

ROBOCALL MITIGATION PLAN
Inphonite, LLC
Updated June 5, 2025

I. OVERVIEW

FCC rules require voice service providers to certify in the FCC’s Robocall Mitigation Database (“RMD”) that they have implemented a Robocall Mitigation Plan. This Robocall Mitigation Plan is submitted by Inphonite, LLC (“Inphonite”) in compliance with FCC Rule § 64.6305. For purposes of this Robocall Mitigation Plan, Inphonite is a “voice service provider” as defined at FCC Rule § 64.6300(o).

Inphonite is committed to ensuring that its systems are used only for proper and lawful purposes. The information, policies, and procedures in this Robocall Mitigation Plan constitute and demonstrate “reasonable steps” taken by Inphonite to avoid or mitigate the origination, carriage, or processing of illegal robocall traffic. Inphonite’s Robocall Mitigation Plan describes and provides detailed practices that can reasonably be expected to reduce the possibility of Inphonite originating illegal robocalls. Inphonite complies with the procedures described herein.

II. INPHONITE

Inphonite provides a platform by which its clients, which are primarily in the healthcare and dental industry, can contact patients about appointments, test results, and other patient information. Reminders and related communications are sent over Inphonite’s platform to patients via text messages, voice calls, and email. Inphonite’s services include HIPAA-compliant two-way texting, creation of patient portals, and related services. Inphonite’s platform integrates with patients’ electronic health records (“EHRs”) to conveniently and securely deliver timely and needed information to patients.

Because of the nature of Inphonite’s business—delivering calls and texts from established medical providers such as hospitals and medical offices directly to specified patients, based on information in the patients’ EHRs—Inphonite believes that it would be very unlikely for its system to be used for the origination of illegal or improper robocalls. Nevertheless, Inphonite recognizes the importance of providing detailed information regarding its efforts to mitigate the origination or carriage of illegal robocalls.

Inphonite’s contact information is:

Inphonite, LLC
2942 N 24th St, Ste 115
PMB 160681
Phoenix, Arizona 85016-7849
800-350-6793
inphonitesales@inphonite.com

Robocall Mitigation Contact: Jason Heath, CFO, fcc@inphonite.com, 800-350-7693

III. MEASURES TO PREVENT NEW AND EXISTING CUSTOMERS FROM ORIGINATING ILLEGAL ROBOCALLS

FCC Rule § 64.6305(d)(2)(ii) requires that a voice service provider describe specific reasonable steps taken to avoid originating illegal robocall traffic. Inphonite provides the following information in compliance with this requirement.

A. “Know Your Customers”

FCC Rules §§ 64.6305(d)(2)(ii) and 64.1200(n)(4) require that a voice service provider take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.

Inphonite has affirmative, effective measures in place to prevent new and renewing customers from using its network to originate illegal calls. One such measure is “knowing its customers.” Most of Inphonite’s customers are hospitals, doctor’s offices, dentist’s offices, or other similar providers of medical services. Inphonite spends time to get to know each of these customers. This is necessary in part so that Inphonite and each customer can decide what package of Inphonite’s services will be used by the customer. As part of this process of getting to know its customers, Inphonite undertakes due diligence to ensure that the customer is credit-worthy and not the kind of operation that would engage in illegal or improper practices, including the origination of robocalls. Inphonite collects information such as the customer’s physical location, contact person, state or country of incorporation, federal tax ID, and the nature of the customer’s business. Inphonite does not provide services for customers located outside the United States.

Inphonite also educates its customers about the importance of avoiding and mitigating illegal robocalls and ensuring that all voice and text traffic originated by Inphonite complies with all applicable requirements. In addition, Inphonite’s system is set up so that customers do not have the ability to sign themselves up for Inphonite’s services, or to remotely set up or control Inphonite’s system on their own.

Moreover, all of Inphonite’s customers must agree to the Terms of Service (available at <https://www.inphonite.com/a/legal/terms-of-service>) and Business Associate Agreement (available at <https://www.inphonite.com/a/legal/baa>). The Terms of Service specifically prohibit Inphonite’s customers from using Inphonite’s service in a manner that would give rise to civil liability under any applicable laws or regulations, including the FCC’s regulations. The Terms of Service provide that if Inphonite believes a customer is using Inphonite’s service to break any FCC laws or regulations, Inphonite may take action ranging from pausing the delivery of messages to completely cancelling service to the customer without notice.

B. “Know Your Upstream Providers”

FCC Rule § 64.6305(d)(2)(ii) requires that a voice service provider describe any procedures in place to know its upstream providers. Inphonite does not receive calls or texts from “upstream providers”—that is not part of its business model. Accordingly, this aspect of robocall mitigation is not applicable to Inphonite.

C. Call Analytics Systems

FCC Rule § 64.6305(d)(2)(ii) requires that a voice service provider describe analytics systems it uses to identify and block illegal traffic, including whether it uses third-party analytics vendors and those vendors' names.

Inphonite does not use specific analytics systems (including third-party analytics vendors) to identify or block illegal traffic. However, Inphonite's technical staff closely and continually monitors Inphonite's system and data to confirm that what it is receiving from customers is expected. When Inphonite sees suspicious activity, it immediately investigates. If there was an unexpected spike in traffic or other patterns of traffic on Inphonite's system indicative of illegal robocall traffic, Inphonite believes it would notice such activity and would be in a position to rapidly take affirmative steps as necessary. Inphonite follows Industry Traceback Group-recommended best practices relating to traceback and trace-forward investigations.

D. Other Measures

Inphonite's business depends on ensuring that the correct messages are delivered to the correct recipients. If Inphonite's customers' patients received incorrect or improper communications, including but not limited to illegal robocalls, that would have a negative effect on Inphonite's business. Therefore, Inphonite has a strong business incentive to ensure that its system is not used to originate illegal robocalls.

Consistent with this business incentive, Inphonite takes additional measures to ensure that all communications on its system are accurate, desired, and compliant with applicable laws and regulations. For example, Inphonite educates its personnel about the importance of avoiding and mitigating illegal robocalls and ensuring that all voice and text traffic originated by Inphonite complies with all applicable requirements. In addition, Inphonite provides mechanisms for customers to opt out of messaging, using a three-prong approach: a customer can opt out with Inphonite, with Inphonite's customer, or with Inphonite's vendors. Inphonite's software can implement the opt-out so that the recipient does not receive messages under any circumstances.

IV. COMMITMENT TO RESPOND AND COOPERATE

FCC Rule § 64.6305(d)(2)(iii) requires a voice service provider to commit to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal callers that use the provider's service to originate calls.

Inphonite commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. Inphonite further commits to cooperate with such entities in investigating and stopping any illegal robocallers that use Inphonite's service to originate calls. Inphonite also respond to all requests its customers or call recipients relating to concerns about illegal robocalls. Additionally, if any activity on Inphonite's system is shown to be unlawful or to originate in an unlawful way as determined by our monitoring or by notification from any entity, Inphonite immediately pauses all service in order to further investigate. During

the investigation Inphonite reaches out to its customer to determine the validity and scope of the activity that was flagged as suspicious, working with all parties to fix any issues or, if necessary, terminate service.

V. STIR/SHAKEN IMPLEMENTATION

Inphonite does not “sign” its own calls for purposes of STIR/SHAKEN implementation. Inphonite has not fully or partially implemented STIR/SHAKEN.¹ Inphonite is exempt from the obligation to implement STIR/SHAKEN for two reasons. First, it is a pure reseller with no physical facilities and thus it does not have complete control over the physical network over which its calls travel sufficient to implement STIR/SHAKEN.² Second, Inphonite does not have and cannot get an OCN and therefore it cannot obtain a certificate and token as required to implement STIR/SHAKEN.³

Inphonite relies on its vendors, who are downstream intermediate providers, to provide STIR/SHAKEN capability. Through this process, Inphonite has obtained level B attestation. When one of Inphonite’s customers uses the same downstream intermediate provider vendor that Inphonite uses, Inphonite has level A attestation. Inphonite is continuing to pursue level A attestation with all vendors.

VI. UPDATES

Inphonite recognizes that this Robocall Mitigation Plan, as well as industry best practices and legal requirements, are continually changing in response to the ongoing challenge of combatting illegal robocalling. Inphonite will monitor industry best practices and seek to improve its internal processes to ensure that this Plan and its system adapt as necessary to new developments. In the event of any material change to this Plan, Inphonite will republish it to its personnel and file an update in the RMD within 10 days.

¹ Inphonite is updating its Robocall Mitigation Plan in part in order to comply with the FCC’s clarification that “Providers that do not obtain and use an SPC token and certification must update their Robocall Mitigation Database certifications to state that they have not fully or partially implemented STIR/SHAKEN....” See *In re Call Authentication Trust Anchor*, WC Docket No. 17-97, *Eighth Report and Order*, FCC 24-120 (rel. Nov. 22, 2024) (“*Eighth Report and Order*”), ¶ 30.

² See *Eighth Report and Order* ¶ 8 (“Providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN...are exempt from STIR/SHAKEN implementation requirements”) and notes 35 and 64.

³ See 47 C.F.R. § 64.6304(b) (“Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 [requiring STIR/SHAKEN implementation] until they are capable of obtaining an SPC token.”).