

Ironclad Connect LLC

FRN 0038725693

Robocall Mitigation Program

July 2026

Table of Contents

I. Robocall Mitigation Program Introduction	1
A. Company Summary	1
B. Filing of RMP and Implementation of STIR/SHAKEN	1
C. Regulatory Actions, Investigations and RMD Filing Status	2
II. Robocall Mitigation Program	2
1. Implementing Knowing Your Customer Protocols	3
2. Requiring Contractual Provisions to Mitigate Illegal Robocalls	3
3. Only Accepting Traffic from Providers in the RMD	4
4. Blocking Calls on a Do-Not-Originate List	4
5. Analyzing and Monitoring Network Traffic Routing Through Ironclad's Network .	4
6. Ensuring Foreign Providers Are Not Using Ironclad to Carry or Process High- Volume Illegal Traffic onto the U.S. Network	5
7. Authenticating Voice Traffic	5
8. Responding to Commission, Law Enforcement and ITG Traceback Requests	6
9. Designating an Employee for Addressing Robocall Mitigation- Related Issues	6
10. Updating Ironclad's RMD Submission and RMP	6

I. Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Program (“RMP”) details the policies and practices that Ironclad Connect LLC (Ironclad), FRN: **0038725693**, has established to prevent unlawful robocalls from originating on, terminating to, or routing through its voice network where it is operating as a Voice Service Provider, a Non-Gateway Intermediate Provider, and/or a Gateway Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R. § 64.6300.

A. Company Summary

Ironclad is a provider of cloud based VOIP communications services. With its commercial offerings, Ironclad enables service providers and businesses to transact and communicate with their customers. Depending on the services provided, Ironclad may serve as a Voice Service Provider, a Non-Gateway Intermediate Provider, and/or a Gateway Provider.

Ironclad is wholly owned and operated by Ironclad Connect LLC, a Virginia LLC, with no subsidiaries or DBAs. Ironclad utilizes certain common technical infrastructure in order to align with technical and regulatory compliance requirements and to maximize technical and operational efficiencies.

B. Filing of RMP and Implementation of STIR/SHAKEN

Ironclad has fully implemented STIR/SHAKEN and has submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. § 64.6301(a) 2. In accordance with the RMD 12/2022 Filing Instructions, FCC Rule 47 C.F.R. § 64.6305(b) and because Ironclad is a “Combined Gateway and Voice Service Provider” under these instructions, Ironclad has certified that Ironclad has “fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with FCC Rule, 47 C.F.R. § 64.6302(b).”⁴ In addition, Ironclad has uploaded this RMP into the RMD because it “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic” and has included “a commitment to respond fully and 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 robo-callers that use its service to carry or process calls.”

¹ See Robocall Mitigation Database External Filing Instructions, Version: December 2022 (“RMD 12/2022 Filing Instructions”), available at <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>

C. Regulatory Actions, Investigations and RMD Filing Status

Ironclad is not subject to any Federal Communications Commission, law enforcement, or regulatory agency actions or investigations and has not had its authority to file in the RMD revoked.

II. Robocall Mitigation Program

This RMP applies to Ironclad calling platforms and provides information on Ironclad policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps Ironclad has taken to avoid carrying or processing illegal robocall traffic”:

- (1) Implementing Knowing Your Customer Protocols
- (2) Requiring Contractual Provisions to Mitigate Illegal Robocalls
- (3) Only Accepting Traffic from Providers in the RMD
- (4) Blocking Calls on a Do-Not-Originate List
- (5) Analyzing and Monitoring Network Traffic Routing Through Ironclad’s Network
- (6) Ensuring Foreign Providers Are Not Using Ironclad to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- (7) Authenticating Voice Traffic Originated by Ironclad’s Retail Customers
- (8) Responding to Commission, Law Enforcement and ITG Traceback Requests
- (9) Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- (10) Updating Ironclad’s RMD Submission and RMP

⁴ 47 C.F.R. § 64.6302(b) (stating that Intermediate Provider shall “[a]uthenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, except that the intermediate provider is excused from such duty to authenticate if it: (1) Cooperatively participates with the industry traceback consortium; and (2) Responds fully and in a timely manner to all traceback requests it receives from the Commission, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider”).

⁵ RMD 12/2022 Filing Instructions at 12-13. *See also* 47 C.F.R. § 64.6305(d)(2)(ii) (even if a gateway provider is fully compliance with STIR/SHAKEN, it must file an RMP that sets forth “[t]he specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in § 64.1200(n)(4)”).

1. Implementing Knowing Your Customer Protocols

Consistent with the FCC’s Caller ID Authentication Best Practices No. 16 and 47 C.F.R. § 64.1200(n)(3), Ironclad vets “the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.”⁷ In so doing, Ironclad takes “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.”⁸

In this regard, Ironclad has implemented appropriate Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. As part of its KYC protocols, Ironclad requires any customer to provide sufficient information to ensure its legitimacy. Among other things, Ironclad generally requires its customers to provide the full legal name of the company, state or country of incorporation, the physical address of its operations, the billing name and address (when different), and the customer contact name and telephone number, and nature of the customer’s business. As indicated in Section 3, below, if the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, Ironclad confirms, in accordance with currently effective FCC rules, that the company is appropriately listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.⁹

2. Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of Ironclad are subject to robust terms and conditions that (1) obligate customers not to use Ironclad’s services for unlawful purposes; and (2) preserve Ironclad’s right to terminate customers for violations of the law.

Ironclad’s contracts include terms that forbid the customer from using Ironclad’s services to originate and/or otherwise transmit calls that violate laws restricting robocalls or other telemarketing calls, including the federal Telephone Consumer Protection Act (“TCPA”) and/or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”) and/or the rules promulgated pursuant to these statutes. Ironclad’s contract terms provide that if any calls originated or otherwise transmitted by the customer to Ironclad violate the TCPA, the TRACED Act, or the rules promulgated under these statutes, then Ironclad may, at its sole discretion, suspend or terminate the customer’s service immediately, among other remedies.

⁶ Wireline Competition Bureau Issues Caller ID Authentication Best Practices, WC Docket Nos. 17-97 and 20-324, DA 20-1526, at Appendix A (rel. Dec. 22, 2020) (“FCC’s Caller ID Authentication Best Practices”), available at <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>.

⁷ *Id.*

⁸ 47 C.F.R. § 64.1200(n)(3).

⁹ See 47 C.F.R. § 64.6305(e)(1)-(3).

3. Only Accepting Traffic from Providers in the RMD

Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R § 64.6305(e)(1), Ironclad accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers and Foreign Intermediate Providers. In accordance with 47 C.F.R § 64.6305(e)(2), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), Ironclad accepts calls directly from a Foreign Voice Service Provider or Foreign Intermediate Provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action. Accepting traffic from Gateway Providers. In accordance with 47 C.F.R § 64.6305(e)(3), beginning 90 days after the deadline for filing certifications pursuant to 47 C.F.R § 64.6305(d) (which is April 11, 2023), Ironclad accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD showing that the Gateway Provider has affirmatively submitted its filing and RMP, and (b) has not been de-listed pursuant to an enforcement action.

4. Blocking Calls on a Do-Not-Originate List

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2) and (o)(1)-(4), Ironclad blocks calls purporting to originate from a number on a reasonable Do-Not-Originate (“DNO”) list that is associated with North American Numbering Plan numbers. Ironclad has protocols in place to detect DNO calls and blocks calls that are determined to originate from a DNO number. Ironclad is utilizing the DNO list offered by Somos

5. Analyzing and Monitoring Network Routing Through Ironclad Network

Upon receiving call traffic, Ironclad also analyzes and monitors the call traffic that originates on, terminates to, or routes through Ironclad’s voice network. Consistent with Principle No. 5 of the FCC’s Caller ID Authentication Best Practices, Ironclad monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling. In this regard, Ironclad has in place anti-fraud processes that enable it to, among other things, monitor network usage, identify suspicious network activity (based on call duration, abnormal call patterns, atypical call activity, and subscriber information), receive automatic alerts, investigate traffic to distinguish fraud from honest customer usage, and resolve cases intelligently on a case-by-case basis. When analyzing and monitoring call traffic, if Ironclad discovers call patterns that are consistent with illegal robocalling, Ironclad, after further investigation, takes appropriate action to address such behaviors, which may include working with the originating customer to resolve problematic traffic, blocking the problematic calls and/or terminating the customer’s service.

Ironclad further employs technology that scores calls traversing its network, based on risk scoring data provided by a 3rd party which collects nationwide calling data and operates systems to capture scam and spam calls, to determine the likelihood that each call may be harmful in nature.

Calls that carry high risk of being harmful to the call recipient are blocked from traversing the Ironclad network.

6. Ensuring Foreign Providers Are Not Using Ironclad to Carry or Process High-Volume Illegal Traffic onto the U.S. Network

Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when Ironclad serves as a Gateway Provider for voice traffic that is routing through its network, Ironclad takes reasonable and effective steps discussed under Section 5, above, to ensure that any Foreign Voice Service Provider or Foreign Intermediate Provider from which Ironclad directly receives traffic is not using Ironclad, as a Gateway Provider, to carry or process a *high volume* of illegal traffic onto the U.S. network.

In addition, as a Gateway Provider, Ironclad blocks – to the best of its ability – foreign originating calls with U.S. North American Numbering Plan numbers in the Caller ID, unless the upstream provider has been previously approved for sending such traffic, based on satisfactory due diligence. Furthermore, in the case of such calls, Ironclad will block all calls which are not authenticated, prior to arrival to the Ironclad network, using STIR/SHAKEN.

7. Authenticating Voice Traffic

When operating as a Voice Service Provider, Ironclad does the following (1) authenticates and verifies caller identification information for all SIP calls that exclusively transit its own network; (2) authenticates caller identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifies caller identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.¹⁰

When operating as an Intermediate Provider, Ironclad passes unaltered, any authenticated caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field. With respect to any unauthenticated calls it receives, Ironclad is excused from authenticating such calls as Ironclad participates cooperatively with the industry traceback consortium and responds fully and in a timely manner to all traceback requests it receives from the Commission, laws enforcement, and the industry traceback consortium.¹¹

¹⁰ 47 C.F.R. § 64.6301(a).

¹¹ 47 C.F.R. § 64.6302(b) and (c).

When operating as a Gateway Provider, Ironclad authenticates caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call. ¹¹

8. Responding to Commission, Law Enforcement and ITG Traceback Requests

Ironclad is committed to ensuring that its network is not utilized for the origination, termination or routing of unwanted and illegal robocalls. In accordance with the FCC's regulations 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), Ironclad will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium ("ITG") within-24 hours¹² and will cooperate with such entities in investigating and stopping any illegal robo-callers that attempt to use Ironclad's network to carry or process calls. As part of this commitment, Ironclad will take the necessary steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules.¹³ Ironclad works closely with ITG and typically responds within one hour to ITG traceback requests on average.

9. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Ironclad's network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, Ironclad provides the following name, title, department, business address, telephone number, and email address of the individual within Ironclad that leads Ironclad's team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name: Kasey Skidmore
Contact Title: Chief Operating Officer
Contact City: Portsmouth
Contact State and Zip Code: Virginia 23704
Contact Telephone Number: 757 844 2030
Contact Email: ops@ironcladconnect.com

10. Updating Ironclad's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), Ironclad will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.

¹² This 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission. See FCC 22-37, at n.211

¹³ See 47 C.F.R. § 64.1200(n)(2), (3) & (5)