

**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)	WC Docket No. 17-97

COMMENTS OF I3FORUM

Steven A. Augustino
Debra McGuire Mercer
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8400
saugustino@kelleydrye.com

Counsel for i3forum

December 10, 2021

SUMMARY

i3forum was established in 2007 as an organization to bring together various participants in the international telecommunications industry, including telecommunications carriers that provide international wholesale services, voice and text messaging termination, Internet protocol transit, roaming services and data transport. The membership also includes other service providers and vendors that support international telecommunications, such as companies that provide software, cloud communications, Voice over IP, and network equipment. The members of i3forum collaborate to define best practices; promote technological, commercial and operational innovation; and encourage competition. Many of the members are leading industry players that have a wealth of experience in delivering reliable and high-quality telecommunications services throughout the world. The collective scope and depth of experience i3forum's members have in the international telecommunications marketplace enables i3forum to provide the Commission with a detailed and accurate picture of how the industry works and an informed perspective as to whether certain proposals can be successfully implemented by gateway providers.

i3forum supports the Commission's goal of "eliminating the scourge of robocalling" and agrees that gateway providers, which are a point of entry for foreign calls terminating in the United States, should "lend a hand in the fight against illegal robocalls originating abroad."¹ However, as explained in these comments, gateway providers are at the end of a long and unpredictable chain of carriers that play a role in transporting a foreign-originated call to a recipient in the United States. As such, gateway providers often are several steps removed from the call originator and lack the information necessary to successfully mitigate foreign-originated

¹ Further Notice, ¶ 1.

robocalling using the procedures proposed in the Further Notice. In particular, proposals that require a gateway provider to know the identity of the call originator or to verify the call originator's authorization to use a U.S. number are unrealistic given the nature of most international calling. Thus, while gateway providers are committed to aiding the Commission in its long-standing battle against illegal robocalls, the Commission should be mindful of gateway providers' limited ability meet certain proposed obligations. The Commission therefore should consider alternative robocall mitigation strategies, such as requiring gateway providers to impose an additional charge for receiving calls that meet certain parameters associated with illegal robocalling. The charges would eventually flow back to the fraudulent call initiator, thereby discouraging continued illegal conduct. In addition, i3forum urges the Commission to focus on providing gateway providers with additional tools to identify potentially problematic traffic (rather than asking providers to identify "bad actor" customers) and to provide incentives for gateway providers to use these tools.

TABLE OF CONTENTS

	Page
SUMMARY	i
I. INTRODUCTION AND SUMMARY	2
II. THE COMMISSION SHOULD PERMIT, BUT NOT REQUIRE, GATEWAY PROVIDERS TO AUTHENTICATE CALLER ID INFORMATION USING STIR/SHAKEN.....	3
III. THE COMMISSION SHOULD ENCOURAGE REASONABLE ROBOCALL MITIGATION OBLIGATIONS BY PARTIES THAT CAN SUCCESSFULLY MEET THEM	6
IV. THE COMMISSION SHOULD NOT IMPOSE ‘KNOW YOUR CUSTOMER’ REQUIREMENTS ON GATEWAY PROVIDERS	9
CONCLUSION.....	12

**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)	WC Docket No. 17-97

COMMENTS OF I3FORUM

i3forum, by and through its undersigned counsel, hereby submits its comments on the Federal Communications Commission’s (Commission’s) Further Notice² seeking comment on proposed rules that would place obligations on gateway providers to assist in combatting foreign-originated illegal robocalls. i3forum, an organization representing the interests of prominent stakeholders in the international telecommunications industry, fully supports the Commission’s continuing efforts to eliminate robocalling. As the Commission considers its next steps, i3forum requests that it take into account the complexity of the international telecommunications ecosystem and base its decisions on realistic expectations regarding the ability of gateway providers to meet the obligations proposed in the Further Notice. The FCC can help reduce the volume of illegal traffic coming into the U.S. by equipping gateway providers with additional tools to identify problematic traffic (rather than imposing unrealistic obligations to vet good/bad customers) and should create incentives for gateway providers to use the tools.

² See *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No., 17-59 and 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 (Oct. 1, 2021) (Further Notice).

I. INTRODUCTION AND SUMMARY

i3forum was established in 2007 as an organization to bring together various participants in the international telecommunications industry, including telecommunications carriers that provide international wholesale services, voice and text messaging termination, Internet protocol transit, roaming services and data transport. The membership also includes other service providers and vendors that support international telecommunications, such as companies that provide software, cloud communications, Voice over IP, and network equipment. The members of i3forum collaborate to define best practices; promote technological, commercial and operational innovation; and encourage competition. Many of the members are leading industry players that have a wealth of experience in delivering reliable and high-quality telecommunications services throughout the world. The collective scope and depth of experience i3forum's members have in the international telecommunications marketplace enables i3forum to provide the Commission with a detailed and accurate picture of how the industry works and an informed perspective as to whether certain proposals can be successfully implemented by gateway providers.

i3forum supports the Commission's goal of "eliminating the scourge of robocalling" and agrees that gateway providers, which are a point of entry for foreign calls terminating in the United States, should "lend a hand in the fight against illegal robocalls originating abroad."³ However, as explained in these comments, gateway providers are at the end of a long and unpredictable chain of carriers that play a role in transporting a foreign-originated call to a recipient in the United States. As such, gateway providers often are several steps removed from the call originator and lack the information necessary to successfully mitigate foreign-originated

³ Further Notice, ¶ 1.

robocalling using the procedures proposed in the Further Notice. In particular, proposals that require a gateway provider to know the identity of the call originator or to verify the call originator's authorization to use a U.S. number are unrealistic given the nature of most international calling. Thus, while gateway providers are committed to aiding the Commission in its long-standing battle against illegal robocalls, the Commission should be mindful of gateway providers' limited ability meet certain proposed obligations. The Commission therefore should consider alternative robocall mitigation strategies, such as requiring gateway providers to impose an additional charge for receiving calls that meet certain parameters associated with illegal robocalling. The charges would eventually flow back to the fraudulent call initiator, thereby discouraging continued illegal conduct. In addition, i3forum urges the Commission to focus on providing gateway providers with additional tools to identify potentially problematic traffic (rather than asking providers to identify "bad actor" customers) and to provide incentives for gateway providers to use these tools.

II. THE COMMISSION SHOULD PERMIT, BUT NOT REQUIRE, GATEWAY PROVIDERS TO AUTHENTICATE CALLER ID INFORMATION USING STIR/SHAKEN

The Commission proposes to require "gateway providers to authenticate caller ID information consistent with STIR/SHAKEN for SIP calls that are carrying a U.S. number in the caller ID field."⁴ i3forum recognizes the important role call authentication frameworks play in identifying calls that transmit false or misleading caller ID information (known as "spoofing"). Indeed, when a calling entity spoofs a large number of calls in a robocalling campaign, it magnifies the associated harms to subscribers to the spoofed number, recipients of the calls and terminating carriers. However, because gateway providers frequently lack access to the

⁴ Further Notice, ¶ 38.

information needed to authenticate caller ID information consistent with the STIR/SHAKEN framework, the Commission should not obligate gateway providers to comply with STIR/SHAKEN. Rather, the Commission should encourage and permit gateway providers to authenticate caller ID information using STIR/SHAKEN, when possible, and to accept alternative means of authentication, provided that they are based on reliable information.

The international telecommunications industry is comprised primarily of wholesale service providers. Numerous service providers are responsible for handling a call from origination to termination. Foreign-originated calls typically travel from the originating telecommunications carrier to one or more carriers in the foreign country before being transported internationally and eventually being handed off to a gateway provider in the United States. Moreover, even within the originating country, there is not one distinct call path that all calls from a particular number follow. Therefore, gateway providers, which are several steps removed from the call originator, rarely have the ability to discern the identity of the call originator or to evaluate whether the calling number is legitimate.

As the Commission is aware, STIR/SHAKEN standards allow for three attestation levels, each of which depends on how much information the authenticating provider has. Full or A-level attestation requires confirmation of the identity of the subscriber making the call and that the subscriber is using its associated telephone number; partial or B-level attestation requires confirmation of the identity of the subscriber, but not that the subscriber is using its associated telephone number; and gateway or C-level attestation requires confirmation that the authenticating provider is the point of entry to the IP network for a call that originated elsewhere and that the provider has no relationship to the call originator.

Gateway providers seldom have information necessary to confirm the identity of the call-originating subscriber in a foreign country or whether that subscriber is using its own telephone number or spoofing another subscriber's telephone number. Despite the Commission's assertion that gateway providers would not be limited to assigning a C-level attestation to all calls,⁵ gateway providers, in almost all situations, could only confirm that the provider is a gateway provider with no relationship to the call originator (i.e., a C-level attestation). This lowest level attestation under STIR/SHAKEN fails to provide any useful or meaningful assistance for blocking illegal robocalls. It would be wasteful and unfair to require gateway providers to invest their resources in attempting to comply with STIR/SHAKEN when the outcome does not facilitate the identification or elimination of illegal robocalls.⁶

Although i3forum opposes a requirement that gateway providers authenticate caller ID information using STIR/SHAKEN in all instances, it favors having the option using STIR/SHAKEN in situations in which it has access to information that would enable it to provide an A-level or B-level attestation. Indeed, the FCC's call authentication best practices encourage domestic providers to explore voluntary commercial arrangements with international providers that include terms and conditions that would give the gateway provider the tools, information, and confidence to trust the validity of the calling identity.⁷ This approach has promise to enable an A-level attestation, particularly if a gateway provider receives the call

⁵ *See id.* ¶ 44.

⁶ The Commission's proposal to limit the requirements for gateway providers only to calls that carry a U.S. number in the caller ID field does not solve this issue. *See id.* ¶ 36. Even if a gateway provider knows the originating telephone number, it still cannot determine the identity of the caller or, with current information, assess whether the caller is an authorized user of the telephone number.

⁷ *See Public Notice*, Wireline Competition Bureau Issues Call Authentication Best Practices, at 7, WC Dockets 17097 and 20-324, DA 20-1526 (Dec. 22, 2020).

directly from a trusted foreign carrier that originated the call. The Commission also should encourage development and adoption of methods to rely on a foreign country's caller ID authentication system as a means to assist in identifying the perpetrators of illegal robocalls.⁸ While the opportunities for reliance on these mechanisms are too limited to require attestation in all cases, they are useful in some instances, and the Commission should do its part to enable providers to use this tool in appropriate situations.

III. THE COMMISSION SHOULD ENCOURAGE REASONABLE ROBOCALL MITIGATION OBLIGATIONS BY PARTIES THAT CAN SUCCESSFULLY MEET THEM

Call Blocking

The Commission seeks comment on several proposals that would require gateway providers to block calls, ranging from blocking in response to a Commission notification about certain types of traffic to blocking based on use of reasonable analytics.⁹ Blocking calls is a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic. The risk of over-blocking must be minimized to prevent unintentional harm and serious consequences that can result if lawful calls relaying emergency or urgent information erroneously are blocked. Furthermore, blocking foreign-originated calls requires global synchronization among all service providers that have a role in transmitting a call. All relevant parties must agree on blocking processes and procedures for initiating call blocking and then for terminating it. To avoid the difficult, if not impossible, task of getting numerous international parties to agree on call blocking procedures, the Commission should not extend mandatory blocking requirements to gateway providers.

⁸ See ATIS, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)* (ATIS-1000087).

⁹ See generally Further Notice, ¶¶ 56-79.

In the Commission’s Call Blocking orders, it appropriately has been cautious in authorizing, but not requiring, blocking of traffic suspected to be illegal robocalls. In the *Third Report and Order* in the call blocking proceeding, the FCC adopted rules to encourage terminating providers to block illegal and unwanted calls before they reach the consumer.¹⁰ The FCC established two safe harbors from liability for providers, in order to encourage voice service providers to block calls in certain situations.¹¹ Such blocking is not mandatory for terminating providers, however.¹² There is no reason to mandate blocking for gateway providers, when such blocking is voluntary in the rest of the industry. Moreover, for the same reasons that terminating providers needed a safe harbor from liability in order to encourage blocking, if gateway providers are expected to block any calls, they too will need protection to ensure that they do not face liability for blocking – or failing to block – certain calls. Therefore, rather than making blocking mandatory, i3forum recommends that the FCC extend its safe harbors for blocking based on reasonable analytics and for network-based blocking to gateway providers.

Traceback

The Commission proposes that gateway providers respond to traceback requests from the Commission, civil and criminal law enforcement and the industry traceback consortium within 24 hours of receiving a request.¹³ i3forum agrees that traceback is an essential tool for

¹⁰ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking CG Docket No. 17-59, 35 FCC Rcd 7614 (2020) (*Third Report and Order*).

¹¹ *Third Report and Order*, ¶ 23. Subsequently, the FCC expanded the safe harbor for reasonable analytics to include network-based blocking with certain additional protections. *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221 (Dec. 2020).

¹² *See, e.g.*, 47 C.F.R. § 64.1200(k)(3) (“A terminating provider *may* block a voice call without liability ...”) (emphasis added).

¹³ *See* Further Notice, ¶¶ 52-53.

identifying the source of illegal calls. However, 24 hours is not sufficient time to conduct a thorough and accurate traceback analysis on international calls.¹⁴ Gateway providers need at least three days to complete traceback because they need to obtain information from several other carriers located in foreign countries. In addition, gateway providers may not have clear access to the information requested in a traceback inquiry due to privacy law and other restrictions imposed by the laws of foreign countries. Therefore, the Commission should also make clear that, in responding to a traceback request, gateway providers are not expected to provide information that is restricted from disclosure by foreign law.

Alternative Robocall Mitigation Strategy

The Commission also should consider an alternative mechanism for discouraging foreign-originated illegal calls that appear to be placed from a U.S. number. i3forum suggests that international carriers monitor traffic for suspicious call patterns identified by the FCC, such as high call volumes with short durations, and impose an additional charge for transporting those calls (even if the calls are not completed) on top of the regular per-minute charge. If the Commission required gateway providers to impose an additional charge for transporting calls that meet certain parameters associated with illegal robocalling, those types of charges would eventually flow back to the fraudulent call initiator. This alternative leverages existing contractual relationships among international telecommunications carriers. In addition, creating a cost for call attempts that share characteristics of illegal robocalls would significantly increase the overall cost of fraudulent activities. But such a surcharge should be mandatory; otherwise gateway providers may suffer competitive harm by call originators bypassing those providers

¹⁴ i3forum presumes that the ITG will be unable to compel information from foreign providers upstream from the gateway. Therefore, a response simply identifying the next carrier upstream in the call flow likely is not going to be helpful in combatting illegal robocalls. If the ITG wants more information than this, it must provide sufficient time for investigation.

with a surcharge for others that do not impose the surcharge. Widespread implementation across the entire industry is critical for such a surcharge to have its intended effect.

While it may take time for this surcharge framework to flow down through the international calling industry and become a real cost to fraudulent call originators, i3forum believes that the time and cost for this solution would be modest compared to developing and deploying new technology that would be needed to meet STIR/SHAKEN standards (and likely be ineffective at stemming illegal robocalling).

IV. THE COMMISSION SHOULD NOT IMPOSE ‘KNOW YOUR CUSTOMER’ REQUIREMENTS ON GATEWAY PROVIDERS

The Commission also seeks comment on several proposals to extend “know your customer” obligations to gateway providers.¹⁵ The Commission correctly notes that a gateway provider does not have a direct relationship with the call originator and thus may not have a “customer” to “know” in the ordinary sense of those terms.¹⁶ Nevertheless, the Commission proposes to require the gateway provider to “confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the call.”¹⁷ It further seeks comment on other contractual provisions it might require to ensure that its carrier customers validate the calling number.

The Commission should not mandate these additional obligations described in the Further Notice. As noted, gateway providers do not have a direct relationship with the call originator. It is not possible for a gateway provider to create a contractual relationship with the call originator, either. Not only is it virtually impossible for the gateway provider to identify the specific call

¹⁵ Further Notice, ¶¶ 80-90.

¹⁶ *Id.* ¶ 80.

¹⁷ *Id.* ¶ 81.

originator in order to create a contractual relationship, but the calls in question may follow different paths at different times, meaning that there will not be a one-to-one relationship between a call path and a call originator for which any such rubric could be applied. The gateway provider has no practical way of determining the call originator or of establishing a separate relationship with the call originators in question.

This problem is not solved by defining the gateway provider's carrier partner as the "customer" for these purposes. In most instances, international calls pass through multiple carriers before reaching a gateway provider, which means that the gateway provider's carrier customer likewise is several steps away from the call originator. Therefore, the gateway provider's partner, even if it were defined as the "customer" as the Commission suggests, would not have appreciably more information available to it to determine the call originator's authorization to use the U.S. number. In fact, none of the providers upstream from the gateway provider typically would have been the entity that assigned the U.S. number to a subscriber, so it is not clear that any upstream entity in an international call path could validate this key piece of information. The only entity that has this information is the owner of the U.S. numbering resources used, either because it assigned the number directly to the subscriber (such as in a mobile roaming situation) or it provided the numbering resources to a third party that makes the resources available to foreign customers (e.g., a call center). The Commission's proposals, however, would obligate entities other than this entity to validate the number – something that they simply could not do.

Rather than seeking to fit a square peg into a round hole, i3forum respectfully suggests that the Commission turn its attention to providing gateway providers with new tools to identify fraudulent or suspicious traffic. "Know your customer" in the gateway context should instead be

“know your traffic,” so to speak. This can happen effectively only if the FCC makes additional information available to the gateway provider.

- **Authorized foreign-origination numbers.** The Commission should explore ways in which U.S. carriers that assign numbering resources to subscribers can make available, in a secure, real-time manner, information about which numbers are authorized to be used outside the United States to originate numbers or, alternatively, which numbers are not authorized for foreign origination. If the Commission can make such information available, a gateway provider will more easily be able to determine if a given call is permitted to use a U.S. originating number.
- **Definition of “high volume of calls.”** The Commission’s proposals would only apply to the origination of a “high volume of calls.” It is necessary to identify what that term means so that gateway providers are able to identify the traffic to which any obligations apply. This definition also is needed to identify ordinary, lawful traffic for which the robocall concern does not apply, such as international roaming traffic, geonumbering usage and other non-automated traffic.
- **Sharing of information available to regulators and enforcers.** The FCC should also explore ways that it can make available, in a secure, real-time manner, information regarding traffic that the FCC, other federal enforcement authorities, state AGs or the Industry Traceback Group have identified as potentially fraudulent. Where possible, country of origin and/or U.S. numbers used should be conveyed to gateway providers to inform their call routing decisions. Information about suspicious actors or suspicious numbers would be helpful to gateway providers in identifying traffic that should be blocked or at least requires additional review.

- **Sharing of suspicious patterns and suspicious practices.** The Commission’s reviews can glean additional insight into the types of traffic that are more (or less) likely to involve illegal robocalling. The Commission should explore (possibly through the Call Authentication Trust Anchor Working Group of the North American Numbering Council) ways that it can share information about suspicious usage or call patterns that providers should be on the lookout for. Indicators might include information such as high percentages of failed calls, high percentages of low-call duration or a disproportionate number of call attempts in a particular time period. These suspicious call indicators would be similar to the FCC’s best practices for service providers on call authentication, etc. They could serve as examples to enable a gateway provider to develop its own internal indicators for problematic traffic and help inform the anti-robocall effort in general.

This list is illustrative of the kinds of tools that the Commission might make available to more effectively mitigate illegal foreign-originated robocalls. No single mandate is likely to work in all instances, nor should gateway providers be left on their own to identify illegal traffic with little or no actionable information. Instead, in pursuing the goal of stopping illegal foreign-originated calls before they reach consumers, the Commission should ask “how can we help?” and make that assistance available to gateway providers.

CONCLUSION

Gateway providers share the FCC’s goal of preventing illegal robocalls from traversing their networks. The FCC can help reduce the volume of illegal traffic coming into the U.S. by implementing alternative robocall mitigation strategies, such as requiring gateway providers to impose additional charges for receiving calls that meet certain parameters associated with illegal robocalling or equipping gateway providers with additional tools to identify problematic traffic,

rather than imposing obligations that are impractical to implement in the international calling industry today. i3forum requests the Commission to adopt rules consistent with the positions described in these comments in order to provide those tools.

Respectfully submitted,

A handwritten signature in black ink that reads "Steven A. Augustino". The signature is fluid and cursive, with the first name "Steven" written in a larger, more prominent script than the last name "Augustino".

Steven A. Augustino
Debra McGuire Mercer

KELLEY DRYE & WARREN LLP
3050 K Street NW, Suite 400
Washington, D.C. 20007
(202) 342-8400
saugustino@kelleydrye.com

Counsel for i3forum

December 10, 2021