**Broadband Dynamics, LLC Acceptable Use Policy**

This Acceptable Use Policy (“AUP”) describes actions that Broadband Dynamics, LLC (“BBD”) prohibits when any party uses its Services. By ordering or using BBD’s Services, you, the Customer or service recipient, agree to the terms of this AUP. Each Customer must review and comply with this AUP and all applicable laws, but this AUP is not intended to be interpreted as, relied upon, or used as a substitute for legal advice. You agree not to use, and not to encourage or allow any end user or other party to use, BBD’s Services in unlawful or prohibited manners, including, but not limited to, the following:

* Using the Services to engage in any activities that are illegal, abusive, false, fraudulent, deceptive or misleading, or any activity that exploits, harms, or threatens to harm children.
* Engaging in any unsolicited advertising, marketing, or other unlawful activities using the Services, including without limitation, any activities that violate laws applicable to advertising, electronic communications, and telemarketing, including, but not limited to, Section 5 of the FTC Act (15 U.S.C. § 45), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713), the Telemarketing Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108), the Federal Trade Commission Telemarketing Sales Rule (16 C.F.R. § 310 et seq.), the Telephone Consumer Protection Act (47 U.S.C. §§ 227), the Federal Communications Commission regulations (47 C.F.R. 64.1200 et seq.) and orders implementing the Telephone Consumer Protection Act, all federal and state Do Not Call, calling-time, and call-quantity restriction laws and regulations.
* Using BBD’s Services in any way that fails to conform to any applicable industry guidelines and standards, including, without limitation, the CTIA Messaging Principles and Best Practices, Short Code Registry Best Practices and Short Code Monitoring Handbook.
* Attempting to bypass or disable any security mechanism on any of the Services or using the Services in any other manner that poses a security or service risk.
* Reverse-engineering the Services for any improper purpose.
* Using the Services in any manner that may subject BBD or any third party to liability, damages, or danger.
* Launching or facilitating a denial-of-service attack on any of the Services or any other conduct that adversely impacts the availability, reliability, or stability of the Services.
* Transmitting any material that contains viruses, trojan horses, worms or any other malicious or harmful programs.
* Using the Services to receive, send or otherwise process Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996, as amended, unless you have signed a Business Associate Agreement with BBD or your use of the Services fits within an exception for requiring a Business Associate Agreement.
* Using the Services to store or save credit card information, financial account information, social security numbers, or other information that could be used for fraud or identity theft.
* Using the Services to transmit any material that infringes the intellectual property rights or other rights of third parties.
* Using the Services to transmit any material that is libelous, defamatory, discriminatory, or otherwise malicious or harmful to any person or entity.
* Creating a false identity or forged email address or header, or phone number, or otherwise attempting to mislead others as to the identity of the sender or the origin of a message or phone call, including failing to comply with the Truth in Caller ID Act, 47 U.S.C. § 227, and implementing regulations, 47 C.F.R. § 64.1600 et seq., or using the Services to facilitate a one-ring scam, as the FCC has defined that term (*see* Report and Order, GC Docket No. 20-93; rel. Nov. 30, 2020).
* Transmitting any data to or through BBD unless Customer represents and warrants that it has obtained and will maintain all necessary licenses, authorizations, approvals and consents to use, transmit, and process any data to or through BBD during and/or in the use of the Services.

This list of prohibited uses is meant to be illustrative and should not be considered exhaustive. All determinations related to violations of this Acceptable Use Policy will be made by BBD in its sole, reasonable discretion. BBD reserves the right to change or modify the terms of the AUP at any time, effective immediately when posted to the BBD website or when BBD notifies you via an invoice insert. Customer’s use of the BBD Services after changes to the AUP are posted to the BBD website or sent via an invoice insert shall constitute acceptance of any changes or additional terms. If you have a complaint about abuse or a breach of this AUP, please contact a BBD representative.

If you violate these Terms, we may stop providing Services to you or we may close your account. We may

also block delivery of also block delivery of a communication (such as a telephone call or SMS) to or from the Services in an effort to enforce these Terms. You also understand and agree that we are authorized and required to cooperate with and respond to all lawful civil, criminal, and regulatory inquiries relating to your use of the Services, including, without limitation, Traceback and other legal requests or demands from the FCC, FTC, civil and criminal law enforcement, and the FCC-designated USTelecom Industry Traceback Group consortium or any such successor entity. You also understand and agree that, pursuant to your contract with BBD, you agree to defend, indemnify and hold BBD harmless for any claims, demands, suits or proceedings alleging that you have violated the terms of this AUP or your agreement with BBD. When investigating alleged violations of these Terms, BBD reserves the right to review the content of your communications in order to resolve the issue. But we cannot monitor the entire Services, and make no attempt to do so.