



ROBOCALL MITIGATION PLAN

CUSTOMER AUTHENTICATION

Grand River Mutual Telephone Corporation dba GRM Networks (“Company”) vets new and renewing customers during its enrollment for service through the request for identification information, including but not limited to: 1) Contact Information; 2) Complete Address; 3) Tax Identification Number; 4) Type of Service; 5) Service Location. This information, when verified against other forms of identification, can identify discrepancies which would prompt additional review.

Company has used the *Best Practices for the Implementation of Call Authentication Frameworks*¹ as a reference for educating its employees on vetting caller identity.

TRACEBACK

Grand River Mutual Telephone Corporation dba GRM Networks commits to responding to all traceback requests from the Federal Communications Commission, civil or criminal law enforcement, and the industry traceback consortium within twenty-four (24) hours; and will cooperate with such entities to investigate and eliminate illegal robocalls originating on its network.

MONITORING AND MITIGATION

Grand River Mutual Telephone Corporation dba GRM Networks vets new and renewing customers at the time of service enrollment to authenticate contact and service location information. All originating telephone numbers are associated with a domestic physical address and responsible party.

Company does not currently use a third-party call analytics vendor. Company utilizes reporting functionality provided by its billing vendor, Innovative Systems, to identify and evaluate abnormal calling patterns within call record details. In the event abnormal calling patterns are detected, Company personnel will contact the responsible party for remediation; and if suspicious activity does not cease, Company may ultimately terminate service.

Company does not block calls to emergency services or from public safety answering points and government emergency numbers.

¹ NANC Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Frameworks*

Company knows all carriers from which it receives traffic (“Upstream Providers”) and has confirmed that all carriers are listed in the Robocall Mitigation Database (“RMD”). Company has also reviewed the connected carriers’ Robocall Mitigation Plans to learn how the carriers monitor their originating traffic to mitigate illegal robocalls. In addition, Company is now incorporating traceback and prohibited traffic language in all contractual agreements with Upstream Providers.

STIR/SHAKEN IMPLEMENTATION

Company is a voice service provider with a STIR/SHAKEN implementation obligation serving end-users. Company is also a voice service provider without a STIR/SHAKEN obligation on the non-Internet Protocol (“non-IP”) portions of its network because that portion of the network relies on technology that cannot initiate, maintain, carry, process, and terminate Session Initiation Protocol (“SIP”) calls.

Company certifies that it has implemented STIR/SHAKEN in the SIP portions of its network. Company has registered with the STI-PA and is using its token to verify calls. Company is partnering with Ribbon Communications as its STI-CA to authenticate calls using the Company’s token. Further, Company asserts that the non-IP portions of its network qualifies for a continued extension of STIR/SHAKEN implementation obligations under 47 CFR §64.6304(d).

47 CFR §64.6304 – Extension of implementation deadline.

(d) Non-IP Networks. Those portions of a voice service provider or gateway provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension.

To meet the non-IP network criteria for the continuing STIR SHAKEN extension (§ 64.6303 (a)(2)), Company is a member of NTCA – The Rural Broadband Association, which has representation serving as a member of a working group participating in industry efforts to develop a non-IP caller ID authentication solution.

Company has not been prohibited from filing in the RMD.

Company asserts that, at any time in the prior two years, it, nor any entity for which it shares common ownership, management, directors, and/or control, has not been the subject of a formal Federal Communications Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description.

Company’s Operating Company Number (OCN) is 1888.

APPENDIX 1
PARENT, PRINCIPALS, AFFILIATES, AND SUBSIDIARIES

Filing Entity: Grand River Mutual Telephone Corporation dba GRM Networks does not have a Parent Company.

Company Name	Relationship to Filing Entity	Type of Company	% Owned by Filing Entity	Managing Control of the Entity
Grand River Communications, Inc. (Company does not offer a voice service)	Subsidiary	Non-Operating	100%	Mitchell Bailey, CEO
Lathrop Telephone Company dba LTC Networks	Subsidiary	ILEC	100%	Mitchell Bailey, CEO
South Central Communications, Inc. dba SCC Networks	Subsidiary	ILEC	100%	Mitchell Bailey, CEO
Mi-Fiber, LLC (Company does not offer a voice service)	Subsidiary of SCC Networks	CLEC	0%	Mitchell Bailey, CEO