

MRK Software House LTD

Robocall Mitigation Plan

1. KYC (Know your Customer)

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group.

(<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

2. Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

3. STIR/SHAKEN Extensions

We are eligible for and are taking STIR/SHAKEN implementation extension received under 47 CFR §64.6304 because we have fewer than 100,000 voice subscriber lines. All the voice traffic that originates on our network is subject to the robocall mitigation program described below.

4. Robocall Mitigation Program

Traffic within the MRK Software House LTD network is monitored 24/7, and any unexpected traffic is detected and followed up on with the customer. In case of unauthorized or otherwise unexpected traffic, we do have the right to block any traffic until the appropriate customer clarifies it. Our upstream providers have similar measures in place, further ensuring that any illegal and inappropriate activity is detected and addressed.

At this moment, no part of the MRK Software House LTD's existing network is capable of initiating, maintaining, carrying, processing, or terminating interconnected VoIP calls, with a continued transmission of STIR-SHAKEN attestation data.

For services in the United States, MRK Software House LTD works solely with providers who fully meet the requirements for implementing STIR/SHAKEN and other specifications for mitigating Robocalls. MRK Software House LTD requires that all our upstream providers have a robocall mitigation plan in place, including identifying and reporting suspicious call traffic to us. This enables MRK Software House LTD to be fully compliant with the requirements of the Robocall mitigation.