

SRVR, LLC
Dba VOLOCALL
Robocall Mitigation Plan
V.2 April 2024

BACKGROUND

The Federal Communications Commission (“FCC” or “Commission”) has adopted rules requiring voice service providers, like SRVR, LLC (“SRVR” or “Company”) to, among other things, file certifications and robocall mitigation plans in the FCC’s Robocall Mitigation Database (“RMD”). 47 CFR § 64.6305.

The FCC Order lists three affirmative obligations for voice service providers: (1) Respond to traceback requests from the Commission, civil and criminal law enforcement, or the Industry Traceback Consortium; (2) Take steps to effectively mitigate illegal traffic when it receives notification of such traffic from the Commission through its enforcement bureau; and (3) implement effective measures to prevent new and current customers from using its network to originate illegal calls.

SRVR, LLC (“SRVR” or “Company”) is a small voice service provider that has not been prohibited from filing a certification in the Robocall Mitigation Database and does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations. SRVR uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

ROBOCALL MITIGATION

1. Caller Identification:

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group, including: checking robocalls, unallocated calls and invalid numbers against a pre-existing Do Not Originate" list; use of reputation scoring (i.e., caller ID analysis/lookup) to determine whether a call likely was executed with malicious intent; block lists; and dynamic traffic analysis.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

We also validate, when possible, that the entity has a legitimate right to use its asserted calling numbers. We use this information to support the attestation level we assign to calls that we originate for that customer.

Our contractual provisions and acceptable user policy with customers prohibit them from initiating illegal robocalls. If we find a customer initiating suspicious robocalls, we warn them to stop. If such traffic continues, then we have the right to terminate or suspend their service, reserving all rights and remedies including injunctive (restraining) relief.

2. Traceback:

All traceback requests will be sent to the Company's underlying carrier for processing. We respond within the allotted time to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Traceback Contact Information

Name	Title	Contact Information
Bogdan Coman	CTO	noc@srvrco.com

3. Take Steps to Mitigate Illegal Traffic

For calls originating from other providers the company relies on mitigation processes instituted by the originating providers. Customer contracts have terms of suspension due to illegal calls, additionally the Company's contracts with underlying carriers have similar terms. In addition, all calls on our network are monitored for calls with missing caller IDs, multiple calls from the same caller ID, call patterns that may indicate illegal calls and can block those calls if deemed illegal.

4. Measures to prevent origination of illegal calls

Know Your Customer:

The Company requires all business customers seeking service to have a physical business location and local contact person.

Telephone Number Validation:

A Letter of Agreement is required prior to porting of any numbers to any of the company's underlying carriers.

Network Monitoring:

The company monitors all calls originating from its own network and will block all calls that do not meet the FCC standards.

Call Blocking:

All calls on our network are monitored for calls with missing caller IDs, multiple calls from the same caller ID, call patterns that may indicate illegal calls and can block those calls if deemed illegal.

5. Acceptable Use Policy

The Company's Terms and Conditions are incorporated in its Service Agreement and is a guide for its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our unlimited calling plans and features.

STIR/SHAKEN IMPLEMENTATION

We have our own STIR/SHAKEN certificate issued by the TransNexus Certification Authority (STI-CA) that we use when authenticating calls that we originate. We have implemented a STIR/SHAKEN solution supplied by our equipment vendors.

CONCLUSION

SRVR, LLC submits this robocall mitigation plan to comply with the Federal Communications Commission's Order (47 CFR § 64.6305; *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023) ("*Sixth Caller ID Authentication Report and Order*")). This plan is a work in progress and we continually evaluate the efficacy of its measures to combat bad actors and we take appropriate steps to improve these measures when needed.