

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
Advanced Methods to Target and Eliminate) CG Docket No. 17-59
Unlawful Robocalls)
)
)
)
)
)

Comments of the Cloud Communications Alliance

Joe Marion
President
Cloud Communications Alliance
131 NW 1st Avenue
Delray Beach, FL, USA 33444
(561) 232-3891

August 31, 2020

TABLE OF CONTENTS

	Page
I. SUMMARY.....	1
II. EFFECTIVE REDRESS REQUIRES REAL-TIME NOTIFICATION OF BLOCKING	2
A. MANY VOICE PROVIDERS BLOCKING CALLS ALREADY OFFER INTERCEPT MESSAGES OR OTHER FORMS OF NOTIFICATION.....	3
B. THE IETF HAS PROPOSED A SAFE AND INTEROPERABLE SIP RESPONSE CODE.....	5
C. NOTIFICATIONS SHOULD BE STANDARDIZED, OFFERED AT NO COST, AND BE A CONDITION OF UTILIZING A SAFE HARBOR.....	7
D. NOTIFICATION AND REDRESS ARE NECESSARY TO AVOID UNREASONABLE BLOCKING BASED ON MISSING OR INACCURATE STIR/SHAKEN INFORMATION	7
E. REDRESS MECHANISMS, INCLUDING NOTIFICATION, SHOULD BE REQUIRED WHEN ADVERSELY LABELLING CALLS	8
III. PROVIDERS SHOULD BE REQUIRED TO RESPOND TO APPROPRIATE TRACEBACK REQUESTS.....	10
IV. THE ALLIANCE SUPPORTS ADOPTION OF MITIGATION MEASURES.....	13
V. THE COMMISSION SHOULD ACCOMMODATE USE OF THIRD PARTIES IN ACQUIRING NEW CUSTOMERS.....	14
VI. CONCLUSION	15

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
Advanced Methods to Target and Eliminate) CG Docket No. 17-59
Unlawful Robocalls)
)
)
)
)
)

Comments of the Cloud Communications Alliance

Pursuant to the Public Notice in the above-captioned proceeding, the Cloud Communications Alliance (the “Alliance”) submits these comments in response to the Fourth Further Notice of Proposed Rulemaking (“Notice”).¹

I. Summary

The Alliance respectfully urges the Federal Communications Commission (“Commission”) to require blocking entities to notify voice service providers in real time that they are blocking their calls and to make this notification requirement a condition of any blocking safe harbor. Notification is required to fully implement the relevant provisions of the

¹ *Consumer and Governmental Affairs Bureau Announces Comment Dates for Call Blocking Fourth Further Notice of Proposed Rulemaking*, Public Notice, CG Docket No. 17-97, DA 20-817 (Rel. July 31, 2020). *Advanced Methods to Target Unlawful Robocalls*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, CG Docket No. 19-59, FCC 20-96 (rel. July 17, 2020) (“Order” or “Notice”).

TRACED Act.² The Commission should also extend redress mechanisms, including notification, to mislabeled calls.

The Alliance concurs with the Commission's proposals to require voice service providers to respond to traceback requests and to take effective mitigation steps when acquiring new customers or upon being notified by the Commission that they are carrying illegal traffic. These obligations, however, must be implemented in a fair and reasonable manner that informs providers of their obligations without imposing undue burdens. For example, traceback requests should be sent to appropriate personnel and only the Commission, law enforcement agencies or the Traceback Consortium should send such requests. Moreover, in developing rules regarding due diligence when acquiring new customers, the Commission should accommodate the prevalent industry practice of using third parties to acquire new customers.

II. Effective Redress Requires Real-Time Notification of Blocking

The Alliance applauds the Commission's adoption of redress mechanisms that require voice service providers that block calls to designate a single point of contact to report erroneous blocking, require investigation and resolution of a good faith claim of erroneous blocking within a reasonable period of time, and require the prompt removal of blocks upon receiving a credible claim of erroneous blocking, all at no cost to the originating provider or its calling customers.³

The Alliance disagrees, however, with the Commission's tentative conclusion that these requirements are sufficient to fully implement the directives in the TRACED Act to provide effective and transparent redress for callers whose legitimate calls are erroneously blocked.⁴ An effective and transparent redress mechanism must also include real-time notification by the

² Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019) (TRACED Act).

³ Order at ¶¶ 54-55.

⁴ *See, e.g.*, Notice at ¶¶ 82, 91.

blocking party that the call is being blocked and by whom. The Alliance and numerous others have demonstrated the need for such a requirement to ensure that erroneous blocks can be addressed in a timely manner.⁵

The Commission has raised concerns that notifying legitimate callers that their calls are being erroneously blocked might alert bad actors that they need to change their calling plans, and it has asked whether notifications are feasible in both TDM and IP networks. These concerns appear somewhat misplaced in light of the Commission’s prior express encouragement that voice service providers that block calls “develop a mechanism for notifying callers that their calls have been blocked.”⁶ The Commission noted that “industry has been active in developing solutions that allow callers to communicate with voice service providers and analytics companies to identify themselves and share their call patterns that might otherwise seem to indicate illegal call activity.”⁷ As discussed below, a number of voice service providers already provide some form of notification, many using intercept technology that has been available for years.

A. Many Voice Providers Blocking Calls Already Offer Intercept Messages or Other Forms of Notification

The Commission’s recently released report on the status of blocking confirms that many voice providers already provide real-time notification, at least for some of their blocking efforts, often using a long-available feature called Anonymous Call Rejection.⁸ AT&T states that “[w]hen a blocked line calls a Mobility, U-verse, Prepaid, or Cricket customer, the calling party

⁵ See, e.g., Reply Comments of Cloud Communications Alliance, CG Docket No. 17-59, WC Docket No. 17-97 at 5, n.19 (filed August 18, 2019) (citing comments).

⁶ *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Declaratory Ruling and Third Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4888-89 ¶ 38 (2019) (“2019 Blocking Order”)

⁷ *Id.*

⁸ Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking, CG Docket No. 17-59, Consumer and Governmental Affairs Bureau, June 2020. (“Call Blocking Report”) <https://docs.fcc.gov/public/attachments/DOC-365152A1.pdf>

will hear an intercept announcement, which includes a toll-free number to call if they believe they were blocked in error.”⁹ CenturyLink offers Anonymous Call Rejection service that plays the following intercept message to the calling party: “The party you are calling does not accept blocked calls. If you are calling from a blocked number, please hang up, pick up the receiver, press *87 and redial the phone number. When you do your name and number will appear for this call only.”¹⁰ Similarly, CenturyLink’s “Call Rejection Service” plays a message to the called party that the person being called is not accepting calls.¹¹

Comcast and Cox also state that they provide Anonymous Call Rejection services that incorporate intercept messages to the calling party notifying them that their calls are being rejected.¹² Notably, Cox offers these blocking services through a third party, Nomorobo, which “automatically identifies and blocks unwanted and illegal calls and sends an intercept message to the calling party when calls are blocked.”¹³ Cox’s statement confirms that intercept messages are feasible even when the blocking is accomplished through analytics providers such as Nomorobo. Indeed, virtually all providers discussed in the Call Blocking Report incorporate an intercept message informing calling parties that their calls are not being accepted and steps needed to

⁹ Call Blocking Report at 12, ¶ 24.

¹⁰ Call Blocking Report at 14, n. 109; CenturyLink, *How to Block Unwanted Calls on Your Landline*, <https://www.centurylink.com/home/help/home-phone/calling-features/block-unwanted-calls-from-your-home-phone.html> (last visited August 31, 2020).

¹¹ *Id.*

¹² Call Blocking Report at 15, ¶ 30 (Comcast offers free “Anonymous Call Rejection” as an opt-in feature, but plans on offering this to all Xfinity Voice subscribers as an opt-out feature in the future.”); Comcast: <https://forums.xfinity.com/t5/Phone/ANSWERED-How-to-stop-unwanted-calls/ta-p/3170369> (noting caller will hear a message that the calling party is not accepting calls); Call Blocking Report at 15-16, ¶ 31 (stating Cox offers Anonymous Call Rejection and Selective Call Rejection, both of which “provide calling parties an intercept message when their calls are blocked.”)

¹³ Call Blocking Report at 16, ¶ 31

redial.¹⁴ Anonymous call rejection services, which have been a standard feature on phones with caller ID for many years, demonstrate the feasibility of utilizing intercept messages within the network of both traditional TDM services as well IP-based voice services. There is no reason to believe that similar real-time notifications providing an audio intercept message are not feasible for call blocking programs generally.

B. The IETF Has Proposed a Safe and Interoperable SIP Response Code

As the Commission has recognized, industry is in the process of developing a new SIP response code that can be incorporated into IP networks using existing SIP protocol mechanisms.¹⁵ This proposed new response code, code 608, would allow calling parties to learn that an intermediary, such as an analytics engine or a voice service provider, rejected their call and provides a “redress address” that allows callers to contact the intermediary.¹⁶ As noted in the proposed specification, co-authored by former Commission CTO Eric Burger, a new code is needed to distinguish between existing response codes that enable *users* to reject a call, such as a 607 SIP response code for an unwanted call, and calls that are blocked *in the network* by voice service providers and their intermediate analytics companies using algorithms.¹⁷ With the 607 response code, the called user’s device, the user agent server (usually a phone), sends the

¹⁴ See, e.g., Frontier: <https://frontier.com/~media/HelpCenter/Documents/phone/calling-features/frontier-calling-features.ashx?la=en>; Verizon: <https://www.verizon.com/support/residential/homephone/calling-features/stop-unwanted-calls>; Vonage: <https://support.vonage.com/articles/answer/Anonymous-Call-Block-951>.

¹⁵ See, e.g., Order at ¶ 107.

¹⁶ More specifically, the 608 response code would inform the SIP User Agent Client, the device that initiates a request to start a SIP session, that the call has been automatically rejected by an intermediary such as an analytics engine. Internet Engineering Task Force, RFC 8688, *A Session Initiation Protocol (SIP) Response Code for Rejected Calls* (Dec. 2019), (IETF RFC 8688) (<https://tools.ietf.org/html/rfc8688>).

¹⁷ IETF RFC 8688 at 4.

unwanted call code back to the caller. But the decision to reject the call as unwanted is made in the first instance by a human, the called party.

As we enter the age of analytics based network level blocking, response codes like the 607 unwanted call code will not work because the calling party's device never receives a SIP INVITE. The call is blocked in the network. As stated in the IETF document, "it would be beneficial for the caller to learn who rejected the call so they can correct the misidentification."¹⁸ The proposed new code would include in the header information sent back to the calling party by the intermediary a "redress address" using the same secure mechanism used in STIR.¹⁹ Using this secure mechanism will help prevent potential network attacks.²⁰

The Commission expressed concern that this response code can only be used for IP-based traffic.²¹ The proposed 608 response code specification, however, includes mechanisms for interoperating with legacy networks. It addresses the issue of calls originating from non-IP networks and terminated to SIP networks by having the first IP-enabled device that can apply this specification, such as a media gateway or session border controller, play an audio announcement conveying how to contact the intermediary that blocked the call.²² The proposed specification may require that the intermediary itself provide the announcement, which could be a special information tone, a voice message such as "your call has been rejected by . . . ," or it could be a text-to-speech or speech-to-text message.²³

The proposed 608 response code specification also addresses concerns that the code could be sent to bad actors who could then seek to change the call behavior to defeat the

¹⁸ *Id.* at 5.

¹⁹ *Id.* at 7.

²⁰ *Id.* at 18-19.

²¹ Order ¶ 107.

²² IETF RFC 8688 at 10

²³ *Id.* at 17.

blocking system or could seek to use the contact information contained in the SIP response to launch attacks on the intermediary or for other corrupt purposes. The authors view the latter as the more significant risk. The proposal therefore outlines steps that the intermediary can take to protect itself, including utilizing certain STIR protocols to encrypt information.²⁴

The Alliance urges the Commission to call on the IETF to promptly finalize standards for this response code.

C. Notifications Should Be Standardized, Offered at No Cost, and Be a Condition of Utilizing a Safe Harbor

Given the vast number of providers, analytics companies and devices in the network, it is critical that notification mechanisms be standardized to reduce cost and complexity. Requiring voice service providers or their calling customers to adapt to a variety of proprietary notification systems would be unworkable. Additionally, because notification is an essential element of an effective and transparent redress process, notification must be offered at no cost, as are the other elements of redress. Finally, the Commission should confirm, as it did for the redress mechanisms adopted in the Order, that implementation of a notification mechanism is a condition of obtaining the protections of any blocking safe harbor.

D. Notification and Redress Are Necessary to Avoid Unreasonable Blocking Based on Missing or Inaccurate STIR/SHAKEN Information

The Commission seeks comment on ways to avoid unreasonable blocking based on the lack of, or inaccurate, call authentication information. Specifically, the Commission seeks comment on establishing a process for a calling party adversely affected by caller ID information to verify the authenticity of its calls. It also asks about ways to ensure that calls from customers

²⁴ *Id.* at 18.

of voice providers for whom the Commission has delayed the STIR/SHAKEN implementation deadline are not unreasonably blocked due to the lack of authentication information.²⁵

These are important questions for Alliance members who primarily service enterprise customers. As the Commission is well aware, calls from enterprise customers create unique circumstances that may prevent the originating voice service provider from signing the call with an A-level attestation. These complicated calling scenarios may delay full implementation of STIR/SHAKEN for enterprise customers and lead the Commission to provide an extension for enterprise calling. Moreover, many Alliance members may qualify as smaller providers to whom the Commission grants a deadline extension. Providing real-time notification is one important mechanism to help ensure that voice service providers that have not been able to implement call authentication, or to provide an A-level attestation, are not adversely affected. Upon being notified that their call has been blocked and by whom, the service provider can contact that blocking entity to remove blocks that may have been implemented in part due to the lack of call authentication information or a lower level of attestation.

E. Redress Mechanisms, Including Notification, Should Be Required When Adversely Labelling Calls

The Commission seeks comment on whether it should address call labeling and, in particular, whether redress mechanisms should be required when voice service providers or their analytics partners erroneously place an adverse label, such as “spam” or “scam,” on legitimate calls.²⁶ The answer is a resounding yes. The record is replete with examples of mislabeled calls.²⁷

²⁵ Notice at ¶¶ 85-86

²⁶ Notice at ¶ 109.

²⁷ *See, e.g.*, Reply Comments of ACA International, CG Docket No. 17-59, WC Docket No. 17-97 at 1-2 (filed February 28, 2020); Comments of Sirius XM Radio Inc., CG Docket No. 17-59 (filed September 24, 2018); Letter from American Bankers Association et al., to Marlene Dortch, Secretary of the FCC, CG Docket No. 17-59 at 3-4 (filed July 2, 2020).

Mislabeled is tantamount to blocking. As the Commission has reported, consumers only answer their phone 9% of the time when the call is marked as “spam.”²⁸ This conforms to common sense: Few consumers will answer a call labeled “spam” or “scam likely.” Labelling is based on the same analytics used to block calls and is subject to the same propensity to misidentify legitimate calls based on indicia such as call volume and call duration that apply to legitimate calling campaigns. As Numeracle has previously informed the Commission, different analytics companies apply different risk assessments, and differing labels ranging from spam to no label at all, to the same calling number.²⁹ As a result, critically important and wanted calls are being mislabeled as spam, creating the same harm as outright blocking.³⁰ There is no rational basis to require redress for blocked calls but not for mislabeled calls, particularly when the two actions are being performed by the same entities and based on the same analytics and processes.

Moreover, the TRACED Act requires that labeling be addressed. For example, section 4(c)(2) requires the Commission to incorporate transparent and effective redress mechanisms as part of a safe harbor limiting liability to “the extent to which the provider of voice service blocks *or identifies calls*” based on STIR/SHAKEN or another call authentication framework.³¹ Identification, which implies providing information, is something different than blocking. By including both blocking and identification, Congress expressed its clear intent that the Commission address labeling as well as blocking.

²⁸ Order at n. 8

²⁹ See Letter from Rebekah Johnson, CEO, Numeracle, Inc., to Marlene Dortch, Secretary of the FCC, CG Docket No. 17-59, WC Docket No. 17-97 (filed May 30, 2019) (“Numeracle May 2019 Letter”).

³⁰ Numeracle May 2019 Letter (describing that calls to victims of crime regarding the status of offenders are being mislabeled as spam).

³¹ TRACED Act 4(c)(2)(A) (emphasis added).

Other provisions of the TRACED Act corroborate this understanding. Section 4(c)(1)(B) requires the Commission to adopt rules establishing a safe harbor for the “unintended or inadvertent misidentification of the level of trust” based on call authentication information. That misidentified level of trust will manifest itself as a label on the call recipient’s phone.³² Similarly, the TRACED Act requires the Commission to establish a process to permit a calling party adversely affected “by the information provided” by call authentication to verify the authenticity of the call.³³ Again, that call authentication information likely will be conveyed to called parties in the form of a label.

Given the obvious harm mislabeling imposes on legitimate callers, and the TRACED Act mandate to address labeling, the Commission should extend the same redress mechanisms established for erroneous blocking to erroneous labeling, including notifying callers that a call is being adversely labelled.

III. Providers Should be Required to Respond to Appropriate Traceback Requests

The Alliance concurs with the Commission’s proposal to require voice service providers to respond to traceback requests from the Commission, law enforcement, or the Traceback Consortium.³⁴ Utilized in a fair and responsible manner, the traceback process can be an effective tool to mitigate illegal robocalls. The Alliance believes that all legitimate voice service providers will seek to be responsive to traceback requests. Failure to timely respond to such requests therefore is likely to be caused not by indifference but due to the manner in which the

³² *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97, 34 FCC Rcd 3241, 3266-67, ¶ 54 (2020) (identifying providers that plan to insert a label such as “Caller Verified” on authenticated calls).

³³ TRACED Act, § 4(c)(1)(c).

³⁴ Notice at ¶ 96.

traceback request was sent. For example, traceback requests sent to personnel in the company unfamiliar with the process, such as requests sent to customer care centers or operational personnel, or multiple requests arriving from various sources, may delay response.

The Commission should seek to ensure that traceback requests are addressed to appropriate personnel, such as a company's general counsel, or senior management, and it should preclude adverse inferences for failure to timely respond where the requests are sent to inappropriate personnel. As the traceback process matures, the Alliance believes that identification of appropriate personnel will become normalized. The Commission might consider requiring that the traceback requests sent by the Commission, law enforcement or the Traceback Consortium be copied to a company's registered agent. Virtually all voice providers that interact with the Commission must designate an agent.³⁵

The Commission should limit the entities that can make traceback requests to the Commission, law enforcement or the Traceback Consortium. Authorizing a broad array of actors, such as a provider in a call chain, to make traceback requests may create confusion for the receiving provider if multiple requests, often in the form of trouble tickets, are made regarding the same calls.

The Commission asks about the costs and burdens imposed by responding to traceback requests. There are obviously costs associated with responding to such requests as key personnel are required to divert time and resources to collecting the requisite information. Recipients should, therefore, be afforded a reasonable opportunity to collect information. It would be reasonable, however, to require, in the absence of extenuating circumstances, that recipients

³⁵ 2020 Instructions to the Telecommunications Reporting Worksheet, FCC Form 499-A, at 18. <https://docs.fcc.gov/public/attachments/DA-20-164A3.pdf>

promptly acknowledge receipt of a traceback request that has been directed to appropriate personnel.

The Alliance has previously raised concerns that some traceback requests would call for information that would entail breaching existing contractual provisions that bar disclosure of confidential information unless legally compelled. The Commission rejected these concerns and, among other findings, suggested that providers review and eliminate such provisions as soon as possible.³⁶ The Alliance respectfully suggests that the Commission underestimates the burden such a requirement imposes. Many voice providers, including intermediate carriers, have hundreds of contracts with carriers, many of which were entered into years ago. Moreover, voice service providers cannot unilaterally amend contracts. The other party must agree to the amendment as well. Even where the other party would agree to the amendment, the process takes time.

The confidentiality provisions in these contracts were not adopted in order to hinder then nonexistent traceback processes. They are instead standard confidentiality provisions. Although it may be reasonable to suggest including appropriate language exempting traceback requests from confidentiality provisions in new or renewed contracts, requiring amendment of hundreds of existing contracts is simply unrealistic and imposes an unreasonable burden on providers.

There is, however, a ready solution. Most confidentiality provisions provide for release of information if requested by law enforcement or regulatory authorities. The Commission proposes that traceback requests may come from it or law enforcement. Requests from such entities most

³⁶ *In the Matter of Implementing Section 13(d) of the Pallone-Thune Tel. Robocall Abuse Criminal Enft & Deterrence Act (Traced Act)*, EB Docket No. 20-22, DA20-785 at ¶ 28 (rel. July 27, 2020).

likely would fall within confidentiality provision exceptions for disclosure based on legal process and would enable the release of otherwise confidential information in a timely way.

IV. The Alliance Supports Adoption of Mitigation Measures

The Alliance concurs in the Commission’s proposal that, once notified *by the Commission* that it is carrying illegal traffic, the voice provider should take action to mitigate that traffic.³⁷ The Commission has already determined that, upon receipt of a notification by the Commission, voice providers “should promptly investigate and, if necessary, prevent the illegal caller from continuing to use the network to place illegal calls.”³⁸ The Commission, however, declined to mandate specific mitigation steps other than that they “involve a significant reduction in the traffic.” The Commission stated that a significant reduction should be measured “relative to the entire call stream” and a 20% to 50% (or lower) reduction may be sufficient.³⁹

The Alliance believes that this approach is reasonable and does not require the adoption of more specific mitigation steps at this time. Alliance members do not want illegal traffic on their networks. Such traffic likely violates their contractual provisions and terms of use policies. If alerted by the Commission that such traffic nevertheless appeared on their networks, Alliance members will undertake the investigative and remedial steps necessary to mitigate that traffic. Alliance members are fully prepared to sever ties with customers that continue to send illegal traffic on their networks and do not require regulatory compulsion to take appropriate actions.

The Alliance also concurs in the Commission’s proposal to require voice service providers to take “affirmative, effective measures to prevent new and renewing customers from

³⁷ Notice at ¶ 98.

³⁸ Order at ¶¶ 39, 41 (requiring voice providers to determine the source of the traffic and prevent the source from continuing to originate the traffic and to implement safeguards to prevent new and renewing customers for using its network to originate illegal calls.)

³⁹ Order at n. 100.

using their networks to originate illegal calls.”⁴⁰ Providers would benefit from guidance as to what constitutes a minimum level of mitigation sufficient to demonstrate compliance with this proposal. Such guidance, however, need not be overly prescriptive.

The Alliance believes the following steps are sufficient to meet the Commission’s call for affirmative and effective measures to prevent new and renewing customers from originating illegal traffic. Following guidance from USTelecom’s ITG, now the Traceback Consortium, the provider should “confirm the identity of new commercial customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of customer’s business.”⁴¹ Collection of this information should satisfy any “know-your-customer” due diligence requirement. The provider should also include in its contracts and terms of use policy that customers may not send illegal traffic to the provider. Both of these steps are already taken by the vast majority of voice service providers. Coupled with an obligation to respond to a notice from the Commission that illegal traffic is crossing the provider’s network, these steps should demonstrate that the provider has taken sufficient mitigating steps with respect to new or renewing customers.

V. The Commission Should Accommodate Use of Third Parties In Acquiring New Customers

It is a common practice in the communications industry (indeed in many industries) for voice providers to utilize third parties to identify and sign up new enterprise customers. In some circumstances, these third parties may simply identify and sign up new customers who are then served by a voice service provider. In other instances, the third parties may retain the retail relationship with the customer and resell the network services of an underlying network provider.

⁴⁰ Notice ¶ 101.

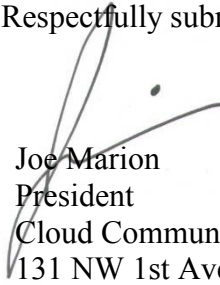
⁴¹ USTelecom Whitepaper; How to Identify and Mitigate Illegal Robocalls, Oct. 2019, at 8 (<https://www.ustelecom.org/research/how-to-identify-and-mitigate-illegal-robocalls>).

The Commission should ensure that it assigns any “know-your-customer” due diligence requirements for new customers on the entity that is in a position to undertake the obligation – the entity that identifies the customer to be served. If a voice service provider utilizes a third party to acquire the customer, it should be sufficient for the voice service provider to require in its contract with the third party that the third party obtain any required “know-your-customer” information.

VI. CONCLUSION

The Alliance strongly supports the Commission’s ongoing efforts to combat illegal robocalls while ensuring that legitimate calls can be completed. Those efforts will be enhanced by requiring real-time notification of blocking or mislabeling, and by providing appropriate information and guidance to voice service providers to assist in their efforts to keep illegal traffic off of their networks.

Respectfully submitted,



Joe Marion
President
Cloud Communications Alliance
131 NW 1st Avenue
Delray Beach, FL, USA 33444
(561) 232-3891

August 31, 2020