

LREMC Technologies, DBA RIVR Tech ROBOCALL MITIGATION PROGRAM

LREMC Technologies d/b/a RIVR Tech (“RIVR Tech”) does not have an obligation to implement STIR/SHAKEN because it lacks the facilities necessary to implement STIR/SHAKEN. RIVR Tech does not meet the qualifications to obtain an SPC token. 47 CFR § 64.6304.

RIVR Tech has contracted with Momentum to provide numbering for assignment to some of RIVR Tech’s customers. RIVR Tech and Momentum connect via SIP. Momentum has fully implemented STIR/SHAKEN within its network and signs the originating calls on behalf of RIVR Tech’s customers routing on Momentum’s IP network.

RIVR Tech originates calls via SIP connections within its network. RIVR Tech has contracted with Momentum Telecom to sign all SIP calls that originate on its network. Momentum Telecom has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. Momentum Telecom signs the calls originating on the IP portions of RIVR Tech’s network.

Robocall Mitigation Program

All voice traffic that originates on LREMC Technologies, DBA RIVR Tech (“RIVR Tech”)’s network is subject to the following Robocall Mitigation Program.

Call Analytics

RIVR Tech has contracted with **Momentum Telecom** to provide robocall analytics and reputation scoring of our network’s outbound traffic. The vendor uses software to monitor outbound voice traffic in real time and provides detailed reporting identifying if our network originates any calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database or has a poor reputation. RIVR Tech has access to the vendor’s portal and receives notifications about telephone numbers originating suspected illegal robocalls on its network. The software’s identification of suspected illegal robocalls and alerts helps prevent the origination of illegal robocalls.

Investigation

RIVR Tech investigates calls identified by Momentum Telecom as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if RIVR Tech has any other reason to suspect illegal robocalling or spoofing is taking place over its network, RIVR Tech will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Enforcement

Illegal robocalls and fraudulent spoofing are prohibited on our network. If it is determined a RIVR Tech customer is using our network to fraudulently spoof calls or to originate illegal robocalls, RIVR Tech will either warn the customer to stop such practices or terminate their service as allowed per RIVR Tech policy.

Know your Customer

RIVR Tech has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. RIVR Tech thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Residential customers are asked to provide their full name, address (physical and mailing, if different), last four digits of their social security number, date of birth, phone number, email, and establish a security question, and a password. Business customers are asked to provide their full name, address (physical and mailing, if different), tax identification number, phone number, email, and establish a security question, and a password. To initiate an account change, a customer must provide their password or the answer to their security question prior to initiating a change. If the customer is unable to provide that information the customer service representative will call the customer back using the number, they provided at account setup. RIVR Tech also requires a photo ID for all new customers requesting voice service.

Upstream Provider Knowledge

RIVR Tech knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. RIVR monitors all incoming traffic for suspicious call patterns indicative of illegal robocall activity. The connected carriers are made aware of any suspicious or illegal traffic and are notified that, if the traffic does not cease, the calls may be blocked from entering RIVR Tech's network. In addition, incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers.

Role In the Call Chain

RIVR Tech does not have an obligation to implement STIR/SHAKEN because it lacks the facilities necessary to implement STIR/SHAKEN. LREMC does not meet the qualifications to obtain an SPC token. 47 CFR § 64.6304. RIVR Tech is a voice service provider without a STIR/SHAKEN obligation.

Traceback

RIVR Tech commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. RIVR Tech commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours.

Robocall Mitigation Database Eligibility

RIVR Tech has not, within the prior two years, been involved in any recent formal law enforcement or regulatory investigation into suspected unlawful robocalling.

RIVR Tech has not been prohibited from filing in the Robocall Mitigation Database (RMD).