



Dialzilla LLC ROBOCALL MITIGATION PLAN

Below is the Robocall Mitigation Plan filing for **Dialzilla LLC**. This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices. **Dialzilla LLC** has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

Pursuant to 47 C.F.R. § 64.6305 **Dialzilla LLC** submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures

Dialzilla LLC has in place to mitigate illegal robocalls as of August 24, 2025. **Dialzilla LLC** may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time to respond to changes in its business, its capabilities and its needs.

Dialzilla LLC accepts pre tokenized calls. Furthermore, **Dialzilla LLC** is a Voice Service provider for our retail traffic only. We attest all retail traffic that is being dialed through our network with a A attestation if they use our DIDs, a B if they use others DIDs and can show us a bill and the numbers they are using, and a C attestation if they don't provide us with DIDs or a order form but they are all using our PD system or our P1 system. Since we manage their campaigns and know what traffic they are sending. We make sure they are on our platforms otherwise we dont sign random clients traffic at all. Only using our platforms. They are identified by their company name and filling out our kyc. Then we make sure they send us proof they own the DIDs if they dont buy DIDs from us and provide proof we sign with a B otherwise if no proof we sign with a C. We dont sign any traffic coming from outside our software. All traffic that we sign are from our software only others that are sending us traffic we make sure they sign their own traffic. **Dialzilla LLC** is judiciously working to prevent unlawful robocalls from originating on its network while we have implemented the new STIR/SHAKEN authentication architecture. **Dialzilla LLC** ensures rigorous compliance with the STIR/SHAKEN standards and the

Pallone Thune Telecom Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The Company has implemented the following robocall mitigation plan to address unlawful robocall traffic. Dialzilla LLC |1C has enforceable term of ties and/or an acceptable tse policy noted in informed of the upstream providers “Know-Your-Customer” guidelines and have provided them with the necessary KYC documentation they’ve requested that we complete.

Dialzilla LLC follows the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers. This process includes the collection and review of entity-identifying information to confirm that **Dialzilla LLC** has an authenticated relationship with the customer. The Company uses 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.

Dialzilla LLC also validates, when possible, that the entity has a legitimate right to use its asserted calling numbers. The Company uses this information to support the attestation level it assigns to calls that it originates for that customer.

Dialzilla LLC contractual provisions with customers prohibit them from initiating illegal robocalls. If the Company discovers a customer is initiating suspicious robocalls, it warns them to stop. If such traffic continues, then the Company terminates their service. **Dialzilla LLC** requires that upstream providers have a reasonable Robocall Mitigation Plan, including a vetting process for their customers as well as their upstream providers, and that they use call analytics to identify suspicious traffic.

Prior to installing services for new customers, **Dialzilla LLC** takes the following measures to weed out end users that could potentially generate robocall traffic: Our Know-Your-Customer (KYC) confirms the following about its customers:

- Customer’s identity
- Customer’s right to use the telephone number presented on calls
- Service Address
- Authenticated legal campaigns and compliance
- 499 Filer ID
- Robocall Mitigation Plan and RMD #
- FEIN Number
- Customers Tokens

Dialzilla LLC’s contract explicitly prohibits the initiation of illegal robocalls, with immediate termination for non-compliance. When the customer is a business, **Dialzilla LLC** requires Business Incorporation Documents and verifies they have a reputation as a valid business that abides by the law.

Dialzilla LLC will immediately investigate any identified suspicious calls to determine if the caller or upstream provider was attempting to originate or transit unlawful robocalls. If the Company determines that the traffic was likely unlawful, then we warn them to stop sending

such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

Dialzilla LLC will comply fully with all conditions set forth in the FCC'S 2024 Report and Order Mandating the implementation of the STIR/SHAKEN framework, as well as with the Commission's rules and policies more generally.

Dialzilla LLC has designated an individual as a dedicated point of contact for addressing traceback requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. **Dialzilla LLC** will respond promptly to inquiries from the Industry Traceback Group (ITG) within 24 hours.

If **Dialzilla LLC** detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. And take appropriate action.

Appropriate action will

- Suspend and/or terminate client

Dialzilla LLC will provide valid law enforcement and regulatory agencies with the relevant nonproprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated Robocall Mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. We respond within 24 hours 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 the Company's service to originate, carry, or process illegal robocalls.

Dialzilla LLC performs the same mitigation steps for all outbound calls regardless of our role in the call chain for a particular call. **Dialzilla LLC** has not had any agency action or investigation due to suspected unlawful robocalling or investigations.