Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF WEST TELECOM SERVICES, LLC

Robert W. McCausland
VP, Regulatory and Government Affairs
West Telecom Services, LLC
3200 W. Pleasant Run Road
Suite 300
Lancaster, TX 75146-1086
RWMcCausland@west.com
Phone: 469-727-1640
Fax: 866-432-3936
Cell/Text: 469-644-4954

Helen E. Disenhaus
Carolyn A. Mahoney
Telecommunications Law Professionals PLLC
1025 Connecticut Ave, N.W., Suite 1011
Washington, DC 20036
Phone: 202-789-3123
Fax: 202-789-3112
hdisenhaus@telecomlawpros.com
cmahoney@telecomlawpros.com
Counsel for West Telecom Services, LLC

July 24, 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY

West Telecom Services, LLC ("West") applauds the Commission's commitment to ending the scourge of illicit robocalling that has become a pervasive and incessant threat to American consumers. West supports the Commission's efforts to empower carriers to identify and root out unlawful calls and to stop the fraudsters and bad actors responsible for them. Both the recent Declaratory Ruling permitting analytics-based default call blocking on an opt-out basis, and the anticipated imminent decision declaring it to be illegal to originate overseas calls that spoof U.S. telephone numbers, are important steps in facilitating vigorous efforts by carriers to interdict illegal robocalling.

However, the Commission should ensure that carrier default call blocking does not inadvertently sweep up and prevent delivery of important legal calls and messages that consumers want and need to receive. West therefore proposes that the Commission expeditiously take the following steps, with further review of the need for their modification once SHAKEN/STIR is generally deployed in the U.S. telecommunications system:

1. Now that international spoofing is about to be declared illegal, limit the definition of calls that carriers may block by default, on an opt-out basis, to illegal and unlawful calls only, with any blocking of "unwanted" calls (that is, calls from any caller not on the consumer's individual contact list) left to consumer choice after a fully-informed election among possible blocking options.

2. Clarify that it is Commission policy that carriers take substantial measures to avoid blocking important calls, including but not limited to those from schools, medical providers, and pharmacies, as well as to prevent blocking of calls to and from emergency and similar services whose numbers are included in a Critical Calls list.

3. To that end, require that, to be deemed "reasonable," and therefore eligible for protection from liability for blocking of non-illegal calls, default call blocking program analytics must comprise blocking-antidote "negating" factors (that is, those characteristic primarily of illegal and illicit calls) as well as "neutral" factors also characteristic of legitimate automatically-delivered calls.

4. In recognition that the SHAKEN/STIR framework is not yet widely deployed throughout the industry due to multiple valid factors, delay mandatory implementation of

the SHAKEN/STIR framework until January 1, 2021, and in the interim prohibit call blocking programs from relying on SHAKEN/STIR verification and validation as the basis for transmission of a call or for qualification for a Safe Harbor from liability for "over-blocking" of lawful calls.

5. In the interim, establish a Safe Harbor from liability for inadvertent over-blocking of lawful calls that is based on a provider's compliance with the following requirements:

    a. Using only default blocking programs implemented on a basis that is nondiscriminatory both on its face and in application, that:

        1) Use only analytics that comprise negating as well as neutral factors and that target only illegal or unlawful calls;

        2) Do not permit call blocking merely based on the absence of SHAKEN/STIR verification and validation; and

        3) Do not give preferential blocking protection to calls originating on the networks of the carrier, its affiliates, and/or its partners.

    b. Fully informing consumers of the types of calls that may be blocked by election of default carrier-initiated blocking (on an opt-out basis); by election of customer-specific blocking of all calls originated from numbers not on the customer's individual contact list; and by election of no blocking.

    c. Registration in a Commission-maintained and Commission-overseen database of contact representatives that requires certification of the registrant's commitment to and implementation of the above conditions, as well as to the registrant's proactive participation in a cooperative complaint response process to ensure immediate resolution of complaints of over-blocking and refinement of methodologies to minimize further over-blocking.

Implementation of this approach should encourage carriers to deploy robust default blocking systems that are effective against illicit robocalling but minimize the risk of inadvertent over-blocking and its serious adverse consequences for the public. It should also promote expansion of existing cooperative industry traceback efforts and lead to refinement of blocking algorithms that may in the future be combined with SHAKEN/STIR to, it is hoped, virtually eliminate illegal robocalling.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF WEST TELECOM SERVICES, LLC

West Telecom Services, LLC ("West")[1] submits these comments ("Comments") in response to the *Declaratory Ruling and Third Further Notice of Proposed Rulemaking* ("*Ruling* and *FNPRM*") issued by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding.[2]

I. INTRODUCTION AND SUMMARY

Illicit robocalls originating with scammers and other bad actors have become a pervasive and incessant threat in the everyday lives of American consumers. West appreciates and

[1] West Telecom Services, LLC ("West") is a wholly-owned subsidiary of West Corporation, a leading technology enablement company connecting people and businesses around the world. West Corporation is a global provider of communications and network infrastructure services, offering services including unified communications services, safety services, and interactive services like automated notifications, as well as telecom services. Affiliates of West Corporation complete over 4.2 billion consumer-desired messaging voice calls per year, such as school and healthcare notifications.

[2] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-97 (rel. June 7, 2019) (hereinafter, "*Ruling*" and "*FNPRM*").

supports the Commission's efforts to help carriers achieve the ultimate goal of stopping these illegal scam calls and the fraudsters behind them. However, it is important that, in adopting rules to implement the call blocking policy change announced in the recent *Ruling*, the Commission makes thoughtful and critical clarifications that provide additional protections for legitimate calls and the consumers who expect and need to receive them. In these Comments, West therefore makes several recommendations for Commission action that would promote robust and non-discriminatory call blocking; minimize over-blocking and its adverse consequences for the public; ensure consumers are fully informed of the implications of their blocking choices; and promote cooperative industry efforts to eliminate bad actors and promptly resolve complaints of inadvertent call blocking. West also recommends implementation of an interim Safe Harbor for inadvertent over-blocking pending a necessarily-delayed mandate for implementation of the SHAKEN/STIR[3] framework.

First, the Commission should now permit carrier-initiated "default blocking"[4] *only* of calls that may be reasonably presumed, based on objective criteria, to be *illegal or unlawful*. Significantly, next week the Commission is expected to make clear that calls originating outside the United States that spoof U.S. telephone numbers are illegal calls.[5] As a result of this

---

[3] Secure Telephone Identity Revisited ("STIR") and Signature-based Handling of Asserted information using toKENs ("SHAKEN") (referred to collectively as "SHAKEN/STIR").

[4] That is, analytics-based blocking that a voice services provider enables by default absent an opt-out election by a specific consumer subscriber.

[5] *See* Implementing the Anti-Spoofing Provisions of the RAY BAUM's Act, Draft Second Report and Order, WC Docket Nos 18-335, 11-39 (rel. Jul. 11, 2019) (for consideration in August 1, 2019 Federal Communications Commission Open Meeting) ("*Anti-Spoofing Draft Second R&O*"). The Commission has never defined what an "unwanted call" is. Now, however, because of the imminent decision on international spoofing, in order to be "aggressive" or "robust," default blocking programs no longer need to reflect a carrier's unilateral decisions as to what calls may be subjectively "unwanted" by a consumer.

important clarification, default blocking programs now may, and should, reasonably target only illegal calls, rather than both illegal and "unwanted" calls.[6] If they do so aggressively, the programs are likely to detect the vast majority of illicit and fraudulent calls, because the Commission's expected upcoming decision will close the only currently significant omission from the definition of "illegal" calls.[7] At the same time, default blocking will be far less likely to result in "over-blocking"[8] of lawful calls, which can have serious adverse consequences.

Second, the Commission should delay mandatory implementation of the SHAKEN/STIR framework until January 1, 2021. However, until blocking programs are further refined, and the SHAKEN/STIR call authentication framework is generally available in the industry, the FCC should establish an interim safe harbor approach ("Interim Safe Harbor") that would protect participating carriers from liability for inadvertent over-blocking, provided they implement non-discriminatory default blocking programs, participate in cooperative industry efforts to resolve over-blocking complaints, and fully inform consumers of the types of calls that may be blocked as a result of their election of a specific call-blocking option. As discussed below, such an

---

[6] Not only users of messaging services but also at least one provider of SHAKEN/STIR implementation software similarly recommends limiting default blocking, even if SHAKEN/STIR is used, to illegal calls only. *See* Ex Parte Presentation of Michael A. Shuster, General Counsel, Professional Association for Customer Engagement, to Marlene H. Dortch, Secretary, Federal Communications Commission at 2 (May 29, 2019) ("*PACE Ex Parte*") (arguing that before the Commission allows carriers to implement opt-out call blocking, it "must provide guidance as to how carriers should distinguish between wanted and unwanted calls.").

[7] *See Anti-Spoofing Draft Second R&O* at ¶ 2. As discussed below, if permitted by the carrier, a consumer, after receiving complete information as to the implications and possible consequences of its decision, may elect to block all calls not included in the consumer's contact list.

[8] "Over-blocking" is used in these Comments to refer to blocking of legitimate calls through use of imprecise blocking program analytics that are not sufficiently narrowly targeted to block only illegal calls and thus return a large number of false positives, unfortunately keeping consumers from receiving important communications.

Interim Safe Harbor approach can be readily implemented, and it should provide almost immediate benefits.

With respect to permissible "analytics-based" call blocking programs, in addition to limiting default blocking programs to targeting only illegal calls, the Commission must restrict the eligibility for Interim Safe Harbor protection to carriers that implement default call-blocking programs that meet specific requirements. These include using only a default blocking program (referred to in these Comments as a "multi-factor" program) whose algorithms rely on a range of both "neutral" factors (that may be characteristic of both illegal and legitimate automated calls) and blocking-antidote "negating" factors (characteristics most typically of illicit calls), as well as ensuring non-discrimination in implementation of blocking programs.[9] Interim Safe Harbor eligibility would also require registration in a Commission system to promote rapid resolution of erroneously blocked calls and a commitment to cooperative traceback efforts, including certification of compliance with requirements for non-discriminatory multi-factor default blocking programs, as well as certification of the carrier's commitment to provide consumers with transparent disclosures of the implications of their blocking choices.

This combination of a clearer definition of the types of calls that may permissibly be blocked and the ways blocking programs may operate, promotion of cooperative industry efforts to address illegal robocalling, and Interim Safe Harbor over-blocking liability protection pending SHAKEN/STIR general availability will encourage vigorous efforts to eliminate illegal robocalling while preventing over-blocking and its adverse consequences, particularly until the SHAKEN/STIR framework is generally deployed industry-wide.

---

[9] *See Ruling* at ¶ 35.

II. THE COMMISSION MUST LIMIT DEFAULT CALL BLOCKING TO AVOID BLOCKING OF IMPORTANT CALLS.

A. The Commission Should Permit Default Call Blocking Only of Calls That Are Reasonably Presumed to Be Illegal Now That This Term is Expected Almost Immediately to Comprise Calls Spoofed from Overseas Bad Actors to United States Call Recipients.

1. International-Originated Calls to U.S. Residents That Spoof U.S. Numbers Should Be Blockable by Default.

The *FNPRM* seeks comment on how the Commission can best leverage Caller ID authentication technology to combat illegal calls originating outside the United States.[10] But the Commission itself has already provided a major part of the answer. The Commission is now expected to adopt a prohibition on spoofed calls from overseas actors to recipients within the United States, expanding implementation of the Truth in Caller ID Act and allowing call authentication technology to identify and block these types of illegal calls.[11] Because carrier networks are generally capable of recognizing calls as originating outside the U.S.,[12] review of call signaling information indicating an international call origin together with review of potentially inconsistent call data record ("CDR") information may detect discrepancies in the call information. Carriers can fairly easily tag such a call as a likely "illegal spoofed call,"[13]

---

[10] *See FNPRM* at ¶ 82.

[11] *Anti-Spoofing Draft Second R&O* at ¶ 10; *see also* RAY BAUM's Act § 503(a)(1), 132 Stat. at 1091.

[12] *See PACE Ex Parte*, Communications Prot. Coal., Report On Best Practices For Mitigating Adverse Impacts Of Robocall Processing On Legal Communications at 13 (May 22, 2019) ("*PACE Best Practices Report*"). The PACE Communications Protection Coalition ("CPC") Report summarizes analytics-based robocall call processing, and explains that "typically," non-analytics-based call blocking functions [to] block facially illegal calls" and thus a carrier blocking calls based on invalid, unassigned, or unallocated numbers are presumed "facially illegal."

[13] *Anti-Spoofing Draft Second R&O* at ¶ 3.

potentially warranting trace-back efforts, especially if the same number is used to initiate multiple calls in a brief period and exhibits other characteristics of calling by illicit spoofers.

The definitional change that the Commission is now making to confirm that internationally-originated calls illicitly spoofing U.S. numbers are illegal calls[14] is a significant contribution to balancing carriers' interest in robust call blocking against the need for completion of legitimate calls. There should no longer be any need for reliance on the value-judgments of carriers as to what constitutes "unwanted" calls in order for carriers to effectively weed out illegal robocalls. The Commission therefore should now adopt implementing rules that clarify that carriers may block by opt-out, default analytics-based programs *only* "illegal" calls, a category that should almost immediately also comprise internationally-originated calls from illicitly-spoofed U.S. numbers.

Allowing blocking by default of only illegal calls should now target the vast majority of scam callers and fraud-call originators and will address the types of calls that consumers and providers most want to block. Further, now that the definition of illegal calls is expected to cover international spoofing, and especially if blocking targets only illegal calls, well-informed consumers should be less likely to opt out of default blocking in favor of broad blocking of all calls originating from numbers not in the specific consumer's contact list (although the option for broad blocking relying on consumer contact-list whitelisting may be preserved to address blocking of calls that are subjectively "unwanted" by a specific consumer). Moreover, limiting default blocking to illegal calls, as re-defined, will also minimize the adverse consequences of over-blocking that can be expected to lead some consumers, albeit reluctantly, to accept the nuisance and potentially fraudulent consequences of the no-blocking option in order to avoid

---

[14] *Anti-Spoofing Draft Second R&O* at ¶ 2.

missing any important calls.[15] Thus, limiting default call blocking to presumed unlawful calls is likely to maximize the consumer welfare resulting from default opt-out analytics-based blocking by carriers.

Also, because the *Ruling* did not take into account the critical factor of the origin of an unwanted call in determining whether it should fall to default blocking, the Commission should take this opportunity to expressly refine the *Ruling* to reflect the forthcoming expanded definition of an illegal call.[16] Because a large proportion of illicit robocalls are spoofed-number calls with international origins,[17] which are now expected to be unlawful under the Commission's upcoming action,[18] providers can effectively use this much clearer, objective standard for default call blocking, at least until there has been sufficient experience with call blocking programs to fine-tune their ability to avoid over-blocking. Once that international-originated illicit spoofing calls are formally recognized as illegal, the Commission can be comfortable in limiting default blocking to targeting only illegal calls, as the Commission had

---

[15] *See* Ex Parte Presentation of Jim Dalton, Chief Executive Officer, TransNexus, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-89, at 2 (July 19, 2019) (explaining that most providers do not want to block calls by default, specifically those providers that may be hospitals or health clinics. These health services providers will "generally answer all calls no matter what" to avoid missing any important call.") ("*TransNexus Ex Parte*").

[16] *See Anti-Spoofing Draft Second R&O*.

[17] As discussed in "Robocalling Wars – Chapter B (for Blocking)" Panel on July 20, 2019 at the National Association of Regulatory Utility Commissioners ("NARUC") Policy Summit in Indianapolis, IN; Moderator Robert McCausland; Panelists: David Bergmann, Ohio Consumers Counsel; Michael Eades, Deputy Attorney General for the State of Indiana; and David Frankel, ZipDX.

[18] *See Anti-Spoofing Draft Second R&O,* at 10-11, revising the Commission's Caller ID rules to cover communications originating outside the United States aimed at recipients within the United States. Section 64.1604 [will] state[s], "No person in the United States, nor any person outside the United States if the recipient is in the United States, shall, with the intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly, or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information in connection with any voice service or text messaging service." 47 CFR § 64.1604.

initially proposed, without concern about undermining carriers' aggressive efforts to interdict illicit calls, and with the positive benefit of minimizing the adverse consequences of over-blocking. Therefore, any default blocking programs should be limited to targeting only unlawful or illicit calls.

2. "Unwanted" Calls Should Be Blockable Only By Express Consumer Election.

a. There is No Need to Block "Unwanted" Calls.

"Unwanted" calls should be blocked by carriers only through implementation of a consumer-elected option, based on a full disclosure of the potential adverse over-blocking consequences, to block all calls not on the specific consumer's contact list. The Commission's rules should reflect the important differences between these two distinct categories of calls, and it should refrain from authorizing opt-out default (rather than consumer white list-based opt-in) call blocking for subjectively unwanted calls.

The *Ruling* permitted voice service providers to block "unwanted calls" using programs informed by "reasonable analytics" and consumer-contact based white list blocking programs.[19] For the first time, the Commission allowed voice service providers to offer call blocking programs on an opt-out basis "based on any reasonable analytics to identify unwanted calls."[20]

However, nowhere in the *Ruling* or *FNPRM* does the Commission define what specific call characteristics would warrant classification as an "unwanted call." Indeed, such a determination would have to require second-guessing what can only logically be a consumer-

---

[19] The Commission defines "blocking" in the *Ruling* "to mean stopping calls outright so that they do not ring a phone, routing the calls directly to voicemail without ringing the phone, or some other treatment, such as an interactive voice response session or voice call screening." *Ruling* at n. 47.

[20] *Ruling* and *FNPRM* at ¶ 34.

specific subjective determination.[21] Nor does the *Ruling* explain the shift from the Commission's proposal to permit blocking only of "illegal" calls in the Commission's 2017 *Notice of Proposed Rulemaking and Notice of Inquiry*.[22] Rather, the *Ruling* only irrelevantly relies on the FCC's authority to provide consumer choice and the legal authority and consumer right to block unwanted calls.[23]

Throughout the *Ruling* and *FNPRM*, the Commission does not clearly define what separates an illegal call from an unwanted call, and often the Commission uses these terms interchangeably.[24] While West supports the Commission's goals and the industry efforts to eliminate illegal calls, "illegal calls" and "unwanted calls" are not one and the same. From a

---

[21] *See* ATIS Comments, CG Docket No. 17-59 at 4 (July 4, 2017) (while supporting the Commission's TCPA definition of an "illegal call," ATIS explains that "in many cases the difference between a legal and illegal robocall may depend on the call originator's intent, which is generally not something that the industry can identify.").

[22] *See 2017 NPRM* at ¶ 10. "Specifically, we propose that voice service providers may block telephone calls in certain circumstances to protect subscribers from illegal robocalls." *Compare with FNPRM* at ¶ 75, stating, "Unwanted and illegal robocalls and caller ID spoofing are problem that affect all consumers, however, not just those who are served by larger service providers."

[23] For example, the *Ruling* states that, "[s]etting a call-blocking program as the default can significantly increase consumer participation [in opt-in programs] while maintaining consumer choice." *Ruling* at ¶ 27. The *Ruling* elaborates that against the background of consumer choice, the Commission "reiterates that 'there appears to be no legal dispute in the record that the Communications Act or Commission's rules do not limit consumers' right to block calls, as long as the consumer makes the choice to do so.'" *Ruling* at ¶ 31, citing *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, WC Docket No. 07-135, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8035, ¶ 156 (2015) ("*2015 TCPA Order*").

[24] Significantly, in asking the Commission to clarify that the Ruling applies to unwanted calls, rather than illegal calls, CTIA and USTelecom noted that the "interchangeable use of the terms 'illegal' and 'unwanted' may create uncertainty that deters voice service providers from taking aggressive actions." *See* Ex Parte Presentation of Matthew Gerst & Farhan Chugtai, CTIA and USTelecom, to Marlene H. Dortch, Secretary, FCC, at 2-3 (May 30, 2019) ("*CTIA/USTelecom Ex Parte*). With the clarifications and implementation of the Interim Safe Harbor approach West recommends, carriers should have no such uncertainty or be deterred thereby from taking vigorous, targeted blocking action.

provider perspective, voice service providers may use different tools to block and label illegal calls compared to the tools used for unwanted calls.[25] Conflating these terms allows the carrier unilaterally and imprecisely to substitute its own view of what is an "unwanted" call for what inherently is a subjective determination by an individual consumer. Whether a call is an "unwanted call" that should be blocked is a determination that should be left to the subjective discretion of the consumer, who may be offered an option to block all calls not originating from a number on the consumer's white list.[26]

b. Default Blocking of "Unwanted" Calls Risks the Adverse Consequences of Over-Blocking.

If the Commission nonetheless decides to allow default blocking even of carrier-determined "unwanted calls," the Commission should clarify and narrow the types of calls that may be classified as "unwanted calls" and then targeted by default call-blocking programs. The category of "unwanted calls" must expressly *exclude* both calls that fall under the *Ruling*'s definition of "emergency calls," and calls from numbers not included on a Critical Calls list but

---

[25] Comments of the USTelecom Association, CG Docket No. 17-59 at 3 (noting that "[j]ust as there are a diversity of tools available to consumers to mitigate illegal or unwanted robocalls, there is a similar diversity in identifying such calls.") *See also PACE Best Practices Report* at 11-12. PACE has pointed out that there are two types of carrier-initiated blocking methods. The first relies on information in call signaling to fairly objectively identify discrepancies, such as the international origin of a call purporting to be from a U.S. caller, that might mark a particular call as potentially unlawful. The second may use independently-derived algorithms based on analysis of characteristics of a traffic stream in an effort to distinguish unlawful from lawful calls. Using the non-U.S. origin of a call purportedly from a U.S. number may be a relatively straightforward example of the first approach to identifying a potentially spoofed call. *See also* Ex Parte Presentation of John C. Ayers, VP, First Orion Corp., to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97 (July 23, 2019) ("*First Orion Ex Parte*") (outlining First Orion's use of its in-network analytics to identify specific call elements and determine whether a call is fraudulent).

[26] *See TransNexus Ex Parte* at 2, explaining that, for instance, certain consumers would choose different blocking program levels, and that consumers should accordingly be given this choice – "one size does not fit all."

that are still important to consumers and whose completion is in the public interest.[27] The Commission has previously recognized and, in fact, encouraged using call-blocking technologies that incorporate features that ensure calls like municipal and school alerts are not blocked,[28] and suppliers of blocking applications such as YouMail represent that they can protect these important calls from blocking.[29] Yet such protection is jeopardized if a carrier may default-block important calls based on its insufficiently-informed unilateral determination that a given call is "unwanted."

Allowing blocking programs to target even subjectively-determined "unwanted" calls, in addition to "illegal calls" as the category is soon to be re-defined, can result in substantial and unnecessary "over-blocking" of important, legitimate calls that may be swept up by imprecise default blocking programs that are not focused on eliminating bad actors. Such over-blocking can have serious adverse consequences for the public, as consumers fail to receive critical and important information about such matters as the availability of important medical test results or sudden school closings.[30]

---

[27] The *Ruling* defines emergency calls as calls originating from "public safety entities, including PSAPs, emergency operations centers, or law enforcement agencies." *Ruling* at ¶ 36, citing *2015 TCPA Order*, 30 FCC Rcd at 8036.

[28] *See Ruling* at ¶ 33, n. 72, citing *2015 TCPA Order* at 8038, ¶ 161

[29] YouMail vs. Nomorobo, YouMail, https://www.youmail.com/home/competitor/youmail-vs-nomorobo (last visited July 24, 2019). Such companies may rely on consumer involvement to refine their databases, although the specific methods they use are proprietary, and their public disclosure may risk circumvention by bad actors.

[30] *See* Ex Parte Presentation of Mark W. Brennan, Counsel to the American Association of Healthcare Administrative Management, to Marlene K. Dortch, Secretary, FCC, CG Docket Nos. 02-278, 17-59, 18-152, WC Docket No. 17-97, at 2 (May 28, 2019) ("*AAHAM Ex Parte*") (explaining that the Ruling creates "problematic side effects" because it places legitimate alerts and reminders from legitimate companies in the same category as fraudulent scam calls. Further, because the Ruling places the burden on customers to opt-out, "consumers may not receive the calls they want (and may not even know that such calls were blocked).").

Thousands of West's customers are subscribers to West Notification Services, which includes West's SchoolMessenger Service. SchoolMessenger provides critical messages to students and parents. Delivering more than a billion messages per year with speed and accuracy,[31] SchoolMessenger delivers emergency communication services in times of crises (as well as important, but non-emergency communications) to parents, students, and communities. These notifications are delivered via voice calls and texts from unique ten-digit numbers to subscriber devices. Such communications made from schools are vital, especially in all too frequent times of school emergencies when parents and guardians need to be alerted as quickly as possible. It is therefore imperative that these calls not be included in any definition of an "unwanted" call that would authorize their default blocking. For example, a frequently-used number not stored in a contact list could be the number of a school, business, or health center. Yet, under the current over-permissive policy, that number could be at risk of being blocked by default opt-out blocking, even though, in contrast to calls from spoofed numbers, the caller uses the same number or same set of numbers in "bursts," calling repeatedly over a period of time to reach the same consumer devices. Not only would blocking these messages place families and communities at risk of harm, but it would also imperil the ability of messaging services to provide the important service platforms to calling parties on a cost-effective basis.

Customers are able to make an informed decision to stop receiving these types of messaging services by electing the option to do so through individual contact list-based blocking or by unsubscribing to individual message alerts. The Commission therefore has no reason to

---

[31] *See SchoolMessenger Communicate: Trusted by the Most K12 Schools*, West (2019). Providing these services to school districts across the nation, SchoolMessenger is the largest communications network in K-12 education, featuring the most full-featured messaging product for schools to communicate with parents and guardians. Furthermore, SchoolMessenger is used by three branches of the military, as well as numerous first responders.

allow, and should not allow, default blocking of these types of critical calls, because of the significant risk of adverse consequences to the public.[32]

B. To Qualify as a "Reasonable" Analytics-Based Default Call Blocking Program, a Program Must Comprise Analysis of "Negating" Characteristics Exhibited Primarily by Unlawful Calls as Well as Analysis of "Neutral" Call Characteristics Typical of Both Unlawful and Lawful Robocalls.

The *Ruling* also provides that voice service providers may block calls by default using programs applying "any reasonable analytics" to identify calls to block. In allowing for *any* reasonable analytics to inform these programs, the Commission rationalizes that this will promote flexibility for providers and allow for blocking schemes to evolve.[33] West agrees that blocking programs must have the ability to respond and advance with new technologies, and to respond to new bad actors and illicit calling schemes. However, in order to optimize identification of the set of calls to be blocked so as to avoid over-blocking, and to ensure consumers receive the important calls they need and expect, the Commission must require that default blocking programs include negating factors that would counter an initial tagging of a call or traffic stream as unlawful. Without required use of such negating factors to better assist in identifying the appropriate set of calls to be blocked, consumers will all too frequently be deprived of important calls through false-positive over-blocking.[34]

---

[32] The Commission should similarly exclude notifications from medical providers, pharmacies, and other similar important services, from calls targetable for blocking. *See TransNexus Ex Parte* at 1 (arguing that customers should have the choice to block calls, specifically those customers who are hospitals or health clinics and "will generally answer all calls no matter what" to avoid missing any important call).

[33] *Ruling* at ¶ 34.

[34] *Id.*; *See* Letter from Linda Vandeloop, AVP Federal Regulatory, AT&T, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 at 4 (filed Mar. 6, 2018).

In the *FNPRM*, the Commission offers a list of possible factors that "may be effective" in creating a call-blocking program based on reasonable analytics, including identifying bursts of calls, call duration, low call completion ratios, and dialing patterns, among several other factors.[35] These are, however, all "neutral" factors characteristic of both lawful and unlawful calling. Significantly, when the Commission proposed in the *2017 NPRM* "provider-initiated blocking based on objective criteria," the Commission expressly inquired into incorporating false positive data into the analysis, among objective factors.[36] Inexplicably, those factors were left out of the suggested analytical factors in the *Ruling*.[37] Especially in light of the imminent expanded redefinition of an illegal call, the Commission should now rectify that deleterious omission.

When negating factors are incorporated into an analysis protocol, they provide a critical "antidote" against false positive blocking of calls exhibiting neutral factors characteristic of both unlawful and lawful robocalling. In addition to the absence of discrepancies as to the origin of the calls, such negating factors may include no clear pattern of the same spoofed numbers initiating a high volume of calls, and that there had not been misuse of the same initially-suspect

---

[35] *FNRPM* at ¶ 35 (also suggesting common Caller ID Name ("CIDN") values across providers, volumes of complaints related to a suspect line, neighbor spoofing patterns, patterns that indicate TCPA or other contract violations; correlation of network data with data from regulators, consumers, and carriers; and comparison of dialed numbers to the National Do Not Call Registry).

[36] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 2306 at 2314, ¶ 29-30 (2017) (*2017 NPRM*). *See First Orion Ex Parte* at 2, noting that the Commission has previously said that "a combination of certain relevant factors or objective standards serve as reasonable analytics," and elaborating on its call registry which allows legitimate originators to register their numbers to help prevent false positives.

[37] *Id.*; *Ruling* at ¶ 34, "clarify[ing] that voice service providers many offer opt-out call blocking programs based on any reasonably analytics designed to identify unwanted calls."

number to initiate robocalling previously determined to be unlawful. Additionally, to warrant being deemed "reasonable," analytics programs should account for other characteristics of legitimate calls that can better distinguish and minimize blocking of wanted calls.[38] For example, a number that is used on a regular, repeated basis, but not necessarily on the same day, in calling groups of consumers, especially if many of the called recipient groups have a common area code or codes, may be an indication that it is a legitimate calling number, rather than one that should be default blocked. The absence of consumer complaints when a large number of calls are placed in a short period of time, many of which are sent to numbers with common area codes, may also indicate legitimate calls.[39] Repeated use over time of a number to contact a fairly consistent set of numbers, especially in similar area code areas, could also be a useful factor in ensuring that a legitimate number is not blocked by default.

Requiring both negative and neutral factors to be reflected in call blocking programs will go a long way toward ensuring that providers will more accurately filter out scam calls without over-blocking and denying completion of important calls. This approach will create better

---

[38] *See AAHMA Ex Parte* at 2, explaining that the *Ruling* risks blocking or mislabeling of important, wanted calls, namely health and safety calls, due to "the large volume of outbound calls that a company places from each number in a short period of time, which is one analytical factor described for determining when a call can be blocked."

[39] Conversely, a large number of complaints of missed calls of the same or similar nature should alert a carrier to remove the originating number from any internal blacklist, especially when there are no indicia of international spoofing or other characteristics of unlawful calling. The carrier should also utilize the contact system to immediately alert the affected calling party or its provider. Applications such as those provided by YouMail and NoMoRobo utilize consumer interaction as a means of refining lists of blockable numbers.

blocking systems that serve consumers effectively by tracking a wide range of factors to differentiate scam calls from legitimate calls that should be completed.[40]

III. THE COMMISSION SHOULD ENSURE CONSUMERS BASE OPT-IN AND OPT-OUT CHOICES ON A CLEAR UNDERSTANDING OF THE TYPES OF CALLS THAT MAY BE BLOCKED BY THEIR INTENTIONALLY-CHOSEN OPTIONS.

In the *Ruling*, the Commission authorizes voice service providers to block calls using white list programs; that is, programs that block all calls from numbers not saved in an individual consumer's contact list.[41] Consumers have the choice to affirmatively opt-in to this blocking. However, blocking calls solely based on a customer's unique contact list is likely to lead to drastic over-blocking of important, wanted calls even if a consumer is extremely diligent in attempting to keep the white list up-to-date. The *FNPRM* seeks comment on other ways to block calls that would protect callers from erroneous blocking, and on any other bases for blocking unwanted, illegal calls.[42]

The Commission should require that voice service providers provide consumers full disclosures of the types of calls that may be blocked by each option. This is needed for consumers to make fully-informed call blocking choices among the options of no call blocking; blocking based on their specific carrier's analytics (which should target only illegal calls and

---

[40] *See TransNexus Ex Parte* at 3, explaining that call authentication frameworks become the most valuable when combined with other blocking or analytics services. TransNexus notes that rural customers may be particularly vulnerable to over-blocking, and the failure to require inclusion of negating factors may thus run counter to the achievement of the Commission's rural call completion goals.

[41] *FNPRM* at ¶ 43.

[42] *FNPRM* at ¶ 70.

conform to the requirements recommended here); and white list blocking[43] of all calls originating from numbers not stored in the consumer's contact list.

To be adequate, the disclosure should include information reasonably likely to alert a consumer that election of a particular call-blocking option may result in the consumer's missing, for example, important notifications from schools, medical providers, and pharmacies,[44] unless, and even if, the consumer proactively takes affirmative steps to update the consumer's contact list to include the relevant entities.[45] To adequately protect consumers, providers should also be required to include in the disclosures the express types of calls that could be blocked if the carrier blocks calls that it subjectively deems "unwanted," potentially including calls from schools, medical services, and pharmacies. Further, in ensuring consumer understanding of the implications of each call blocking option, providers must convey to consumers the importance of keeping contact white lists updated.

Such mandatory disclosure would implement the *Ruling*'s requirement that providers offering opt-out programs "must offer sufficient information" regarding their opt-out options,

---

[43] That is, as expressly elected by an individual consumer, blocking of every call not originating from a number other than those on that consumer's individual contact list (or consumer-specific "white list").

[44] The Commission explains that it "knows consumers value calls from schools, doctors, local governments, and alarm companies, as well as fraud and weather alerts, and…calls from recall centers hospitals and flight alerts." *FNPRM* at n. 115, citing Comments of TNS at 19 (July 3, 2017).

[45] While, for example, a parent may diligently update the contact list to include new school system, school, and teacher numbers, even some school-originated communications come from a variety of numbers not distributed in advance to parents. It is even less likely, for example, that a consumer could update the contact list to include every number used by every one of the consumer's medical providers or pharmacies. It would also be helpful for the Commission to also implement a consumer-friendly mechanism for consumers to use to report important missed calls to their carriers, with carriers required promptly to report to call providers the inadvertent transmission blockages and to modify blocking programs to prevent future over-blocking.

and further that providers "should" clearly disclose what kinds of calls may be blocked and the risk of those blocked calls.[46] This will help to ensure that significant numbers of wanted calls are not subject to erroneous blocking and that customer expectations are met with regard to the type and amount of blocking that the consumer intends and the calls the consumer expects to receive or not receive.

IV. THE COMMISSION SHOULD PROVIDE CARRIERS WITH AN EXTENDED TIMEFRAME TO COMPLY WITH THE SHAKEN/STIR FRAMEWORK, AND PROVIDE AN INTERIM SAFE HARBOR FROM CALL BLOCKING LIABILITY DEPENDENT ON CERTIFIED COMMITMENT TO AND IMPLEMENTATION OF MULTI-FACTOR ANALYSIS, NON-DISCRIMINATORY PRACTICES, FULL DISCLOSURE TO CONSUMERS, AND PARTICIPATION IN A RAPID RESPONSE OVER-BLOCKING COMPLAINT REMEDIATION PROCESS.

A. The Commission Should Provide Carriers With an Extended Timeframe to Comply With the SHAKEN/STIR Framework Before the Commission Takes Any Mandatory Compliance Action.

The *FNPRM* proposes that if major voice service providers fail to meet the current end of 2019 deadline for voluntary SHAKEN/STIR implementation, the Commission will mandate that those providers meet the implementation timeline.[47] However, the Commission also recognizes that smaller providers "will eventually implement the SHAKEN/STIR framework, [but the Commission is] also conscious that they may need more time" than larger providers to appropriately transition their networks.[48] Moreover, the *FNPRM* acknowledges that many small providers "lack the financial ability and in-house professional expertise necessary" to quickly implement the framework, and the Commission asks if it should therefore adopt staggered

---

[46] *Ruling* at ¶ 33.

[47] *FNPRM* at ¶ 71.

[48] *FNPRM* at ¶ 56.

timetables for implementation deadlines.[49] The *FNPRM* also proposes a narrow safe harbor for voice service providers that offer call-blocking programs using SHAKEN/STIR authentication to determine whether a call has been properly authenticated, and for calls that fail authentication in other specific instances under the framework.[50]

West agrees that smaller carriers should have an extended timeframe for SHAKEN/STIR implementation. Industry and service providers, including West, are working quickly to implement and effectuate SHAKEN/STIR attestation within their networks to authenticate calls and weed out bad actors.[51] However, as deployment of this framework requires valuable time and resources, some providers are able to move faster than others in ensuring a workable network authentication process, and as of now, in many cases, joint testing of SHAKEN/STIR systems has not been completed, and they are not yet ready for full provider implementation.

To accommodate unanticipated industry-wide delays in SHAKEN/STIR deployment, the Commission should delay mandatory SHAKEN/STIR deployment for smaller providers. West therefore recommends a January 1, 2021 deadline for compliance. This extended timeframe will allow smaller providers one additional year beyond the current proposal to mandate SHAKEN/STIR authentication for major providers by the end of 2019.[52] Several carriers currently estimate that they expect to fully deploy the framework in either early- or mid-2020.[53]

---

[49] *FNPRM* at ¶ 78.

[50] *FNPRM* at ¶ 49, 51.

[51] West, in addition to participating in the ITG, also uses a "know your customer" onboarding protocol to ensure the bona fides of new wholesale customers.

[52] *FNPRM* at ¶ 71.

[53] *See, e.g.*, Letter from Thomas M. Rutledge, Chair, Charter Communications, to Commissioner Geoffrey Starks, GC Docket No. 17-59, WC Docket No. 17-97 at 2 (July 10, 2019).

A January 1, 2021 compliance deadline will ensure that carriers are granted a reasonable amount of time to fully deploy call authentication, but will still encourage providers to move quickly to aim to deploy before the deadline expires.

West also supports the Commission's eventual creation of the safe harbor for providers that employ SHAKEN/STIR authentication and validation. In the meantime, to encourage vigorous efforts to remediate illicit call blocking, carriers should be entitled to Interim Safe Harbor protection if they meet the requirements discussed below.

B. An Interim Safe Harbor Will Accommodate Carriers' Concerns That May Inhibit Robust Call Blocking, While Avoiding Over-Blocking Prior to Widespread Deployment of SHAKEN/STIR.

Until the SHAKEN/STIR framework is implemented by all carriers, and all providers can successfully complete full call attestation and experiment with blocking metrics that pose a lower risk of causing discriminatory conduct or over-blocking, an Interim Safe Harbor should be implemented to provide liability protection for inadvertent over-blocking. This would encourage carriers to engage in good faith robust call blocking efforts as they refine their default blocking systems.

1. The Interim Safe Harbor Would Require Provider Registration and Certification.

To qualify for the Interim Safe Harbor protection, providers would obtain certification as a verified provider, through a system building on the Commission's existing certification processes.[54] The verification would require the provider to consent to being under the legal

---

[54] The Commission's Intermediate Provider Registry, which is a brief registration to certify provider status, is an example that could be emulated for this purpose. This new system could be an amendment to that one, although some providers would participate that do not participate in that system, and vice versa. It would only require amending the existing form and periodic certification statements to reflect this additional registration and certification. Points of contact

jurisdiction of the United States and of the Commission itself, should the registrant commit deliberate violations of the robocalling rules, and to certify the registrant's compliance with the implementing standards required for Safe Harbor protection. This type of certification would also allow a provider to affirmatively confirm its status as a legitimate call originator, rather than an illegal or scam call originator, and identify a main "call blocking" point of contact for other certified providers to contact in cases of erroneous call blocking and with whom to engage in immediate unblocking of affected numbers and collaborative efforts to avoid any blocking problems in the future.

As part of their registration, providers would make a certified commitment: to implement only default blocking systems that use a combination of neutral and negating factors (a multi-factor analysis) to inform call blocking analytics; to implement call blocking on a non-discriminatory basis; to participate pro-actively in a rapid complaint response process; and to fully inform consumers of the implications and consequences of their blocking options.

2. Participation in an Efficient Rapid-Fix Complaint Resolution Process Should be a Prerequisite for Safe Harbor Protection.

The interim Safe Harbor system should incorporate a streamlined, cooperative industry process to allow over-blocking complaints regarding the call blocking process to be almost instantly resolved. Cooperative implementation of problem resolution procedures would also provide experience to help providers refine the analytics used by default blocking programs. West therefore encourages the Commission to establish cooperation in the program as a requirement for eligibility for the Interim Safe Harbor.

---

could be specific for this purpose, or existing registered contacts could also be designated for this purpose.

Many providers already participate in cooperative efforts to identify fraudulent callings, and the Industry Traceback ("ITB") Group has been a valuable resource in quickly rooting out scam callers.[55] For example, West and AT&T have enjoyed a successful collaborative relationship working in concert to identify and block illegal calls. The Commission has already urged providers not yet involved in industry traceback groups to participate in these efforts, agreeing that "industry cooperation is vital to achieving" the goal of catching and stopping illegal call scammers.[56] Participation in rapid-response cooperative efforts should also allow carriers to refine their analytics to exclude the types of calling patterns that characterize legitimate calls, as well as to mitigate the adverse effects of any blocking. A collaborative rapid-response effort from a coalition of providers would result in an effective solution against over-blocking and benefit each provider as they hone blocking programs designed to effectively identify and block illegal calls.

Implementation of the Interim Safe Harbor would establish a self-effectuating rapid-response complaint resolution system for erroneously blocked calls.[57] The Commission already

---

[55] Managed by USTelecom, "Traceback" is a "cooperative effort by telecommunications providers to address the illegal robocall scourge." The traceback process "traces back to calls using a secure, web-based automatic process" and can trace calls to the origin within hours or days. *https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/*. For Interim Safe Harbor eligibility, providers should commit to participation both in over-blocking complaint resolution and in cooperative traceback efforts in matters involving their networks and traffic.

[56] FCC News Release, *FCC Calls on Network Voice Providers to Join Efforts to Combat Illegal Spoofed Scam Robocalls: Enforcement Chief and Chief Technology Officer Wrote to Voice Providers About Helping 'Traceback' Efforts to Stop and to Catch Scam Callers* (Nov. 6, 2018).

[57] The *Ruling* states that callers may file a petition for reconsideration with the Commission for review of a call-blocking program if they believe their calls have been inadvertently blocked or misidentified as an unwanted call and subsequently blocked. *Ruling* at ¶ 38. However, call recipients that expect to receive certain calls and that have concerns about a particular blocking program should not be required to jump the hurdles of administrative process to alert the Commission of misapplied call blocking.

requires carriers to establish a point of contact for call blocking issues, but merely *encourages* voice service providers to develop a mechanism for notifying callers of their blocked calls.[58] Call originating providers need to have an easier and more accessible mechanism for alerting other providers of a call-blocking program that is erroneously blocking calls. Specifically, there must be an efficient, provider-friendly system to quickly alert the blocking provider, and the Commission should require voice service providers to develop a mechanism for dealing with blocked calls to ensure that callers have a way to resolve the issue directly with the blocking carrier.[59] Lastly, providers also must play a self-monitoring role in ensuring that consumer calls are not inadvertently blocked and that there are appropriate mechanisms to remedy these situations expeditiously.

The Commission's role could be limited to hosting the system and oversight monitoring to gain information about blocking concerns, and to stepping in promptly if there are complaints about certifying registered providers failing to comply with their Interim Safe Harbor status commitments and obligations. The Commission could also implement a simplified consumer complaint system, perhaps similar to that established by Mississippi, that would promote further refinement of program analytics by flagging instances of illicit calling, or of over-blocking of wanted calls.[60]

---

[58] *Ruling* at ¶ 38. (emphasis added).

[59] *See PACE Ex Parte* at 2. PACE similarly suggests that the Commission implement transparency and mitigation practices for mistaken call blocking, and that "any safe harbor should be available only if the carrier offers mitigation mechanisms to quickly identify, notify, and correct such mistakes."

[60] *See Complaint Filing*, Mississippi Public Service Commission No Call Program, https://www.psc.state.ms.us/nocall/complaint.aspx (last visited July 24, 2019).

3. Non-Discriminatory Blocking Protections Must be a Prerequisite for Interim Safe Harbor Eligibility, Including Prohibiting Reliance on the SHAKEN/STIR framework for Blocking Purposes Instead of Multi-Factor Criteria Until Carriers Have Had Sufficient Time for SHAKEN/STIR Implementation.

The Commission must also ensure that, as required by the *Order*, call blocking is implemented in a neutral, non-discriminatory manner.[61] By not defining the call-blocking programs or reasonable analytics that would qualify as non-discriminatory, however, the Commission has left a vacuum, thereby, for example, allowing larger carriers to create programs that may favor their own message distribution customers, even though the standards applied may, on their face, be objective.[62] West recommends that the Commission establish a more defined prohibition against discriminatory tactics with set criteria to better guide and inform providers' call-blocking programs, and encourage joint industry efforts to tackle the problem of illegal robocalls.

West encourages the Commission to implement in the Interim Safe Harbor a requirement that a qualifying blocking program not only incorporate multi-factor criteria, but also that those criteria be implemented in a non-discriminatory manner, and not just in a way that is seemingly neutral on its face. For example, to qualify for Interim Safe Harbor protection as a "reasonable" analytics-based default call blocking program, a default blocking program must implement call

---

[61] *See Ruling* at ¶ 35.

[62] *See* Ex Parte Presentation of Michael Romano, Senior Vice President, NTCA – The Rural Broadband Association, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 17-59, WC Docket Nos. 17-79, 18-155, CC Docket No. 01-81, at 2 (July 18, 2019) ("*NCTA Ex Parte*") (encouraging the Commission to establish clear rules to govern SHAKEN/STIR interconnection issues, as without such guidance, smaller providers could be at the control of larger providers. NTCA argues that as a result, "these larger providers could quite easily shift to these small carriers the costs of transporting voice calls between rural operators' local network edges and distant points of interconnection – fundamentally remaking the economics of interconnection and foisting the costs of transport fully onto small rural customer basis.").

blocking in a manner that is nondiscriminatory both on its face and as applied. Blocking program analytics and protocols must, for example, incorporate "negating" criteria holistically and objectively. Because negating factors operate as an antidote to blocking, it would not be sufficient for such potentially offsetting factors, to, in practice, be characteristic only of communications originating on the carriers' own network or on a small group of networks including those of its affiliates and partners.[63]

Further, at this stage of implementation of the SHAKEN/STIR framework, and before carriers have refined their analytics to avoid over-blocking, there is potential for anti-competitive and discriminatory actors to rely exclusively on SHAKEN/STIR to neutralize a preliminary blocking "hit." This gives unwarranted preferential treatment to the largest providers who have already been able to implement SHAKEN/STIR authentication practices. To avoid this problem, which would cause carriers without framework implementation to experience unnecessary call blocking, the Commission should find that, until there has been a reasonable period, until January 1, 2021, for the majority of IP-based carriers to implement SHAKEN/STIR call authentication and verification systems,[64] default call blocking programs may not block calls merely because they are not yet authenticated by the SHAKEN/STIR framework in order to qualify for a liability Interim Safe Harbor.

---

[63] Moreover, if, for example, the fact of such "self-origination" is a dispositive go-no go criterion for blocking a call, the system could accord preferential freedom from over-blocking for "self-originated" calls while blocking legitimate calls originating on other networks.

[64] SHAKEN/STIR refers to the industry-developed system to authenticate Caller ID and address unlawful spoofing by confirming the caller number or at least that the call entered the US network through a particular voice service provide or gateway. The Commission notes that since SHAKEN/STIR is intended for Internet Protocol ("IP") networks, calls originating, transmitting, or terminating on TDM networks may not benefit from the framework. However, additional time may allow a similar approach to develop for legacy systems like TDM to implement an authentication technology.

V. CONCLUSION

For the reasons discussed above, West respectfully requests that the Commission adopt its recommendations to ensure that carriers can engage in robust call blocking that is effective against illicit robocalling without causing over-blocking of legitimate calls and its serious adverse consequences.

Respectfully submitted,

WEST TELECOM SERVICES, LLC

Robert W. McCausland
VP, Regulatory and Government Affairs
West Telecom Services, LLC
3200 W. Pleasant Run Road
Suite 300
Lancaster, TX 75146-1086
RWMcCausland@west.com
Phone: 469-727-1640
Fax: 866-432-3936
Cell/Text: 469-644-4954

By: /s/ Helen E. Disenhaus
Carolyn A. Mahoney
Telecommunications Law Professionals PLLC
1025 Connecticut Ave, N.W., Suite 1011
Washington, DC 20036
Phone: 202-789-3123
Fax: 202-789-3122
hdisenhaus@telecomlawpros.com
cmahoney@telecomlawpros.com
Counsel for West Telecom Services, LLC

July 24, 2019