud and ensuring that callers can be held accountable for their calls.

2. Many stakeholders, including members of the Internet Engineering Task Force (IETF), Alliance for Telecommunications Industry Solutions (ATIS), SIP Forum, and other public and private organizations, have worked to develop the protocols and the multi-phase framework outlined below, which is designed to validate calls and mitigate spoofing and fraudulent robocalling. In this NOI, we seek comment on implementing authentication standards for telephone calls; in particular, we seek comment on the ATIS/SIP Forum proposals thus far. We also seek comment on our governance role and other public policy considerations of the proposals.

II. BACKGROUND

3. In a recent Notice of Proposed Rulemaking (NPRM) and NOI, we acknowledged the risks illegal robocalls pose to consumers.[3] In the NPRM, we reiterated that the large volume of illegal robocalls continues despite industry efforts and the protections provided by the 1991 Telephone

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 2306, 2331-34 (statements of Chairman Pai and Commissioner Clyburn) (rel. Mar. 23, 2017) (*2017 Call Blocking NPRM and NOI*).

[2] *See* YouMail Robocall Index, https://robocallindex.com/2016/june (last visited July 11, 2017); *see also 2017 Call Blocking NPRM and NOI*, 32 FCC Rcd 2306, 2331-34 (statements of Chairman Pai and Commissioner Clyburn).

[3] *2017 Call Blocking NPRM and NOI*, 32 FCC Rcd at 2306, para. 1.

Consumer Protection and Truth in Caller ID Act (TCPA).[4] Also, as we continued to explore a range of possible solutions, we proposed to implement one solution to the illegal robocall issue that could have an immediate positive impact: call blocking initiated by voice service providers in certain situations.[5] Although such call blocking is one tool for combatting illegal robocalls, a complementary and parallel task is to positively identify the bad actors making these calls.[6] Malicious actors hide their true originating phone numbers, putting investigators, enforcers, and—most of all—consumers at a disadvantage.[7]

4. While there are a number of legitimate uses for spoofing caller ID numbers,[8] by simply impersonating a different number, spoofing also can help fraudulent robocallers to evade call blocking or filtering tools that identify unwanted calls based on the calling party number—either that of a trusted party or using a random, possibly temporary, identity.[9] These robocallers use cheap and accessible technologies to spoof their caller identity and scam victims with threats (such as false threats of legal action from the Internal Revenue Service), offers of loans, or purported awards of free travel.[10] Moreover, these calls can harm more than their recipients: innocent subscribers whose numbers have been impersonated may find their numbers reported as the source of robocalls, resulting in their calls being blocked.[11]

5. To address unwanted and illegal robocalls, ATIS and the SIP Forum have been working to develop standards to verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network using the Session Initiation Protocol (SIP) for several years.[12] The ATIS and SIP Forum work consists of a three-phase approach to solving the issue of caller identification, using a digital certificate scheme to "verify and authenticate caller identification for calls carried over an Internet Protocol (IP) network."[13] Phase 1 consists of development of the SHAKEN[14] framework,[15] based on the protocols developed by the IETF's STIR[16] working group (the STIR framework), and describes the operations necessary for making an authenticated telephone call using the SHAKEN framework. Phase 2

[4] 47 U.S.C. § 227.

[5] *Id.* at 3, paras. 6, 5, paras. 10-11.

[6] *See* Robocall Strike Force, Robocall Strike Force Report at 1, 3 (2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf (2016 Strike Force Report).

[7] *See Modernizing the Telephone Consumer Protection Act: Hearing Before the Subcomm. on Comm'cns & Tech. of the H. Comm. on Energy & Commerce*, 114th Cong. 2 (2016) (statement of Richard Shockey, Shockey Consulting, LLC), https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act (Shockey 2016 Testimony).

[8] For example, outbound calls from within a large enterprise, such as a bank contacting its customers, could spoof the number of the bank's published and publicized main telephone number, so that customers can more readily recognize it.

[9] Shockey 2016 Testimony at 2.

[10] 2016 Strike Force Report at 1.

[11] Shockey 2016 Testimony at 2.

[12] 2016 Strike Force Report at 3.

[13] *Id*. at 4.

[14] SHAKEN: Signature-based Handling of Asserted information using toKENs.

[15] *See* Joint ATIS/SIP Forum Standard – Signature-Based Handling of Asserted Information Using toKENs (Phase 1 SHAKEN Report), https://www.sipforum.org/download/sip-forum-twg-10-signature-based-handling-of-asserted-information-using-tokens-shaken-pdf/?wpdmdl=2813.

[16] STIR: Secure Telephone Identity Revisited. *See generally*, *Secure Telephone Identity Revisited (stir)*, IETF, https://datatracker.ietf.org/wg/stir/about/ (last visited June 21, 2017) (describing IETF STIR standards and efforts).

consists of the "Governance Model and Certificate Management for the Trust Anchor," describing the way in which entities will be granted the trust necessary to vouch for call authenticity, and the organizational structures needed to manage this process.[17] Phase 3 consists of the "Call Validation Display Framework" that will recommend how to display SHAKEN/STIR information to consumers.[18] Phase 3 is still being developed by ATIS and the SIP Forum and is not a part of this NOI.

A. Authenticating Calls with SHAKEN/STIR – Phase 1

6. STIR is the IETF[19] working group that "defines a [digital] signature to verify the calling number, and specifies how it will be transported in SIP."[20] STIR's framework includes a certificate model[21] to create credentials based on an X.509 credential system.[22] These credentials are used by authentication services to vouch for the authenticity of SIP calls.[23] On January 5, 2017, ATIS and the SIP Forum adopted SHAKEN, the framework by which telephone service providers implement the protocols produced by STIR.[24] When referring to features present both in SHAKEN and in the STIR framework or model, we will refer to the "SHAKEN/STIR" framework or model.

---

[17] *See* Joint ATIS/SIP Forum Standard – Signature-Based Handling of Asserted Information Using toKENs: Governance Model and Certificate Management (Phase 2 SHAKEN: Governance Model Report) (available at https://access.atis.org/apps/group_public/download.php/35256/ATIS-1000080.pdfhttps://access.atis.org/apps/group_public/document.php?document_id=34724&wg_abbrev=ipnni); *see also* Letter from Thomas Goode, General Counsel, ATIS, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, Attach. at 3-12 (filed June 30, 2017). A "trust anchor" is a system that is assumed to be trusted, and can therefore vouch for the authenticity of other claims, or vouch for the ability of other systems to vouch for other claims in turn. *See*, *e.g.*, IBM Knowledge Center, *Trust anchor*, https://www.ibm.com/support/knowledgecenter/en/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/cwbs_trustancv6.html (last visited June 21, 2017).

[18] Richard Shockey, *SHAKEN and STIRed: Thoughts on the Current State of Anti Spoofing/Caller Validation/Robocall Mitigation/Call Validation Display, An Update for the N. Am. Num. Council* at 11 (Mar. 2017), http://www.nanc-chair.org/docs/mtg_docs/Mar17_NANC_Robocall_Spoofing_Update.pdf (Shockey 2017 NANC Report).

[19] "The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet." *Mission Statement*, IETF, https://www.ietf.org/about/mission.html (last visited Apr. 13, 2017).

[20] Eric Burger, Julia Kieserman, Georgetown University Security & Software Eng'g Research Ctr., *Next Generation Caller Identification*, at 1 (2016), https://s2erc.georgetown.edu/sites/s2erc/files/files/upload/stir_status_and_analysis.pdf.

[21] *See generally*, Internet Eng'g Task Force, *Secure Telephone Identity Credentials: Certificates* (2017), https://tools.ietf.org/html/draft-ietf-stir-certificates-13 (IETF STIR Certificates, Version 13).

[22] *See generally*, Internet Eng'g Task Force, *Request for Comments 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (2008), https://tools.ietf.org/html/rfc5280. X.509 is a specific standard for a type of public key infrastructure system that uses certificates to facilitate secure internet communications.

[23] *See generally*, Internet Eng'g Task Force, *OSCP Usage for Secure Telephone Identity Certificates* (2017), https://tools.ietf.org/html/draft-ietf-stir-certificates-ocsp-00. For a description of SIP and the architecture of a SIP request, *see* Internet Eng'g Task Force, Request for Comments 3261: SIP: Session Initiation Protocol (2002), https://tools.ietf.org/html/rfc3261.

[24] *See* Phase 1 SHAKEN Report. ATIS defines SHAKEN as "a framework that utilizes protocols defined in the IETF [STIR] Working Group that work together in an end-to-end architecture for the authentication and assertion of a telephone identity by an originating service provider and the verification of the telephone identity by a terminating service provider." *Id.* at 3.

7. In the SHAKEN/STIR model, a call is authenticated when it is signed with a digital signature by an authentication service, operating on behalf of the party originating the call.[25] An authentication service can be provided by a carrier, a third party service, or even by a device or piece of software controlled by an individual consumer.[26] Regardless of the type of entity operating as an authentication service, the STIR framework requires that the service first receives a certificate from a trusted certification authority.[27] This certificate states, in essence, that the authentication service is who it claims to be, that it is authorized to sign for the number originating the call, and that its claims about the call it is authenticating can thus be trusted.

8. When a subscriber places a call through a service provider under the SHAKEN/STIR model, the originating service provider contacts an authentication service[28] to obtain a private key with which it can sign the call. The originating service provider then uses the key to sign the call with the subscriber's information and the authentication service's certificate. When the terminating service provider receives the call, it sends the identifying information and the certificate to a verification service.[29] The verification service checks with a certificate repository to ensure that the authentication service is authorized and that its certificate is valid. It then uses the public key that corresponds uniquely to the sending authentication service's private key to verify the signed call. Information about whether the call has been verified[30] or if some problem has occurred (e.g., call did not match asserted caller's identity, certificates have expired, information was in an improper format) is then sent to the terminating service provider.

B. Certificate Management and Governance– Phase 2

9. ATIS's SHAKEN/STIR Phase 2 covers the protocol's certificate management and governance model.[31] While Phase 1 discussed how authentication services bearing certificates from a certification authority would sign and authenticate SIP calls, Phase 2 discusses how the authentication services (which are provided by or directed by a service provider) are to receive those certificates in the first place. The *certificate management model* describes the life cycle of those certificates: how they are issued by a certifying authority to authentication services; how the certificates are added to a public repository; and how they may be renewed, updated, or revoked.[32] The *governance model* defines the

[25] Phase 1 SHAKEN Report at 4-6.

[26] Internet Eng'g Task Force, *Authenticated Identity Management in the Session Initiation Protocol (SIP)* 13, 21 (2017), https://tools.ietf.org/html/draft-ietf-stir-rfc4474bis-16 (IETF SIP Authenticated Identity Management, Version 16).

[27] *Id.* at 13-14; Phase 1 SHAKEN Report at 4-5.

[28] The authentication service can be provided by the service provider itself, or by a third party acting under the service provider's direction. The model assumes that the authentication service can vouch for the subscriber's identity, either through a direct relationship with the subscriber (which would be true in the case of an authentication service within or in communication with the calling service provider), or through some other means. Phase 1 SHAKEN Report at 5-6; IETF SIP Authenticated Identity Management, Version 16, at 21.

[29] Like the corresponding authentication service on the originating service provider's end, the terminating provider's verification service can be performed internally, or by a trusted third-party service.

[30] SHAKEN also anticipates that authentication and verification can show different levels of attestation, such as whether the provider can indicate that it knows both the subscriber and the telephone number used for the call; only the subscriber and not the telephone number; or only that it is the point of entry to the network for a call that originates elsewhere (as with an internationally-originated call). *See* Phase 1 SHAKEN Report at 8-9.

[31] *See generally* Phase 2 SHAKEN: Governance Model Report.

[32] *Id.* at 10-25.

roles and relationships of the parties involved in administering SHAKEN/STIR, such as who administers and who uses the digital certificates in VoIP networks.[33]

1. Certificate Management

10. The ATIS SHAKEN proposal suggests seven requirements of an automated certificate management system:

1. A mechanism to determine the certification authority to be used when requesting certificates;
2. A procedure for registering with the certification authority;
3. A process to request issuance of certificates;
4. A mechanism to validate the requesting service provider;
5. A process for adding public key certificates to a certificate repository;
6. A mechanism to renew or update certificates; and
7. A mechanism to revoke certificates.[34]

In summary, the system proposed by SHAKEN operates as follows. The process begins when the service provider, before requesting a certificate, selects a certification authority and registers with it, connecting via a secure, automated protocol.[35] To indicate that it is an authorized service provider[36] qualified to receive a certificate, the service provider presents to the certification authority a token[37] it has been issued by the policy administrator, whose function is described in Part II.B.2 below. Once its authorization is proven to the certification authority, the service provider applies for the certificate by creating a certificate request and applying for the certificate via the secure, automated protocol. When the request is sent by the service provider and accepted as valid by the certification authority, the service provider automatically retrieves the certificate from the certification authority's server.[38] This process should take place before the service provider begins initiating authenticated calls, after which the authenticated calls can be made as described in the Phase 1 SHAKEN Report summarized in Part II.A of this item.

2. Governance

11. According to ATIS, the STIR and SHAKEN models require several roles to be filled in order to operate.[39] These roles are:

1. A *governance authority*, which defines the policies and procedures for who can issue, and who can acquire, certificates;
2. A *policy administrator*, which applies the rules set by the governance authority and

[33] *Id.* at 7-9.

[34] *Id*. at 10.

[35] The protocol specified in SHAKEN is called Automated Certificate Management Environment (ACME). *See id*. at 12.

[36] This summary of the process assumes that certificates vouch that calls are coming from a given provider. However, authentication processes can also use certificates assigned to vouch that a call is coming from a specific number, or from a specific pool or range of numbers.

[37] This process uses an OAuth-style HTTP interface to provide the token. Phase 2 SHAKEN: Governance Model Report at 12. The SHAKEN governance and certificate management framework details how the policy administrator provides a service provider with its credentials. *Id* at 14-18.

[38] *Id*. at 19-24.

[39] *Id*. at 8-9.

confirms that certification authorities are authorized to issue certificates, and that service providers are authorized to request and receive certificates;

3. A *certification authority* (or several certification authorities), which issues the certificates used to sign and verify telephone calls; and

4. *Service providers*, which, as call initiators, select an approved certification authority from which to request a certificate; and which, as call recipients, check with certification authorities to ensure that the certificates they have received were issued by the approved certification authority.[40]

12. Depending upon how SHAKEN is implemented, an entity such as a telephone service provider, or an authority, might perform one or more roles simultaneously. For instance, many large telephone service providers could have an in-house certification authority; however, smaller providers likely would use the services of an independent third-party certification authority.[41]

III. DISCUSSION

13. To determine how best to implement an authentication process to help eliminate spoofing that leads to unwanted and illegal robocalling, we seek comment on the ATIS/SIP Forum proposals. Specifically, we first seek comment on the governance proposal in Phase 2, since it involves the policy and oversight settings of the proposals, including a potential role for the Commission. We then seek comment on the more technical operation and implementation of the SHAKEN/STIR proposal in Phase 1. Finally, we seek comment on the scope of the proposals as to Signaling System 7 (SS7) and international calling as well as other public policy considerations.

A. Governance of the SHAKEN/STIR Frameworks (Phase 2)

1. The Commission's Role in Advancing Call Authentication

14. We seek comment on what the Commission should do, if anything, to promote the adoption and implementation of authentication frameworks, including the SHAKEN and STIR frameworks. Are existing market incentives sufficient for the industry to adopt the authentication mechanisms specified by the STIR working group in a timely manner, or should the Commission require, facilitate, or otherwise encourage adoption of such mechanisms? What evidence or precedent do commenters have to support their recommendations with respect to the role of the Commission and how to best incentivize adoption of the call authentication procedures?

15. As the Commission considers taking action related to call authentication, what are the relevant time frames or milestones it should consider? What are the likely time frames for adoption and implementation of these frameworks? What milestones and metrics should we use to measure the progress of adoption (e.g., fraction of calls authenticated, fraction of calls that allow tracking)? Aside from originating and terminating parties, are there other entities or stakeholders that could delay or impair the implementation framework? If so, how can these risks be avoided or reduced?

16. Are there existing laws, regulations, market failures, or other factors that prevent or discourage stakeholders from developing, implementing, or deploying authentication frameworks? If so, what steps could the Commission take to remove or mitigate any such barriers?

17. Are SHAKEN and the STIR framework the appropriate frameworks for call authentication on SIP-based networks? Are there other viable alternatives or variants? If so, what are their current levels of development and implementation? How would they compare to the SHAKEN and STIR frameworks in terms of feasibility, effectiveness, timing, cost, and other considerations?

[40] *Id.*

[41] *Id.*

2. Selecting a Governance Authority and a Policy Administrator

18. The SHAKEN and STIR frameworks envision a number of entities performing a number of different roles in the end-to-end call certification/authentication process but do not recommend particular entities to perform those roles. We therefore seek comment on what entity would best serve as the governance authority and what entity would best serve as the policy administrator. We seek comment on the mechanisms by which these two entities might interact. We also seek comment on whether these functions should be merged and operated by a single authority.

19. The Commission itself could serve certain functions of the governance authority, but other parties may be better positioned to handle other aspects of governance and policy administration. We seek comment on what qualifications an entity must have to serve effectively as policy administrator and effectively perform certain governance authority roles, either independently, or at the direction of the Commission. These roles include (1) certifying entities that want to authenticate calls that they originate; (2) deciding what entities are qualified to be certification authorities and setting the requirements for a certification authority to remain in good standing; and (3) helping certification authorities (if certifications are assigned by number or number block) validate that an entity requesting a certificate governing a given number is actually entitled to ask for one. Are there other roles that must be filled, and if so, what qualifications must an entity have to demonstrate its ability to fill them? Would the choices and trade-offs depend on whether certificates are issued for specific telephone numbers (or number blocks), or whether a single certificate is issued for each service provider?

20. *Governance Authority.* What entities are best placed to serve as the governance authority? This role could be fulfilled wholly or partially by the Commission, or by other bodies such as North American Portability Management LLC (NAPM). We seek comment on the advantages and disadvantages of these and other alternatives in terms of authority, transparency, and flexibility.

21. *Policy Administrator: Current Administrators.* Among possible approaches, the Commission could designate an existing numbering administrator as the policy administrator for call authentication. We seek comment on the benefits and drawbacks of doing so. We specifically seek comment on designating either the North American Numbering Plan Administrator (NANPA) or the Pooling Administrator to perform as the policy administrator, or as a certification authority. Because the Pooling Administrator allocates the majority of telephone numbers to service providers,[42] it could be well placed to determine which numbers are controlled by which entities and, therefore, which service providers are responsible for any given telephone number. There is also precedent for including new functions in the Pooling Administrator contract, as evidenced by inclusion of Routing Number Administrator (RNA) functions in that contract in 2011.[43]

22. Both the NANPA and the Pooling Administrator provide services pursuant to separate contracts overseen by the Commission.[44] We note that the North American Numbering Council (NANC),

[42] *See Numbering Resource Optimization*, CC Docket No. 99-200, Report and Order and Further Notice of Proposed Rulemaking, 15 FCC Rcd 7574, 7645, para. 158 (2000) (establishing initial rollout of thousands-block numbering pooling in the 100 largest U.S. MSAs); *see also* Number Pooling Administration 2016 Annual Report at 61, https://www.nationalpooling.com/ (last visited June 21, 2017) (explaining that as of December 31, 2016, 88.2 percent of U.S. rate centers are pooling).

[43] In March 2012, the Pooling Administrator assumed the responsibilities of the permanent p-ANI Administrator, also known as the Routing Number Administrator. *See* Neustar Memo, FCC Approved Neustar's Permanent Routing Number Administrator Change Order Proposal #19 (June 20, 2011), http://www.nationalpooling.com/tools/archives/change-orders/2011/index.htm (Neustar RNA Memo); *see also Numbering Policies for Modern Communications et al*., WC Docket No. 13-97 et al, Notice of Proposed Rulemaking, Order and Notice of Inquiry, 28 FCC Rcd 5842, 5874-75, para. 77 & n.207 (2013).

[44] The NANPA and Pooling Administrator contracts are scheduled to expire on July 8, 2017 and July 14, 2017, respectively.

the Commission's federal advisory committee for numbering matters, has proposed that we consolidate the two contracts.[45] Given the similarities in allocating numbers and issuing certificates, should we consider consolidating these roles into a single contract, entered into with a single entity? We seek comment on the advisability of consolidating these administrative functions (allocating and certifying numbers) in a single contract.

23. We also could designate the Local Number Portability Administrator (LNPA) as the policy administrator, or as a certification authority. The LNPA operates the LNP database, called the Number Portability Administration Center (NPAC), which contains data on the current service providers of all ported and pooled numbers in the United States. Since many subscribers frequently port numbers from one service provider to another, certain implementations of authentication systems would require access to the NPAC. Combining the portability function with the authentication function could also promote efficiencies. In addition, because the NPAC is the repository of service provider information for all ported and pooled numbers, the LNPA could also be well-positioned to determine which service providers are responsible for which telephone numbers. We recognize that the LNPA contract is between the LNPA and the NAPM, and that such an additional designation of duties would require a modification of the existing contract. We seek comment on the desirability of giving the LNPA responsibility for call authentication.

24. *Policy Administrator: New Administrator.* Alternatively, the Commission could initiate a process by which a new entity could become the policy administrator for call authentication. We seek comment on the benefits and burdens of this approach. The Commission could follow any of several models to accomplish this process. For example, using the NANPA and Pooling Administrator as governance models, we could enter into a new contract with a neutral entity that solely entails call authentication that would be funded through NANP.[46] And using the LNPA as another model, the Commission could delegate oversight of the policy administrator to an industry group, as is done with the NAPM, which manages the LNPA contract. That new entity would negotiate and manage a contract with the policy administrator, subject to Commission oversight. We seek comment on the advantages and disadvantages of following any of these models in establishing a call authentication scheme.

25. *Other Alternatives.* While we expect there are benefits in modeling authentication governance on existing arrangements, we seek comment on whether alternative means of call authentication may have benefits as well. For instance, some X.509 systems lack a centralized governance authority or policy administrator designating who may serve as a certification authority, instead allowing end users' systems (such as their browsers) to rely upon the reputation of multiple competing self-certifying certification authorities.[47]

26. We seek comment on all the governance options discussed above. What are the costs and benefits of these various options? What are the effects of each of these options on the efficiency, effectiveness, trustworthiness, and flexibility of a call authentication system? What are the effects of these options on competition and innovation in call authentication? What are the factors to consider in comparing a decentralized governance approach with use of a single authority? How should an

[45] *See Comment Sought on North American Numbering Council Recommendation that FCC Consolidate its North American Numbering Plan Administrator and Pooling Administrator Contracts*, CC Docket Nos. 92-237, 99-200, Public Notice, 28 FCC Rcd 5298 (rel. Apr. 22, 2013); *see also* Charter of the North American Numbering Council, 1, https://www.fcc.gov/about-fcc/advisory-committees/general/north-american-numbering-council (last visited June 21, 2017) (explaining the duties of the NANC, including "developing and recommending technical requirements for the selection of neutral third-party numbering administrators").

[46] 47 U.S.C. §§251(e)(1)-(2).

[47] The HTTPS certificate system is one example of an X.509 system that lacks centralized governance. *See*, *e.g.*, Zakir Durumeric *et al.*, *Analysis of the HTTPS Certificate Ecosystem* (2013) https://experts.umich.edu/en/publications/analysis-of-the-https-certificate-ecosystem.

authentication system ensure a minimum level of due diligence in issuing certificates?

27. We also seek comment on what role, if any, the NANC should perform in deciding call authentication governance. The NANC has historically played a role in number administration matters, making recommendations to the Commission on issues ranging from technical requirements documents to recommendations on the selection of specific administrators.[48] Should the NANC play that role here and be involved in either deciding on the appropriate structure for call authentication or recommending the administrator for that function? Are there other or parallel possibilities, such as establishing a federal partner advisory panel that includes offices with experience in certification authorities?

3. Criteria for Designating Certification Authorities and Validating Service Providers

28. ATIS proposes certain criteria that a governance authority might use in selecting certification authorities and validating service providers. We seek comment on these, as well as recommendations on other criteria that could be useful for a governance authority in making these determinations.

29. *Certification Authority.* ATIS recommends that certification authorities meet two criteria: (1) having sufficient certificate management expertise; and (2) having an in-market presence (i.e. being incorporated in the United States).[49] We seek comment on these criteria, as well as any suggestions for other criteria. Are there existing entities that are likely to be appropriate certification authorities, such as numbering-related entities like the NANPA, Pooling Administrator, or LNPA? We also seek comment on the strengths and weaknesses of using both an online and offline certification authority, as used in other systems such as Domain Name System Security Extensions (DNSSEC).[50]

30. *Service Provider.* ATIS proposes that, to be designated a service provider allowed to sign calling party information, a provider must have an Operating Company Number (OCN).[51] We seek comment on this recommendation. Are OCNs a reliable criterion for assuring that a service provider is eligible to sign calls? Are there originating entities that lack OCNs (such as certain non-facilities-based VoIP providers, providers of call center services, corporations using multiple outbound service providers, or software application or device manufacturers) but would require their calls to be authenticated? Are there restrictions that prevent these entities from receiving an OCN? If the governance authority were to select different criteria, what would they be, and how would they prevent bad actors or careless parties from allowing the certification of inauthentic calls, thus undermining the purpose of the system?

31. *Scope of Certificate Coverage.* SHAKEN assumes that certificates will cover particular service providers. However, certificates can alternatively cover specific telephone numbers or ranges of

---

[48] *See*, *e.g.*, *Implementation of Telcordia Technologies, Inc. Petition to Reform Amendment 57 and to Order a Competitive Bidding Process for Number Portability Administration, et al.*, WC Docket Nos. 07-149, 09-109, CC Docket 95-116, Order, 30 FCC Rcd 3082, 3086-91, paras. 8-13 (2015) (explaining the NANC process in selecting Telcordia as the LNPA); *see also supra* note 42, Neustar RNA Memo at 5-6.

[49] *See* Phase 2 SHAKEN: Governance Model Report, Appx. A.

[50] DNSSEC is a set of standards designed to ensure the authenticity and integrity of Domain Name System (DNS) information. *See*, *e.g.,* Internet Corporation for Assigned Names and Numbers, *DNSSEC—What Is It and Why Is It Important?*, https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en (last visited June 21, 2017); Microsoft TechNet, *Offline Root Certification Authority (CA)*, https://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx (last visited June 21, 2017).

[51] Phase 2 SHAKEN: Governance Model Report, Appx. A. OCNs are assigned by the National Exchange Carrier Association and are used to uniquely identify telecommunications service providers. *See* https://www.neca.org/Code_Administration.aspx (last visited June 21, 2017).

telephone numbers.[52] Each approach has advantages and disadvantages, which may differ. Certifying at the provider level may allow for existing governance structures to be used in implementation, but may prevent certain novel uses of the system; while certifying at the number or range-of-number level may allow some of those innovations and lessen the risk that untrustworthy or careless service providers sign for calls that make unauthorized use of numbers, but introduce technical complications.[53] We seek comment on these issues.

32. *Developing and Amending Criteria*. We also seek comment on how the governance authority and the policy administrator should develop, amend, and implement the criteria for selecting certification authorities, designating service providers, and determining certificate coverage. What stakeholders should be involved in these decisions, and how can stakeholders' interests be represented in their outcomes?

B. Implementation and Operation of the SHAKEN/STIR Frameworks (Phase 1)

33. We also seek comment on the SHAKEN and STIR standards developed by ATIS and IETF, respectively. This includes a number of implementation options left open by the STIR standards. We invite commenters to express their views on any relevant aspect of the standards, as well as any proposed alternatives. We set out the issues on which we specifically seek comment below, although commenters are encouraged to raise other issues as well.

34. *Enrollment of Authorized Numbers or Providers.* IETF's certificates standard notes three potential approaches for enrollment in the certification system.[54] The first approach requires the certification authority to work with a centralized authority, such as the NANPA, to issue credentials to providers in a top-down manner. The SHAKEN framework presumes this sort of structure, with a central governance authority instructing a single policy administrator how to enroll providers in the system. The second approach would work from the bottom up, where a certification authority would require an entity to prove its control over a number by some sort of test, such as sending to the purported telephone number a text message containing a URL that the text recipient can use to confirm that it is the originating telephone number. The third enrollment approach, which can work in concert with either of the above approaches, operates by delegation: the holder of a valid certificate (assigned under one of the first two approaches) can delegate to another party its authority to vouch for a number or set of numbers. For example, a local exchange carrier might delegate to an enterprise subscriber a block of numbers used by that subscriber's PBX. This delegation could operate in multiple levels; the enterprise could then delegate an individual number to a particular employee, for instance.[55] We seek comment on these alternatives and, if several models are likely to emerge, estimates of when this might happen.

35. *Valid Types of Authorization and Verification Service Providers*. The general presumption in SHAKEN and STIR is that large telecommunications service providers and third party proxies serving smaller providers will be the typical entities conducting call authentication and verification. However, IETF notes the potential for other types of entities, such as end-user devices, to provide authentication services, including computers, phones, mobile devices, or gaming devices.[56] While this could allow for more granular user identification, IETF does note the "prohibitive[]" complexity of synchronizing signatures and managing credentials across various devices.[57] We seek comment on the potential costs and benefits of allowing different types of entities and devices to provide

[52] IETF STIR Certificates, Version 13, at 3-4; IETF SIP Authenticated Identity Management, Version 16, at 21-22.

[53] *Id.*

[54] IETF STIR Certificates, Version 13, at 6-7.

[55] *See id*. at 7.

[56] IETF SIP Authenticated Identity Management, Version 16, at 21.

[57] *Id*.

authentication and verification services, and how the criteria for selecting them might relate to the criteria for designating authorized service providers.

36. The SHAKEN model also specifies that service providers will communicate with certification authorities using a specific secure, automated protocol called ACME.[58] As ACME is still being developed, we seek comment on the SHAKEN model's reliance on it. Should we consider other certificate management mechanisms and procedures as replacements or interim solutions while the IETF continues work on the ACME protocol?

C. Scope and Policy Effects of Authentication

37. Having sought comment in particular on how we might encourage a workable governance framework for call authentication, we now seek comment on how the SHAKEN/STIR models fit within the larger policy landscape—both for combatting spoofing and unwanted and illegal robocalls, and for other public interest reasons.

1. Scope of Authentication Efforts in Combatting Spoofing and Robocalls

38. Voice calls can now originate not only from traditional, landline phones, but also from multiple platforms using wireless phones and IP based technologies. Voice communications using these myriad platforms are transported over legacy, circuit switched Time Division Multiplexing (TDM)/SS7 networks, packet switched IP/SIP networks, "or a combination thereof."[59] The existence of multiple call origination platforms, each using a number of technology combinations, creates multiple opportunities for bad actors seeking to mislead victims and law enforcement about their identity in order to make unwanted and illegal robocalls. For example, several recent reports[60] have surfaced identifying critical vulnerabilities in SS7, which, if exploited, "threaten[] the user's privacy and can lead to user location tracking, fraud, denial of service, or even call interception."[61] These concerns will not automatically be abated as the nation's service providers transition from legacy telephone network systems to newer SIP/IP-based telephone networks where underlying physical networks can still be exploited.[62] Without safeguards in the new telephone environment, bad actors can find and exploit flaws to continue to exploit consumers.

---

[58] Phase 2 SHAKEN: Governance Model Report at 12.

[59] Alliance for Telecomm. Indus. Solutions, *Developing Calling Party Spoofing Mitigation Techniques: ATIS' Role* 2 (2016), http://www.atis.org/01_resources/whitepapers/ATIS_Robocalling_Summary.pdf. Signaling System 7 (SS7) has been the global standard signaling protocol for telecommunications traffic for the public switched telephone network, and is used in wireline calls as well as in 2G and 3G cellular networks. *See* Communications Security, Reliability, and Interoperability Council Working Group 10: Legacy Systems Risk Reductions, Final Report 5-6 (2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

[60] *See, e.g.*, Lily Hay Newman, Wired, *Fixing the Cell Network Flaw that Lets Hackers Drain Bank Accounts* (May 9, 2017), https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/; Dan Goodin, Ars Technica, *Thieves drain 2fa-protected bank accounts by abusing ss7 routing protocol* (May 3, 2017), https://arstechnica.com/security/2017/05/thieves-drain-2fa-protected-bank-accounts-by-abusing-ss7-routing-protocol/; Craig Timberg, The Washington Post, *For sale: Systems that can secretly hack where cellphone users go around the globe* (Aug. 24, 2014), https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html; Sharyn Alfonsi, *Hacking Your Phone – CBS News* (Apr. 16, 2016), http://www.cbsnews.com/news/60-minutes-hacking-your-phone/; Hassan Mourad, SANS Institute, *The Fall of SS7 – How Can the Critical Security Controls Help?* (2015), https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225.

[61] Mourad, *supra* note 60, at 1.

[62] *See, e.g.*, Roger Jover, *LTE Security, Protocol Exploits and Location Tracking Experimentation with Low-Cost Software Radio* (July 18, 2014), https://arxiv.org/abs/1607.05171.

39. Since the SHAKEN/STIR proposals apply to SIP-based, but not SS7-based systems, we seek comment on the place of SS7 and other legacy technologies in this and other Commission proceedings. Is it practical for the industry to proceed with frameworks that apply to IP-based voice telephony, but not legacy signaling systems? Are there benefits to creating an integrated authentication framework across both IP and older TDM systems, and is doing so practical? Alternatively, will advancing authentication of IP-based calls significantly alleviate, or set the stage for alleviating, the problems of illegal robocalls regardless of whether TDM authentication solutions exist? What percentage of calls and illegal robocalls currently originate from IP-based versus TDM systems? Can authentication of IP-originated calls benefit providers or customers on terminating TDM and SS7 systems? For example, could a telephone service provider operating a TDM or SS7 network block or filter unauthenticated robocalls?[63] Should we, in this or other proceedings, act to facilitate more robust authentication for TDM and SS7 systems? If so, how?

40. Although we are committed to combatting spoofing and illegal and unwanted robocalls in the United States, they remain a global problem. Many such robocalls target consumers in the United States frequently originate elsewhere; meanwhile, other countries also experience high volumes of robocalls and spoofed calls.[64] We anticipate that adopting authentication frameworks in the United States will naturally have less effect on foreign robocalling and seek comment on this view. We seek comment on what effects an authentication framework might have on spoofing and robocalls originating in other countries, as well as potential unintended effects on other types of international calling. For instance, we seek information on the percentage of illegal robocalls originating from domestic numbers, or from numbers in countries that have similarly prioritized the problem of illegal robocalls. We also seek comment on how authentication mechanisms might interact with any applicable international agreements and obligations, as well as how the Commission and other stakeholders might work with other countries' authorities and stakeholders to coordinate or integrate authentication systems and other efforts against misuse of the telephone network.

2. Other Policy Effects of Authentication Systems

41. While the role that call authentication can play in combatting spoofing and illegal and unwanted robocalls is clear, it is also clear that authentication mechanisms can have a variety of other effects. We seek comment on what other effects might result from the implementation of a SHAKEN/STIR system or another system of call authentication. Are there other likely costs and benefits?

42. *Privacy*. IETF notes that a service provider sharing information to authenticate an originator's identity might include in its sharing information that could identify a person, including a name, workplace, service provider, and possibly other details.[65] However, IETF believes that the privacy risks associated with that information are no different from those inherent to non-authenticated forms of IP-based calling, in that poorly structured or configured systems might divulge personally identifying information in either case.[66] We seek comment on this analysis, as well as other privacy issues, such as the potential for authentication mechanisms to inadvertently disclose or use without authorization

[63] These issues are being considered in more detail in the *2017 Call Blocking NPRM and NOI*.

[64] Spoofing and unwanted and illegal robocalling are also the top complaints to the United Kingdom and Canadian regulators. *See, e.g.*, Shockey 2017 NANC Report at 2; *see also* Huw Saunders, Director Infrastructure, Ofcom, Nuisance calls – addressing consumer harm through technology 2 (Nov. 10, 2016), http://www.niccstandards.org.uk/meetings/forum-2016.cfm; Compliance and Enforcement and Telecom Notice of Consultation, CRTC 2017-4, Canadian Radio-television and Telecommunications Commission (Jan. 9, 2017), http://www.crtc.gc.ca/eng/archive/2017/2017-4.htm.

[65] IETF SIP Authenticated Identity Management, Version 16, at 31.

[66] *Id.*

customer proprietary network information (CPNI), personally identifiable information, or other privacy-affecting information in new ways or to new parties.[67]

43. IETF also notes that an entity acting as an authentication service could also act as a privacy service, by vouching for the authenticity of a call but not passing along any further identifying information. For instance, a service provider could indicate it knew that the call was from one of its valid subscribers, but not the subscriber's telephone number or other information. An authentication service might also, at the originating user's request, simply eliminate any identifying information from the call, although doing so should prevent the authentication service from vouching for the call. We seek comment on the feasibility, availability, and desirability of these practices.

44. *Security*. We seek comment on the effects that an authentication mechanism will have on the security of the network, consumers, and service providers. In this connection, we note that Working Group 10 of the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) recommended approaches to bolster SS7 security. We seek comment on whether and to what extent CSRIC's recommendations could be implemented in support of an authentication mechanism,[68] and whether additional security measures should be considered. Regarding the SHAKEN/STIR framework itself, IETF details the anticipated effects of the STIR protocols on various types of attack. We seek comment on these effects, including the potential effects of removing authentication information (which could result in authenticated calls being rejected as unauthenticated), securing connections to authentication services, and strategies for identifying which entities or numbers have implemented the authorization system as it rolls out.[69] We also seek comment on other effects of an authentication system. For example, could an authentication system provide additional opportunities for attack, such as by denying callers the use of an authentication service, thereby increasing the likelihood of their calls being rejected? Are there other examples of effects we should consider?

45. *Other Effects*. We also seek comment on any other effects that commenters anticipate from the development and adoption of call authentication. Are there additional abuses or misuses of the telephone network that would be prevented or hindered by call authentication? Are there other unintended or unanticipated consequences of such a system?

D. Costs and Benefits of Implementing Call Authentication Systems

46. We seek high-level estimates of the costs of implementing call authentication. Would these largely be one-time costs? Approximately how large would annual on-going costs be? We also seek high-level estimates of the benefits that call authentication would bring, for example, due to reduced consumer annoyance, reduced fraud, and more efficient and effective use of voice calling. Lastly, we seek comment on the extent to which such services would be voluntarily (perhaps self-) supplied, and if such services were offered commercially, the extent to which voluntary end-user fees could be expected cover service costs.

47. *Funding the Costs of Administering and Implementing Call Authentication.* We view costs of implementing and administrating call authentication arrangements as "telecommunications numbering administration arrangements,"[70] and seek comment on mechanisms to recover those costs. We seek comment on how stakeholders might bear the costs of a call authentication system. Are the stakeholders who incur costs to administer and implement call authentication best placed to bear those

[67] *See id*. at 32 (noting that certain implementations of PASSporT can, if configured improperly pass information out of a trusted domain).

[68] *See* Communications Security, Reliability, and Interoperability Council Working Group 10: Legacy Systems Risk Reductions, Final Report 5-6 (2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

[69] *See id*. at 33-39.

[70] 47 U.S.C. § 251(e)(2).

costs? To the extent that costs burdens could be shifted among relevant stakeholders, what mechanisms are available to do so? We also note that sources of funds for these efforts may vary depending upon the structure of the governance and administrative bodies.

E. Legal Authority

48. We anticipate relying on Section 251(e) Communications Act (the Act) for authority to take necessary steps to encourage or develop authentication standards for telephone calls to combat Caller ID spoofing and the robocalling it enables.[71] Section 251(e) provides the Commission plenary numbering authority and exclusive jurisdiction over "those portions of the North American Numbering Plan [NANP] that pertain to the United States."[72] The statute charges the Commission with creating or designating "one or more impartial entities to administer telecommunications numbering and to make such numbers available on an equitable basis."[73] The development of a call authentication standard and establishment of a policy administrator will help ensure entities issuing phone numbers determine whether particular phone numbers have indeed been issued, and to whom, via associations with particular certificates. The actions we begin to consider in this NOI will enhance the efficiency and security of NANP and our Nation's telephone networks.

IV. PROCEDURAL MATTERS

A. Ex Parte Rules

49. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[74] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by Rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

B. Comment Filing Procedures

50. Pursuant to Sections 1.415, 1.419 and 1.430 of the Commission's rules, 47 CFR §§ 1.415, 1.419, 1.430, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

---

[71] *See* 47 USC §§ 251(e), 227.

[72] 47 USC § 251(e)(1).

[73] 47 USC § 251(e)(1).

[74] 47 CFR. §§ 1.1200 *et seq.*

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

  - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

- People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

C. Contact Person

51. For further information about this proceeding, please contact Sherwin Siy, FCC Wireline Competition Bureau, Competition Policy Division, Room 5-C225, 445 12th Street, S.W., Washington, D.C. 20554, (202) 418-2783, Sherwin.Siy@fcc.gov.

V. ORDERING CLAUSES

52. Accordingly, IT IS ORDERED that, pursuant to the authority contained in Sections 1, 4(i), 4(j), 227, 251(e), and 403 of the Communications Act of 1934, as amended, 47 U.S.C §§ 151, 154(i), 154(j), 251(e), and 403, this Notice of Inquiry IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *In the Matter of Call Authentication Trust Anchor, Notice of Inquiry,* WC Docket No. 17-97

This *Notice of Inquiry* targets fraudulent robocallers. These robocallers continue to find ways around consumer call-blocking or filtering tools by using inaccurate caller ID information. For instance, they impersonate phone numbers that use the first six digits of the recipient's phone number to make the calls appear as if they originate from a local source. This practice, known as caller ID spoofing or neighbor spoofing, is similar to a villain in an action movie donning a disguise to trick unsuspecting victims into thinking that the villain is someone he is not. Now, in the movies, the hero generally manages to unmask the villain just in time. But all too often, consumers don't realize that a number has been spoofed until it's too late.

That's why we're exploring call authentication—a process for reliably determining whether the caller is in fact who he purports to be—in order to help eliminate fraudulent spoofing attempts and to further secure our telephone networks. At the heart of this *Notice of Inquiry* is the SHAKEN (or Signature-based Handling of Asserted Information Using toKENs) framework developed by the STIR (or Secure Telephone Identity Revisited) working group and other dedicated industry stakeholders. If things go well, our hope is that, just like in the movies, someday soon consumers won't be as easily fooled by a villain's disguise.

I would like to thank the staff who worked on this item: Alex Espinoza, Heather Hendrickson, Dan Kahn, Kris Monteith, and Ann Stevens from the Wireline Competition Bureau and Ken Carlberg from the Public Safety and Homeland Security Bureau.

STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN

Re: *In the Matter of Call Authentication Trust Anchor, Notice of Inquiry*, WC Docket 17-97*; In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry*, CG Docket No. 17-59

The phone rings, you pick it up, then you notice a distinct pause. You sigh heavily because you know that within seconds, a recording will follow saying something like this: "Congratulations! You have just been chosen to receive an all-expenses paid vacation to Florida."

We each have had our encounters with robocalls, and our feelings about them are rarely warm or fuzzy. Too often they come in at the worst possible times … during an important evening meeting, just when you are having a rare conversation with family members or friends, or right when you are about to take that next to the last bite, into an already lukewarm previously frozen TV dinner.

According to the latest data from the YouMail Robocall Index, 2.5 billion of those robocalls were made just last month in the United States. Equally remarkable is that four telephone numbers are responsible for more than 68 million of these calls. Given the severity and complexity of the unwanted robocall problem, this agency recognizes that it must take a multi-pronged approach, to address this persistent issue.

Through the combined efforts of the Wireline Competition Bureau (WCB) and the Consumer and Governmental Affairs Bureau (CGB), we have before us two Notices of Inquiry. The first seeks comment on how to best authenticate, certify and identify calls, in an effort to eradicate unwanted and illegal ones for good. Proper authentication and identification are necessary first-steps in stopping illegal robocalls dead in their tracks. Through an authentication regime, we can better ensure that no spoofed robocall goes undetected, untargeted, or unblocked.

The second notice, initiates an inquiry on how to deal with reassigned numbers. There is no denying that millions of phone numbers change hands each year. This has led to calls for establishing a reassigned number database, an undertaking that has my support. I appreciate the Chairman's willingness to include suggested questions in the item, including the downsides of a safe harbor for robocallers and how to design a reassigned number database in such a way, to maximize its use and reliability.

As is evidenced by recent actions taken by the FCC, including last month's Notice of Apparent Liability (NAL) against an individual alleged to have spoofed nearly 100 million calls, no one action will rid this nation of illegal robocalls for good. But support for both of these NOIs affirms our commitment and willingness to work together, and find new and innovative ways to make sure this Commission stays one step ahead.

Thanks are due to the staff of WCB and CGB for your continuing efforts to stop unwanted and illegal robocalls.

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

Re: *In the Matter of Call Authentication Trust Anchor, Notice of Inquiry*, WC Docket 17-97*; In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry*, CG Docket No. 17-59

Many thanks to the Chairman for combining the discussion of these two items, addressing similar but distinct aspects of the same topic.

Overall, I appreciate the challenge of trying to corral and decrease illegal robocalls, many of which originate overseas. Do note that I said *illegal* robocalls, as not every robocall is problematic. In fact, many are extremely beneficial to consumers, providing information they want and expect to receive from trusted companies. The Commission's job should be to ensure that it doesn't prevent or squash legitimate robocalls in its ferocious quest to curtail unlawful ones.

I find the second item, regarding reassigned numbers, to be extremely pertinent to the entire discussion. Quite frankly, I think this item shines a bright light on just how misguided and fundamentally broken the Commission's 2015 TCPA Declaratory Ruling really was. At that time, I begged the Chairman, my fellow Commissioners, and the staff to accept reality and address the issue of reassigned telephone numbers in a meaningful way. I was ultimately unsuccessful. Instead, the Commission tried to pretend the problem wasn't valid despite estimates that 100,000 cell phone numbers are reassigned to new users each day and telephone numbers are typically withheld for only 90 days or less before being recycled to new users. This meant the scope of the problem was much larger and thornier than the Commission ever acknowledged, making any type of "prior consent" extremely difficult and essentially worthless in a short amount of time.

Exacerbating the situation, the Commission created a faulty and intellectually dishonest solution of "one free call to a consumer" exemption as a fig-leaf remedy. Recall that the exemption does not require consumers to accurately inform the caller that the number has been reassigned; ignores the worthlessness of uninformative voicemails; and even counts call attempts or informational texts where there was no response at all against the one call policy. Moreover, accidental misdials receive no protection whatsoever. In my limited time, I won't belabor how bankrupt this really is and how it has ensnared legitimate companies in needless, financially-crippling litigation for the simple practice of trying to contact their willing customers. I am hopeful that the D.C. Circuit will overturn this and other portions of our previous declaratory ruling and install an intended recipient or actual knowledge standard as the proper legal test, which is completely consistent with the underlying TCPA. In addition, the Commission should initiate a new proceeding to effectuate this change.

To the extent that the issue is not mooted by court action or our own initiative, the item before us explores the creation of a reassigned number database as one option to deal with the issue. The idea being that companies could cross-check their calling lists against an accurate and consistently updated database of reassigned numbers to significantly limit the number of stray calls. While not a new idea, as many people in the past have proposed differing options, such as using part of the Commission's existing numbering resources, the Second Notice of Inquiry explores many of the relevant issues that would need to be sufficiently answered before creating such a database. Chief among these is language, added at my behest, that examines whether to similarly create a safe harbor for companies that use the database to minimize calls to reassigned numbers. Simply put, there must be some benefit for companies to help establish, pay for and use such a database, and a properly constructed compliance safe harbor must be part of any equation, if this item is to proceed forward.

In the first item pertaining to call authentication, I am less sanguine. While I applaud the Chairman for creative efforts to further curtail illegal robocalls and will vote to approve since it's an NOI, I am not exactly as comfortable with some of the direction or suggestions posed. Certainly, I am not in favor of having the Federal government via the Commission actively involved in these functions – either

as a governance authority or policy administrator – no matter how meritorious it may be for reducing unlawful robocalls. Creating, facilitating, or mandating such a regime, which seems to be very close to establishing a de facto technology mandate, is not the proper role of the Commission. Those functions should be left to the private sector. Moreover, ATIS, the purveyor of the SHAKEN framework, favors a minimalist government role or none at all. That seems to beg the question why we would contemplate anything more. To the extent that the Commission feels it must get involved, and we would need to see some very convincing evidence, holding roundtables with applicable parties or letters seeking information on the potential roadblocks would be the best course of action, if any. Maybe we can use the TAC and CSRIC for that?

Operationally, I am a bit puzzled how this structure would actually work in relation to the authentication that already exists for data packets, which was initiated without FCC or other government involvement. For data packets that contain voice would there be some extra certification and authentication structure separate from that applicable to all other data packets?

In the end, the item raises the most salient issue, stating: "We anticipate that adopting authentication frameworks in the United States will naturally have less effect on foreign robocalling…" In other words, if this item were eventually turned into final Commission rules, its likely to have questionable impact on illegal robocalls initiated overseas. Given that most experts agree that a good portion of robocalls initiate outside the boundaries of our good nation, this would certainly need to be fed into a cost-benefit calculation as to whether FCC intervention is warranted, as opposed to industry-led efforts.

With that, I will vote to approve each of the two items.