

Robocall Mitigation Compliance with TRACED Act

• Telephone Connections

Telephone Connections, voice service providers, (the "Company"), submit this robocall mitigation certification and attached Robocall Mitigation Plan pursuant to Section 64.6305 of the FCC's rules.

STIR/SHAKEN

The Company has fully implemented STIR/SHAKEN. All calls that the Company originates are compliant with Sections 64.6301(a)(1) and (2) of the Commission's rules.

TRACEBACK

The Company commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any robocallers that use our service to originate unlawful robocalls. The Company will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our service to carry, process, or originate robocalls.

ENFORCEMENT

All voice traffic that originates on our network is subject to the attached Robocall Mitigation Plan. The Company has never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program. The Company has not been prohibited by the Commission from filing in the Robocall Mitigation Database.

I, Randy Hobson, submit this certification on behalf of the Company, which has implemented the STIR/SHAKEN authentication framework as indicated in the Robocall Mitigation Database. Pursuant to section 1.16 of the FCC's rules, I certify, under penalty of perjury, that the information and statements contained herein are true and correct to the best of my knowledge and belief.

R. Hobson (signature)

3-30-26 (date)

MITIGATION PROGRAM

As detailed below, Company has taken specific reasonable steps to avoid, the origination, carrying, or processing of illegal robocall traffic. All voice traffic that originates on our network is subject to the below Robocall Mitigation Plan.

The Company monitors its network to identify suspicious traffic patterns, and has implemented anti-spoofing tools on its network to identify and block illegal calls and traffic.

The Company uses tools purchased from trusted third parties including: Somos (from whom

the Company purchases a commercial DNO list) and YouMail Watch Call Detail Record service ("YouMail CDR") (a traffic monitoring service). Based on information the Company receives from ITG, YouMail CDR, Somos and other carrier information, the Company maintains an internal Do Not Originate ("DNO") list. The Company periodically updates its tools and internal DNO list to detect and include invalid phone number formats, area codes,

and unassigned number blocks. The Company also utilizes internal data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

The Company's resellers tend to be small businesses who sell voice services to other small businesses.

The Company's Know Your Customer (KYC) requirements and processes include:

- Limiting a customer's capacity via call per second and/or concurrent session limits;
- Regularly checking call patterns for possible abusive traffic;
- Vetting all new resellers with a combination of electronic and manual verification systems,

credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. The Company severely limits the capabilities of new

resellers until these processes are complete.

The Company examines the identity of its resellers prior to entering into any contract to provide service. The Company does not onboard a reseller if it is unable to verify the reseller's identification. This verification process includes confirmation of business names and addresses, EIN confirmation, confirmation of reseller in secretary of state databases and

website verifications. The Company's resellers are expected to verify their end-users consistent with federal and state robocall mitigation and anti-spoofing laws.

The Company has an Upstream Provider. The Company will confirm that its upstream providers are appropriately listed in the FCC's RMD and have not been delisted pursuant to an enforcement action. The Company works with its resellers to provide information concerning efforts to reduce illegal calls.

The Company's service agreements contain acceptable use and traffic integrity terms that prohibit the use of Company services for illegal purposes. Pursuant to our service agreements,

the Company may terminate services for fraudulent use of our services, for illegal, improper

or unauthorized use of services, and/or for violations of any laws, rules and regulations applicable to the use of Company services. The Company may block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number transiting the Company's networks.

The Company will respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any robocallers that use our network to originate robocalls.

The Company reserves the right to modify and/or supplement this Robocall Mitigation Plan to adapt to risks and to improve the overall effectiveness of our program.