



Robocall Mitigation Plan

June 2021

1. Introduction - This Robocall Mitigation Plan (RMP) is being provided pursuant to the TRACED Act and the rules adopted by the Commission requiring voice service providers to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol portions of their networks. Since its inception 8 years ago, DialTower's primary objective has been to build and maintain a state-of-the-art platform for users of DialTower services. We have been and continue to be dedicated to guard our network from being used for nefarious or fraudulent purposes. As technology accelerates and changes, so do the abusers of such technology. Our goal is to stay ahead of them to protect our network and our customers. As such, this plan will remain fluid and is subject to revision as warranted.

2. Acceptable Use Policy (AUP) – DialTower's AUP requires the responsible use of our networks, systems, services, websites and products (collectively, "DialTower Services") by our Customers, Customers' end-users and customers, and other users of DialTower Services (collectively, "Users"), and to enable us to provide Users with secure, reliable and productive services.

3. We Know Our Customers - In addition to reviewing and confirming business information such as taxpayer identification, incorporation details, management team, etc. our sales team is trained to ask probing questions to clearly understand the nature of our customers' business. We ask for specific use cases for the nature of their calls. We inquire if they've ever been named in a Telephone Consumer Protection Act (TCPA) lawsuit or received a subpoena resulting from concerns over their traffic. We analyze a month's worth of Call Detail Records to better understand their traffic patterns. We sample the customer's traffic prior to putting them in production and then we may sample it again after they've been placed in production to confirm legitimacy and quality. We also cooperate with our providing carriers regarding allegations and CDR reporting for their monitoring practices.

4. Telephone Number Authorization - DialTower sources its TFNs from well-respected carriers in the US. These carriers also have

restrictions and monitoring in place to ensure that the numbers are being utilized by legitimate enterprises for legitimate purposes. ThinQ is implementing STIR/SHAKEN and will sign all unsigned calls originating from their network. Only calls originating from thinQ provided ANIs and from IP addresses authorized on the assigned customer's account will be signed with attestation level A. Calls originating from non-thinQ ANIs and from verified customers IP addresses will be signed with attestation level B. All International, non-NANPA, and unverifiable phone numbers will be signed with attestation level C. Signed calls entering our network from authorized customers will be passed through with the identity header and signing information of the responsible party. Bandwidth has similar restrictions in place and is compliant with STIR/SHAKEN as well.

5. Monitoring - DialTower monitors metrics and ratios of failure types, quantity, calls per-second, and ANIs originating from multiple sources and complete rates to detect behavior consistent with robocalling.

6. Traceback Activity and Support - DialTower works in lockstep with its carriers, the government, and other industry leaders to advocate for aggressive civil and criminal enforcement and provide call-blocking tools and technology to put consumers in control of their communications. We have implemented processes to ensure all traceback requests and subpoenas are responded to timely and accurately.

7. Blocking - Offensive ANIs flagged by our monitoring metrics will be blacklisted from originating traffic on our network.

8. Plan Update Information - Due to the changing nature of our industry and regulatory requirements, this plan is subject to change at any time and such changes will be communicated as necessary.