Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 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

REPLY COMMENTS OF VERIZON

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 500 East
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon

January 10, 2022

TABLE OF CONTENTS

SUMMARY AND INTRODUCTION

The Commission has correctly committed to taking aggressive action to mitigate the flow of illegal robocalls from abroad.[1] To do so, it should strengthen and internationalize the regulatory regime it has already built: it should adopt USTelecom's proposal[2] to close the loophole that allows foreign intermediate providers to bypass the Robocall Mitigation Database and impose meaningful robocall mitigation obligations on *all* service providers that handle calls with U.S. "calling party" numbers. It should not pursue policies that would create substantial burden, uncertainty, and disruption without corresponding consumer benefits. In particular, it should not attempt to define a new class of "gateway" providers and expect them to single-handedly stop illegal foreign-generated traffic because bad actors would readily bypass that regime. And it should not mandate a burdensome STIR/SHAKEN obligation for intermediate providers because that would not protect consumers.

While the Commission should not attempt to assert jurisdiction over any foreign entity that uses *foreign* telephone numbers to call U.S. consumers, it can and should regain control over U.S. numbering resources. The Commission's anti-robocall strategy should be driven by the principle that every entity, regardless of location, that chooses to handle traffic with U.S. "calling party" numbers should be required to step into a regime that ensures such traffic is not illegal. Without that common-sense principle in force, illegal foreign robocallers will continue to

---

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct. 1, 2021) ("*FNPRM*").

[2] *See* Comments of USTelecom – The Broadband Association, CG Docket No. 17-59, WC Docket No. 17-97 (filed Dec. 10, 2021) ("*USTelecom Comments*").

impersonate U.S. callers and scam U.S. consumers. The centerpiece of the Commission's policy should be creating a "chain of trust" for all calls to U.S. consumers if those calls purport to be made from U.S. telephone numbers. That chain of trust requires that all service providers seeking to handle calls with U.S. telephone numbers must register in the Robocall Mitigation Database and to treat every upstream relationship as binary: either the traffic is from an end user (in which case it must have measures in place to ensure that customer is not making illegal robocalling) or it is from another service provider (in which case it must ensure that upstream service provider is in the Robocall Mitigation Database and should be appropriately vetting and monitoring that service provider).

As the industry leader on "know your customer" and monitoring at interfaces between service providers, Verizon has demonstrated that robocall mitigation by intermediate providers can materially clean up the traffic traversing the Public Switched Telephone Network (PSTN). Our dedicated team of data analysts, fraud specialists, and attorneys have removed *billions* of illegal robocalls from Verizon's networks by monitoring traffic, engaging with providers that send unhygienic traffic, and where necessary terminating relationships with providers unwilling to clean up their traffic. Every service provider should certify to having a similar program, although these programs do have limitations and cannot by themselves be mandated as a panacea. To promote uniform meaningful robocall mitigation practices that can be implemented at scale by all Robocall Mitigation Database registrants, the Commission should consider encouraging the use of private sector-led reputation monitoring services so registrants can easily determine whether or not they are doing business with trustworthy service providers.

Other proposals raised in the FNPRM would stymie, not advance, the Commission's call authentication and robocall mitigation goals. The proposal to foist all responsibility to stop

foreign-originated illegal calls onto a new class of "gateway" providers would create a complex set of burdensome and ineffective obligations with which only good actors would comply, while bad actors would readily find ways to avoid being classified as "gateways." And the proposal to require gateway service providers to add STIR/SHAKEN signatures to unsigned calls they receive would flood the ecosystem with billions of useless "C" attestations that will not benefit consumers or help with tracing back illegal traffic. If the Commission perceives the need to improve on the existing traceback process, a far more effective (and far more cost-effective) policy would be to require service providers to step up their participation in the Industry Traceback Group (ITG). While some service providers balk at being required to respond to tracebacks even within 24 hours, Verizon has implemented a secure automated traceback response system that on average responds to ITG in less than a minute.

Finally, regardless of whether the Commission pursues USTelecom's proposal or some version of the proposals in the FNPRM, it should ensure that foreign service providers have sufficient time to understand clearly the new regime and how it may affect their operations. Although no foreign service provider would be affirmatively obligated to do anything under any of the proposals in the record (as long as it refrains from using U.S. numbering resources), the new rules would likely substantially disrupt existing "least cost routing" arrangements, thereby restructuring traffic flows and potentially requiring the re-sizing of certain telecommunications infrastructure. The Commission also should actively coordinate with those of its foreign counterparts that are similarly working to address the international robocall problem, and conversely should address the fact that for geopolitical or other reasons, some foreign regulators and foreign service providers may not embrace the Commission's policies.

I. THE COMMISSION SHOULD FOCUS ON STRENGTHENING ITS ROBOCALL MITIGATION DATABASE REGIME AND APPLYING IT INTERNATIONALLY

A. The Commission Should Protect Consumers with an Unbroken "Chain of Trust" from the Origination Point of the Call to the Consumer.

The Commission should require all types of voice service providers handling calls from one U.S. phone number to another U.S. phone number to protect the called party from illegal robocalls. The registration requirement will ensure that all entities in the call path are subject to Commission oversight and provide the Commission with tools to remove complicit service providers from the call path.[3] That will create a chain of trust between the originating service provider (who ensures the calling party is not making illegal calls), through a chain of registered intermediate providers, to a terminating provider.

To create that chain of trust it is important that the Commission not leave any gaps by permitting service providers that register with the Robocall Mitigation Database to take traffic from any untrusted entities. Currently, the Robocall Mitigation Database is sometimes complicated by ambiguity about the status of certain entities, such as conferencing services, that may not clearly be "voice service providers" under the Commission's definitions and that also currently may not be considered "end users" by some service providers. The Commission should remove that ambiguity by making clear that *every* relationship a Robocall Mitigation Database registrant has with an upstream entity falls into one of two categories:

- Service Provider Relationships. If the registrant's relationship is with an upstream entity that is registered in the Robocalling Mitigation Database, then the registrant is an "intermediate voice service provider" and the registrant's core obligation (regardless of where it is located geographically or in the call path) is to ensure that it takes traffic from that upstream entity only if the upstream entity

[3] *In the Matter of Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) - Knowledge of Customers by Entities with Access to Numbering Resources,* Comments of Verizon, CG Docket No. 17-59, WC Docket Nos. 17-97, 20-67, at 5-6 (filed May 15, 2020); *USTelecom Comments* at 3.

is registered in good standing in the Robocall Mitigation Database. In addition, intermediate service providers should be required to describe in their Robocall Mitigation Database certifications the steps they take to know the identities of the upstream entities from which they take traffic and to monitor those entities.

- End User Relationships. If the registrant's relationship is with an upstream entity—of any type or nature—that is not registered in the Robocall Mitigation Database, that upstream entity must be considered an "end user" by the registrant, so the registrant is an "originating voice service provider" that must take appropriate measures to ensure (under the existing rules applying to originating voice service providers) that the upstream entity's calls are not illegal.

The Commission's evaluation of an originating provider's robocall mitigation program (for calling parties) should differ from its evaluation of an intermediate provider's robocall mitigation program (for upstream service providers). An originating provider is in a stronger position to directly monitor the calling party to ensure it does not make illegal robocalls, whereas even the strongest robocall mitigation program by intermediate providers cannot be completely effective. The Commission should thus – at least until scalable, bright-line know-your-customer and due diligence tools become widely available – primarily focus its enforcement resources on an intermediate service provider's obligation to ensure the service provider upstream from it is registered and in good standing in the Robocall Mitigation Database.

B. Every Service Provider Handling Traffic With U.S. Telephone Numbers Should Be Required to Certify it Only Takes Traffic from Other Registered Service Providers and Describe its Robocall Mitigation Plan.

As USTelecom explains, the Commission should require every provider that registers with the Robocall Mitigation Database to certify to specific anti-robocall measures.[4] Every voice service provider should be required to ensure that it takes traffic only from other service providers that are in the Robocall Mitigation Database or from end users (in which case it

[4] *USTelecom Comments* at 4.

certifies that it ensures those end users are not making illegal calls). That is the only way to create a "chain of trust" from the caller, through registered Robocall Mitigation Database voice service providers and to the terminating voice provider.

While ensuring that all intermediate Robocall Mitigation Database registrants take traffic only from other Robocall Mitigation Database registrants is a crucial step, it is not by itself enough. The Commission should also require intermediate service provider registrants to describe with particularity the processes they follow to know the identities of the upstream service providers they accept traffic from and to monitor those service providers for illegal robocall traffic.

Verizon's industry-leading commitment to know-your-customer and traffic monitoring for upstream service providers belies the claim that meaningful robocall mitigation cannot occur at the intermediate provider level.[5] Despite the fact that Verizon almost always is substantially removed – by multiple service providers in the call path – from the complicit upstream voice service providers that directly accept traffic from illegal robocallers, Verizon estimates that its wholesale robocall mitigation program has removed more than *fourteen billion* illegal robocalls from our networks. Our provider rating methodology continuously measures wholesaler and direct peer calling patterns over time and considers factors such as call duration, percentage of calls declined by the recipient, number of calls made using invalid numbers, calls originating from industry or government identified problematic providers, and illegal calls made to our expansive honeypot. Verizon actively monitors these metrics, allowing us to identify and focus our dedicated team of data scientists and attorneys on those upstream service providers that pass us the highest volumes of unwanted traffic. If an upstream provider identified as consistently

[5] *See, e.g.*, Comments of T-Mobile USA at 4; Comments of INCOMPAS at 7.

sending us illegal traffic is unwilling to materially improve its traffic patterns, Verizon will discontinue the relationship. Indeed, Verizon has ceased accepting traffic from dozens of upstream service providers that have failed to maintain adequate anti-robocall hygiene – both ones that have failed to achieve meaningful improvement in their know-your-customer ratings and for voice service providers unwilling to participate in traceback in good faith.[6]

C. Intermediate Service Providers Should Not Be Penalized for Illegal Traffic that Leaks Through Despite Reasonable Robocall Mitigation Efforts Until There Are Industry Best Practices to Which They Can Certify.

The Commission should calibrate its enforcement activities to acknowledge that in the current environment, where large volumes of international traffic flow over multiple service provider providers via least-cost routing arrangements, it is impossible for any intermediate provider to consistently stop all illegal traffic. Its enforcement efforts in the short run should focus on intermediate providers that are shown to consistently accept illegal traffic despite having certified to having robocall mitigation processes in place, and on ones that improperly accept traffic from unregistered service providers.

Although Verizon has demonstrated that know-your-customer and traffic monitoring can have tangible benefits when applied at intermediate provider interfaces, unfortunately the robocall problem persists on Verizon's networks because the same service providers with which Verizon has declined to do business still frequently arise in tracebacks as they find other service

---

[6] In addition to leading the industry on know-your-customer and traffic monitoring, Verizon unilaterally pushed traceback participation throughout a substantial portion of the voice communications ecosystem at a time when traceback was not required by the Commission's rules and many providers refused to participate. Several years ago, Verizon began requiring its wholesale customers to contractually agree to participate in traceback themselves and also to incorporate traceback amendments in *their* contracts with upstream providers. Those customers' traceback amendments similarly required that *their* customers sign the same traceback amendment. Verizon ceased doing business with multiple providers that failed to sign the amendment.

providers willing to accept their traffic. That same pattern would thwart the Commission's anti-robocalling efforts if the Commission were to impose monitoring and know-your-customer only on a subset of service providers, such as only on "gateway" providers as proposed in the FNPRM: bad actors would simply intermediate other service providers between themselves and the gateway provider, making it impossible for the gateway provider to identify and consistently stop the illegal traffic. It is thus crucial that the Commission require *all* providers in the call path for calls carrying U.S. calling party numbers to register in the know-your-customer and to certify that they have robocall mitigation in place.

As a longer-run policy, the Commission should incent the development of industry robocall mitigation best practices that can be readily implemented and certified to by all intermediate service providers in the call path.

D. The Commission Should Consider Incenting the Use of Private Sector Reputation Monitoring Services.

While it would be good policy to require all U.S.-based intermediate service providers over which the Commission has jurisdiction to certify that they have monitoring programs in place and to describe those programs in particularity, the Commission should recognize that such programs will not solve the robocall problem by themselves. Leaving the specifics of due diligence and monitoring to each individual registrant will prompt a myriad of efforts ranging from Verizon's best-in-class and monitoring activities to some service providers who will fail to even follow the policies that they describe in their know-your-customer filings. And many foreign intermediate providers, which often have a limited understanding of the U.S. regulatory regime, are unlikely to implement effective robocall mitigation programs absent bright-line guidance from the Commission.

To some extent the Commission can address those challenges by focusing its Robocall Mitigation Database auditing efforts on companies who – based on traceback results – are found to have materially deficient robocall mitigation programs. But a more sustainable approach to addressing this challenge may be to encourage – and incentivize – the emergence of private sector-led initiatives to establish reputation scores for service providers. Ideally, third party vetting services would emerge that service providers can routinely rely on for reputation monitoring, and potentially for creating routing tables of trusted companies over which international calls call can safely flow.

Verizon and others routinely use a variety of third party reputation monitoring and risk management services to help efficiently evaluate vendors and partners in the U.S. and in international markets, such as Dun & Bradstreet, NAVEX Global, Rapid Ratings, Dow Jones, and RiskRecon. The Commission should consider encouraging the emergence of reputation monitoring services that could be relied on by U.S. and foreign carrier registrants in the Robocall Mitigation Database to satisfy their robocall mitigation obligations by confirming reliance on an acceptable monitoring service meets those obligations. An adequate service provider reputation monitoring service would likely, for example: take into account the extent to which ITG tracebacks have passed through that entity (taking into account its volume of traffic); evaluate the service provider's governance structure and the identities of its owners and officers (including by doing proprietary and public Internet research on them and sending them standardized questionnaires) to ensure that a service provider removed from the Robocall Mitigation Database has not simply reconstituted itself under a different corporate name; and consider whether the service provider is effectively regulated by its home country's telecommunications regulator.

By incenting the emergence of such reputation monitoring services, collaborating with other like-minded regulators on the criteria for and use of such services, and endorsing ones found to be acceptable for Robocall Mitigation Database purposes, the Commission can help create the foundation for an international ecosystem in which all service providers in the call path are themselves trustworthy and are only taking traffic from others that are trustworthy. The goal should be to ensure that all calls can be routed over such trusted paths.

II. THE COMMISSION SHOULD COORDINATE WITH FOREIGN REGULATORS AND SERVICE PROVIDERS TO MANAGE ITS POLICIES' IMPACT ON GLOBAL TELECOMMUNICATIONS

While the Commission should not shy away from extending globally its anti-robocall regime, it should acknowledge and manage the potentially profound impact that doing so may have on existing international traffic flows. Whether the Commission chooses to follow USTelecom's proposal to extend the Robocall Mitigation Database regime internationally or to go forward with a version of the FNPRM's proposals, it may cause a substantial restructuring of the existing global telecommunications industry by requiring service providers to modify existing route structures and eliminate certain inter-carrier relationships. The Commission should thus actively consult and coordinate with foreign regulators prior to putting the new rules in place, and should conduct outreach and education to foreign service providers so that the implications of the new U.S. policy are well understood.

The Commission is not alone among global regulators in taking action to address the robocall problem. Regulators in Canada, the U.K., France, Germany, Australia, Singapore, and other countries around the world are searching for the right policies to protect their consumers against illegal robocalls and should look to the Commission for collaboration and best practices. The Commission should coordinate with like-minded foreign counterparts to explore ways to

address the problem collectively, including by potentially harmonizing policies, avoiding burdensome regulations that could hinder legitimate enterprise customers use cases, and encouraging service provider best practices such as the use of reputation monitoring services.

The Commission also should reach out to foreign service providers so that they understand the regime it is putting in place and have clear guidance on how to comply. That could partially take place as part of the Commission's coordination with foreign regulators, but also should include issuing press releases and public notices specifically directed to the foreign service provider community.

Finally, the Commission should design its anti-robocall regime with sufficient flexibility to account for the fact that some foreign governments and their service providers may not be in a cooperative posture. For example, U.S. consumers benefit from the ability to roam on foreign providers in virtually every corner of the world, including in places where foreign roaming providers may decline to register in the Robocall Mitigation Database for geopolitical or other reasons. Consistent with iBASIS's comments, the Commission should design its chain of trust rules to permit Robocall Mitigation Database registrants to accept roaming traffic (which is unlikely to include illegal robocalls) in appropriate circumstances even if those foreign providers are not registered.[7] And at least until bright-line best practices are in place for service providers to follow, the Commission should consider focusing its Robocall Mitigation Database certification requirements on service providers subject to its direct jurisdiction.

[7] *See* iBASIS Comments at 4-5.

III. THE COMMISSION SHOULD AVOID POLICIES THAT WILL NOT BENEFIT CONSUMERS

A. Attempting to Impose Special Obligations Solely on a New Class of "Gateway" Providers Would Leave Insecure Links in the Call Path.

USTelecom's proposal to impose meaningful responsibilities onto every service provider in the call path is better than the proposal to pick just one class of intermediate provider ("gateway" providers) and impose on them the burden of stopping all illegal foreign-originate traffic.[8] Placing the burden of robocall mitigation exclusively on "gateways" will not benefit consumers because many gateway providers will be too far removed from the originating service providers to effectively identify and stop illegal traffic and because foreign bad actors will find ways to bypass service providers that self-identify as "gateways."

First, as discussed in Section I.C above, imposing obligations on just a subset of intermediate providers ("gateway providers") would leave a major gap in the Commission's anti-robocall framework. As multiple commenters explain, the gateway provider will often be unable to reliably identify and stop illegal robocalls because it will be too far removed from the origination point.[9] So while it is appropriate for the Commission to look to address the foreign-originated robocall problem by protecting the edges of the PSTN, foisting obligations only on gateways, without creating a "chain of trust" throughout the call path, will not benefit consumers.

Second, attempting to define "gateway provider" is hard, and the definitional ambiguity would lead to opportunities for gamesmanship. As USTelecom explains, based on its experience with tracebacks, it is often hard to determine whether a service provider is "foreign" or

---

[8] *FNPRM* Section III.D.

[9] *See,* e.g., iBASIS Comments at 3; CTIA Comments at 13; Comcast Comments at 9.

"domestic," and many purportedly "domestic" companies have little or no physical presence in the United States.[10] Many providers that ITG classifies as "gateway" can pursue "fly-by-night" strategies whereby they can disappear and subsequently reconstitute themselves as new entities.[11] According to USTelecom, these challenges "obfuscate which provider – whether the gateway provider or the provider one or two hop downstream – is most responsible and can best be held accountable by the Commission…."[12] If the Commission's rules fail to address the entire chain of intermediate service providers, these ambiguities will present opportunities for bad actors to effectively bypass the gateway provider regime.

B. The Purported Benefits of Requiring Intermediate Providers to "Authenticate" Calls with STIR/SHAKEN Are Illusory and Can Be Better Achieved With Other Tools.

The Commission should not adopt its proposal to require "gateway" service providers (or any intermediate voice service providers) to add STIR/SHAKEN signatures to unsigned calls they receive.[13] That proposed mandate's purported benefits are questionable at best and its policy goals can be better achieved – with less cost and risk – with other policy tools.

1. "C" Attestations Do Nothing to "Authenticate" Calls and Can Actually Confuse Some Analytics Engines and Blocking Tools.

The first rationale for the proposal to require "gateway" providers to "authenticate" unsigned calls with STIR/SHAKEN is that it will facilitate "analytics" and "blocking."[14] As a starting point, the term "authentication" does not describe the proposal to require "gateway"

---

[10] *USTelecom Comments* at 7-8.

[11] *Id.*

[12] *Id.* at 8.

[13] *FNPRM* at para. 38 *et seq*.

[14] *FNPRM* at para. 39.

providers (or any other intermediate service providers) to add STIR/SHAKEN signatures to unsigned calls they receive. That would generally result in those service providers placing "C" level ("gateway") attestations on calls they receive because in most instances an intermediate provider does not have sufficient knowledge of the calling party to be able to attest either to the calling party's identity or to whether it is using an authorized number.[15]

As Verizon and others warned prior to the Commission's initial STIR/SHAKEN mandate, an intermediate service provider STIR/SHAKEN mandate would not materially benefit consumers in the form of better blocking or analytics because "C" attestations are *just* as likely to be attached to unwanted, illegal, and even fraudulent robocalls as they are to be attached to wanted calls.[16] The data since the STIR/SHAKEN went into effect on a large scale in July 2021 prove that out. Verizon's analysis of calls with "C" attestations from a variety of service providers, including from ones supporting the proposed gateway provider STIR/SHAKEN mandate, indicates that such calls cover the full spectrum from affirmatively wanted calls to ones that have invalid telephone numbers to ones that appear to be patently fraudulent.

At best, some analytics engines might benefit slightly from the ability to ingest data about the attestation level and the identity of the service provider. To the extent an analytics engine is configured to see the entire STIR/SHAKEN header, it would be able to consider those data points – along with other relevant data such as the calling party number and the call patterns – in order to *potentially* make a somewhat better overall assessment about how to treat the call. Theoretically, for example, an analytics engine may choose to dis calls arriving with a particular

---

[15] *See, e.g.*, CTIA Comments at 14-15; iBasis Comments at 5; *USTelecom Comments* at 11; i3forum Comments at 5; iconectiv Comments at 3.

[16] *In the Matter of Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a), Knowledge of Customers by Entities with Access to Numbering Resources*, Verizon Reply Comments, WC Docket Nos. 17-97, 20-67, at 8-11 (filed May 29, 2020).

service provider's "C" attestations after detecting a pattern whereby virtually all of "C" attestations from that service provider are attached to unwanted calls. But those additional data points would not substantially improve the consumer's blocking experience because traffic patterns can change suddenly, so the analytics engine would not be able to give that data point substantial weight in the overall holistic scoring determination.

Many other analytics engines do *not* ingest the entire STIR/SHAKEN header and thus cannot evaluate the more granular data associated with which service provider has signed which level of attestation. That is why the STIR/SHAKEN standard converts the result of verification into a "verstat" and shares that value with the called party's device or analytics engine. Because the verstat is binary (either the call passes validation or it fails), the analytics engine cannot consider the attestation level. For analytics engines that rely on the verstat, a C attestation mandate will either not be useful or create confusion. It will have zero usefulness if the terminating service provider – to avoid the confusion associated with C attestations associated with spoofed and often illegal traffic – follows the IP-NNI best practice of not delivering a "passed" verstat if the call is signed with a "C."[17] And it will create confusion for the analytics engine if the service provider delivers a verstat indicating that each of the "C" attestation calls "passed validation" because the analytics engine cannot tell the difference between "C" verstats (on calls that in many cases will be spoofed and illegal) and verstats associated with "A" attestations (which are not spoofed and often likely to be wanted).

In sum, for some analytics engines, mandating STIR/SHAKEN at gateways might add a data point (which would be weighted lightly) to slightly improve blocking or labeling decisions;

---

[17] *See* ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000074.v002, ATIS and SIP Forum (2020), https://access.atis.org/apps/group_public/document.php?document_id=52807.

for others it would have no utility at all; and for others it would create confusion and potential harm in the form of causing consumers to trust calls with "C" attestations that should not be trusted.

2. The Purported Traceback Benefits of an Intermediate Carrier "C" Attestation Mandate Are Questionable and Could Be Better Achieved By Requiring More Robust Participation in the Industry Traceback Group.

The other purported benefit of a gateway provider STIR/SHAKEN mandate is that it may facilitate traceback.[18] As the industry leader in both providing ITG with automated traceback responses and using honeypots to efficiently source traceback candidates for the ITG, Verizon can attest that a stronger industry-wide commitment to double down on the existing traceback systems and processes would do more to protect consumers than would attempting to use C attestation data to initiate or conduct tracebacks.

As a starting point, the Commission-designated ITG has already become highly adept at tracing back illegal robocalls. ITG has made traceback efficient by, among other things, creating a secure online portal that keeps track of tracebacks and prompting each service provider in the call path to input information about where it received the suspicious call. There is no record evidence that the existing traceback processes are deficient and in need of bolstering via the proposed "C" attestation mandate (or via any other policy).[19]

---

[18] *FNPRM* at para. 39.

[19] *In the Matter of Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a), Knowledge of Customers by Entities with Access to Numbering Resources*, Comments of USTelecom, WC Docket Nos. 17-97, 20-67, at 12-13 (filed May 15, 2020). The extraordinary strides industry has made just in the past few years advancing traceback techniques was not foreseeable when the standards bodies were developing the "C" attestation as a potential tool to aid in traceback. So the fact that the "C" attestation was contemplated at that time as potentially useful for traceback purposes is irrelevant to the Commission's policy determinations today.

If, however, the Commission's policy goal is the get the traceback process into a higher gear, by far the best way to do that is to require or encourage service providers to participate more robustly in the ITG. Whereas some service provider balk at a proposed traceback turnaround time of 24 hours,[20] Verizon has put in place automated systems that on average return traceback results to the ITG in less than a minute.[21] The IT systems work that Verizon undertook to securely automate its participation in traceback was trivial compared to the costs and complexities that would be involved in implementing STIR/SHAKEN in order to enhance tracebacks.

3. A "C" Attestation Mandate Would Take Years to Implement and Divert Resources from Initiatives that Can Actually Benefit Consumers.

For Verizon, complying with a STIR/SHAKEN mandate on platforms providing intermediate voice services would present burdens and timelines similar to those associated with the Commission's initial STIR/SHAKEN mandate. Verizon strongly supported that initial mandate because it was aimed at addressing the spoofing problem by requiring originating service providers to authenticate traffic. But this new proposed mandate (as discussed above) does not drive the ecosystem towards a similar outcome and therefore requires a different cost-benefit analysis.

The resources Verizon would need to devote to a new STIR/SHAKEN would involve millions of dollars in payments to vendors for modifying systems with new software, but that is a minor portion of the overall burdens such a mandate would create. Verizon would need to

---

[20] *See, e.g.*, Incompas Comments at 9.

[21] Currently about five percent of Verizon's tracebacks still require manual research. If the Commission imposes more aggressive traceback obligations, it should impose a "best efforts" standard that accounts for the fact that service providers with complex networks (including non-IP ones) occasionally face challenges with some tracebacks.

dedicate a substantial amount of specialized internal resources from multiple functional areas to such a project, diverting those resources from other projects that promise more meaningful consumer protection benefits. Given that much of the relevant infrastructure is end-of-life, the project management work required to implement a "C" attestation mandate would involve first devoting tens of thousands of hours to replacing the existing infrastructure, then implementing STIR/SHAKEN on the upgraded infrastructure, and then migrating customers to the upgraded infrastructure.[22] Those steps need to proceed serially and would take multiple years and cost tens of millions of dollars..[23]

While that level of cost and burden might be reasonable to impose if the mandate were likely to result in tangible consumer benefits, here consumer benefits are unlikely and other more reasonable options are available to achieve the proposed mandate's goals. The proposed C attestation mandate would likely divert industry resources away from other complex projects that are currently underway and that do promise tangible consumer benefits. For example, Verizon and other industry leaders are actively developing, deploying, and standardizing new techniques for efficiently exchanging traffic in IP format (which will increase the exchange of STIR/SHAKEN traffic) and for providing consumers with authenticated logos and other information about legitimate calling parties.

[22] Also, adding STIR/SHAKEN to billions more calls would consume bandwidth, so service providers would need to expand capacity to manage the mandate.

[23] Just the migration process for moving existing customers from the legacy infrastructure to the upgraded infrastructure would take years to complete and millions of dollars based on conservative estimates of roughly four person-hours of work per trunk.

C. The Commission Should Reject the Fiction that Implementing STIR/SHAKEN Obviates the Need for a Service Provider to Mitigate Robocalls.

The Commission should not permit any voice service provider to simply certify it has implemented STIR/SHAKEN in place of certifying that it has a robocall mitigation program. The ability to certify to STIR/SHAKEN in place of undertaking robocall mitigation is the *status quo* with respect to originating service providers,[24] and some parties assert that STIR/SHAKEN implementation should also be sufficient for intermediate provider to implement in place of robocall mitigation.[25] While an important tool for restoring trust in telephone calls, STIR/SHAKEN does not by itself stop illegal robocalls, so excusing service providers from helping stop illegal robocalls if they implement STIR/SHAKEN harms consumers.

With respect to originating service providers, Verizon supports USTelecom's proposal to require them to certify to appropriate robocall mitigation program even if they certify to STIR/SHAKEN.[26] The industry has recently experienced a troublesome increase in non-spoofed illegal robocalls, including the car warranty scam that has affected tens of millions of consumers.[27] Signing STIR/SHAKEN to an illegal robocall can actually *increase* the risk of fraud because some service providers may present the call to the consumer in ways that may imply it is a wanted call, such as by placing a green checkmark on the consumer's device.

As the Commission extends the Robocall Mitigation Database requirement to intermediate providers, it is even more important that it reject requests to permit such providers

---

[24] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1935-1941 (2020).

[25] *See, e.g.,* T-Mobile Comments at 9; Twilio Comments at 3; Incompas Comments at 9.

[26] *See USTelecom Comments* at 4.

[27] Robocallers obtain large pools of numbers and cycle through them.

to avoid robocall mitigation simply by signing calls with STIR/SHAKEN. An intermediate service provider that places a "C" attestation on an unsigned call originated somewhere upstream from it knows nothing about the calling party, and so is neither addressing the spoofing problem nor ensuring that the call is not illegal. Absolving such intermediate service providers of robocall mitigation obligations would result in more illegal traffic traversing the PSTN and harming consumers.

Indeed, the worst possible outcome for U.S. consumers would be T-Mobile's proposal to mandate STIR/SHAKEN for "gateway" providers but to do nothing to require them – or any other intermediate service providers in the call path – to take any action to disrupt the chain of illegal robocalls destined for consumers.[28] Such a policy would create substantial burdens for those T-Mobile competitors that have substantial intermediate service provider operations without doing anything to stop the flood of illegal robocalls that reach U.S. consumers.

CONCLUSION

For the reasons set forth above, the Commission should focus on strengthening and internationalizing its existing Robocall Mitigation Database rules, and on aggressively enforcing those rules. It should not experiment with layering on top of its existing regime new regulatory innovations that are unlikely to benefit consumers and instead are likely to result in uncertainty and unintended consequences.

[28] *See* T-Mobile Comments at 3 (asserting incorrectly that the gateway STIR/SHAKEN mandate would "result in fewer spoofed calls") and 7-9 (arguing the Commission should refrain from imposing any know-your-customer or robocall mitigation obligation on intermediate providers).

Respectfully submitted,

/s/ Christopher D. Oatway

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 500 West
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon and Verizon Wireless

January 10, 2022