

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

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

**REPLY COMMENTS OF iBASIS, INC.**

iBASIS, Inc. (“iBASIS” or the “Company”), by and through counsel, respectfully submits these reply comments to the Further Notice of Proposed Rulemaking in the above-captioned proceedings.<sup>1</sup> Rather than imposing unique mandates on gateway providers, the initial comments reflect a general consensus that the most efficacious approach to reducing illegal foreign-originated robocalls is to require gateway providers to register in the Robocall Mitigation Database (“RMD”) and certify that they have implemented a reasonable mitigation plan. iBASIS supports this approach. iBASIS again urges the Federal Communications Commission (“Commission”) to exempt conversational traffic, such as roaming traffic, from any obligations it establishes in this proceeding. Conversational traffic is highly unlikely to be the source of foreign-originated illegal calls.

**I. Solutions Should Be Carefully Tailored to Address the Problem**

The robocall mitigation measures that emanate from this proceeding should be carefully tailored to address the primary concern, which is the proliferation of high volume, largely randomized scam calls using U.S. numbers in the caller ID field to enhance the prospects of the

---

<sup>1</sup> *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) (“Gateway Notice”).

call being answered. Conversational traffic, such as wireless roaming calls, should be exempt because these calls are not the source of the problem. As noted by ZipDX and others, providers should be “looking for high-volume-short duration traffic.”<sup>2</sup> Similarly, the Commission should restrict any and all obligations it adopts in this proceeding to foreign calls using U.S. numbers.<sup>3</sup>

## **II. There is Virtually No Support for Mandates**

The record demonstrates that requiring gateway providers to authenticate calls, engage in mandatory blocking, or respond to all traceback requests within 24 hours is unnecessary and potentially counterproductive.<sup>4</sup>

The Commission Should Not Require Gateway Providers to Authenticate Calls. There is virtually no support in the record for the Commission’s proposal to mandate gateway providers to authenticate foreign-originated calls. As iBASIS noted in its initial comments, rather than mandate authentication, the Commission should retain its current policy of allowing intermediate providers, including gateway providers, to authenticate calls where they deem it appropriate.<sup>5</sup>

The majority of commenters addressing the issue agree with this approach.<sup>6</sup> Various commenters

---

<sup>2</sup> Comments of ZipDX, CG Docket No. 17-59, WC Docket No. 17-97, at 17 (filed Dec. 7, 2021) (“ZipDX Comments”); Comments of YouMail, CG Docket No. 17-59, WC Docket No. 17-97, at 9 (filed Dec. 8, 2021) (“YouMail Comments”) (“for any gateway provider with significant call volumes, the majority of those calls should have durations of more than 20 seconds each”); Comments of i3forum, CG Docket No. 17-59, WC Docket No. 17-97, at 11 (filed Dec. 10, 2021) (“i3forum Comments”) (“The Commission’s proposals would only apply to the origination of a high volume of calls.”). *See also* Comments of Belgacom International Carrier Services, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed Nov. 22, 2021) (“BICS Comments”) (asking if roaming traffic is excluded from the authentication requirement); Comments of Comcast, CG Docket No. 17-59, WC Docket No. 17-97 at 10-11 (filed Dec. 10, 2021) (“Comcast Comments”) (recommending thoughtful examination of the CTIA petition to reconsider the foreign provider prohibition, which raises reasonable concerns over blocking legitimate wireless roaming traffic).

<sup>3</sup> Gateway Notice ¶ 36. *See* ZipDX Comments at 17 (noting that “almost all illegal robocalls use US caller ID values”).

<sup>4</sup> *See generally* Comments of USTelecom, CG Docket No. 17-59, WC Docket No. 17-97, at 7 (filed Dec. 10, 2021) (“USTelecom Comments”) (stating that “gateway provider-specific rules may be counterproductive.”).

<sup>5</sup> Comments of iBASIS, CG Docket No. 17-59, WC Docket No. 17-97, at 5-6 (filed Dec. 10, 2021) (“iBASIS Comments”).

<sup>6</sup> *See, e.g.*, i3forum Comments at 3-5; Comments of AB Handshake, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (filed Nov. 26, 2021) (“AB Handshake Comments”); USTelecom Comments at 9-10; ZipDx Comments at 18-19. *But see* Comcast Comments at 4 (strongly supporting the proposal to require gateway providers to apply STIR/SHAKEN-compliant attestation to unauthenticated foreign calls using U.S. numbers).

correctly note that an authentication mandate would result in a flood of “C-Level” attestations that provide no useful information regarding the validity of the number in the caller ID.<sup>7</sup> Moreover, any utility of a C-level attestation in facilitating traceback has been overtaken by advances in the traceback process that now works very quickly.<sup>8</sup> Moreover, the exceedingly marginal benefits of mandating authentication are far outweighed by the substantial costs of undertaking necessary network modifications.<sup>9</sup>

Although mandating authentication is unwise, should a gateway provider determine that it may be able to attach meaningful attestations to incoming foreign-originated calls, the Commission can facilitate such authentications by revising, or encouraging the STI governing authority to revise, the criteria to obtain STIR/SHAKEN tokens. Specifically, the requirement to have an OCN should be eliminated.<sup>10</sup> As noted by ZipDX, many providers in the calling ecosystem do not have OCNs but do file 499 forms.<sup>11</sup> Filing a Form 499 combined with registering in the RMD should be sufficient to obtain a token. Finally, as recommended by the i3forum, the Commission should consider alternative means of authentication for foreign-originated calls.<sup>12</sup> To date, only the U.S. and Canada are implementing STIR/SHAKEN. Thus, gateway providers are unlikely to receive STIR/SHAKEN compliant authentications. One such alternative is described in the comments filed by AB Handshake, which has deployed an out-of-band verification solution on an international level that entirely eliminates the need for

---

<sup>7</sup> See, e.g., AB Handshake Comments at 4-5; BICS Comments at 3 (“It is very unlikely that gateway providers will use any other attestation level but C”); iBASIS Comments at 5-6.

<sup>8</sup> See, e.g., ZipDX at 18 (noting that “[t]raceback is already very fast.”); USTelecom Comments at 11 (“industry traceback process has advanced to become so quick and efficient that C-level attestations offer at best marginal benefit for traceback”).

<sup>9</sup> iBASIS Comments at 6; USTelecom Comments at 11 (noting substantial costs to deploy upgrades “up to eight figures for some providers” and would “involve multiple years of complex project management activity.”).

<sup>10</sup> See iBASIS Comments at 7.

<sup>11</sup> ZipDX Comments at 36. See generally BICS comments at 3 (noting difficulty in obtaining tokens).

<sup>12</sup> i3forum Comments at 4.

intermediate carriers to transmit caller ID authentication information.<sup>13</sup> Instead, using their solution, U.S. terminating carriers would be able to verify numbers directly with foreign-originating carriers.<sup>14</sup> Therefore, rather than mandating the implementation of expensive authentication options for gateway providers that provide minimal benefits, the Commission should instead consider enabling flexible approaches to address foreign-originated illegal robocalls.

Rather Than Mandates, The Commission Should Enable Permissive Blocking with Safe Harbor

Protections. The Commission incentivizes voice service providers to block potentially illegal robocall traffic under defined circumstances by protecting them from liability through safe harbors. The record overwhelmingly supports extending this permissive framework to gateway providers and almost uniformly rejects mandatory blocking requirements.<sup>15</sup> As aptly noted by USTelecom, “blocking mandates can cause unintended consequences,” including the blocking of legitimate calls.<sup>16</sup> USTelecom also correctly observes that the terminating carriers that are directly serving the called parties are already undertaking “sophisticated blocking” and that therefore there is “limited benefit to gain of a blocking mandate further upstream.”<sup>17</sup>

The comments also recognize the importance of extending safe harbor protections to gateway providers that do engage in blocking.<sup>18</sup> The Commission should adopt this consensus

---

<sup>13</sup> AB Handshake Comments at 5-7.

<sup>14</sup> *Id.* at 7.

<sup>15</sup> *See, e.g.*, i3Forum Comments at 6-7; Comments of CTIA, CG Docket No. 17-59, WC Docket No. 17-97, at 12 (filed Dec. 10, 2021) (“CTIA Comments”) (deviating from the existing permissive call blocking approach would have “serious call completion implications for legitimate calls originating outside of the United States”); Comments of INCOMPAS, CG Docket No. 17-59, WC Docket No. 17-97, at 11 (filed Dec. 10, 2021) (“INCOMPAS Comments”); Comments of T-Mobile, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (filed Dec. 10, 2021) (“T-Mobile Comments”); USTelecom Comments at 12. *See also* Comcast Comments at 8 (suggesting that the Commission explore mandatory blocking but appropriately tailored).

<sup>16</sup> USTelecom Comments at 12.

<sup>17</sup> *Id.* at 12.

<sup>18</sup> *See, e.g.*, BICS Comments at 5; i3forum Comments at 7; Comments of Transaction Network Services, Inc., CG Docket No. 17-59, WC Docket No. 17-97, at 2-4 (filed Dec. 10, 2021) (“TNS Comments”) (providing a safe harbor

view and extend safe harbor protections to gateway providers that engage in blocking calls under the circumstances currently authorized by the Commission.<sup>19</sup> Commenters also agree with iBASIS that the Commission should provide more guidance on what constitutes reasonable analytics.<sup>20</sup>

The Record Reflects that Imposing a 24-Hour Response to Traceback Requests is Unnecessary.

A number of commenters concur that mandating that gateway providers respond to traceback requests within 24 hours is unnecessary and may unfairly expose providers to enforcement action when a response is impracticable within that time frame.<sup>21</sup>

**III. The Record Identifies a Number of Alternative Approaches to Curbing Illegal Foreign Robocalls**

Rather than imposing a number of specific mandates, the record reflects a consensus approach that would require gateway providers to file mitigation plans in the Robocall Mitigation Database.<sup>22</sup> iBASIS proposed this approach in its initial comments.<sup>23</sup> In assessing the reasonableness of mitigation plans, the Commission should acknowledge the indisputable fact

---

“is crucial to encourage [gateway providers] to adopt zealous analytics to identify and block calls”); YouMail Comments at 4; T-Mobile Comments at 6; INCOMPAS Comments 12-13.

<sup>19</sup> Various comments also agree that gateway providers should have an opportunity to investigate suspicious traffic before initiating any blocking after being notified by the Commission. *See, e.g.*, ZipDX Comments at 25; T-Mobile Comments at 6. The safe harbor should not be conditioned on the same redress and notification requirements applied to domestic traffic. Gateway providers, typically far removed from the call originator, have no way of transmitting real-time notifications to the call originator or the originating network. As noted by the i3forum, blocking foreign-originated calls “requires global synchronization” and agreement on “blocking processes and procedures” that do not currently exist. i3forum Comments at 6.

<sup>20</sup> *See* iBASIS Comments at 11; Comments of Twilio, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (filed Dec. 10, 2021) (“Twilio Comments”). *See also* i3forum Comments at 11 (suggesting the Commission to define high volume of calls). *But see* TNS Comments at 5 (the Commission should decline to provide further guidance on what constitutes reasonable analytics).

<sup>21</sup> *See, e.g.*, i3forum Comments at 8 (24 hours may not be enough time to conduct a thorough and accurate traceback analysis of international calls.); CTIA Comments at 11; T-Mobile Comments at 7; INCOMPAS Comments at 9; ZipDX Comments at 19-20 (noting that response time is generally not an issue because most providers respond promptly and that imposing a 24-hours deadline just on gateway providers is neither necessary nor particularly useful).

<sup>22</sup> CTIA Comments at 6-7 (all providers, including intermediate providers and gateway providers should implement mitigation programs); Comcast Comments at 10; Twilio Comments at 3; USTelecom Comments at 3.

<sup>23</sup> iBASIS Comments at 13.

that gateway providers do not have direct relationship with the call originator and thus are in no position to confirm that the call originator is authorized to use the number in the caller ID or conduct know-your-customer due diligence where the customer is the call originator.<sup>24</sup> A reasonable mitigation plan for gateway providers would involve the monitoring of high volume traffic for foreign calls using NANPA numbers, promptly investigating suspicious traffic and responding to traceback requests, and taking affirmative action, including blocking traffic when it determines such action is appropriate to stop the influx of identified illegal calls.

iBASIS again respectfully urges the Commission to eliminate the requirement that foreign voice service providers register in the RMD or have their calls blocked.<sup>25</sup> Requiring U.S. gateway providers to register and submit reasonable mitigation plans along with extending the authority to block calls with safe harbor protections is sufficient, as a next step, to address illegal foreign robocalls.<sup>26</sup> The Commission should allow gateway providers who, like iBASIS, were imported into the RMD to supplement their RMD entry by submitting a mitigation plan without having to completely refile.<sup>27</sup>

The Commission should explore other alternative avenues suggested in the record. Economic incentives may be one approach.<sup>28</sup> The i3forum, for example, recommends that the

---

<sup>24</sup> See, e.g., i3forum Comments at 9-10; CTIA Comments at 13; INCOMPAS Comments at 10; Twilio Comments at 3-4. As noted by i3forum, the problem is not solved by identifying the gateway providers' direct upstream partner as the customer because that provider too is also unlikely to have information about the call originator. i3forum Comments at 10.

<sup>25</sup> iBASIS Comments at 13. See also INCOMPAS Comments at 14; Comcast Comments at 11 (supporting decision to suspend enforcement of the foreign provider prohibition).

<sup>26</sup> See INCOMPAS Comments at 14-15.

<sup>27</sup> The Commission should reject USTelecom's suggestion that the Commission remove from the RMD any provider currently in the database that was imported by the Commission as an intermediate provider. USTelecom Comments at 6. USTelecom offers no explanation for taking this action. iBASIS was imported into the database and there is no reason why it should be removed. Instead, intermediate providers, or at least those that are also gateway providers should supplement their filing with a mitigation plan.

<sup>28</sup> See generally ZipDX Comments at 22 (suggesting economic penalties to motivate compliance).

Commission require gateway providers to impose a surcharge on high volume traffic.<sup>29</sup> The surcharge, which would be assessed on all completed calls and call attempts, would ultimately be passed through to the call originator. The additional surcharge would potentially eliminate one of the drivers of these calls: the relatively minor expense to generate large volumes of calls.<sup>30</sup> Further information sharing with gateway providers would also help mitigate illegal calls.<sup>31</sup> Providing ready access to a single, comprehensive database for do not originate numbers is one specific example.<sup>32</sup>

Other technical solutions have been suggested. As noted above, AB Handshake has begun internationally deploying an out-of-band solution that would enable terminating providers to verify traffic directly with originating providers. SipNav also describes a solution that leverages the unique media IP address of the servers that initiate robocalls.<sup>33</sup> The Commission should consider exploring these alternative approaches that may supplement, or, in appropriate circumstances, replace existing mitigation techniques.

## CONCLUSION

iBASIS looks forward to continuing working with the Commission on the adoption of balanced and efficacious mechanisms to reduce illegal, foreign-originated robocalls.

---

<sup>29</sup> i3forum Comments at 8 (suggesting that gateway providers monitor for high call volumes with short duration and assess a surcharge above regular per minute rates for such calls.)

<sup>30</sup> i3forum Comments at 8-9. The surcharge would have to be mandatory or bad actors would simply find providers that do not assess the charge. *Id.*

<sup>31</sup> *See, e.g.*, i3forum Comments at 11-12 (identifying various types of information and tools that could enhance gateway providers' ability to detect and deter fraudulent calls).

<sup>32</sup> *See* Comments of Somos, CG Docket No. 17-59, WC Docket No. 17-97, at 3-4 (filed Dec. 10, 2021); USTelecom at 2-3.

<sup>33</sup> Comments of SipNav, CG Docket No. 17-59, WC Docket No. 17-97 at 2-4 (filed Dec. 10, 2021).

Respectfully submitted,

\_\_\_\_\_  
/s/

Michael H. Pryor

Shareholder

Brownstein Hyatt Farber Schreck, LLP

1155 F Street NW, Suite 1200

Washington, DC 20004

(202) 383-4706

[mpryor@bhfs.com](mailto:mpryor@bhfs.com)

*Counsel to iBASIS, Inc.*

January 10, 2022