

ROBOCALL MITIGATION PLAN
BREVARD WIRELESS, INC. dba FLORIDA HIGH SPEED INTERNET

Brevard Wireless, Inc. dba Florida High Speed Internet ("FLHSI") submits the following Robocall Mitigation Plan, in compliance with 47 CFR § 64.6305(f), describing: (1) the specific reasonable steps FLHSI has taken to prevent new and existing customers from originating illegal robocall traffic; (2) its commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls; and (3) FLHSI's process for updating its robocall mitigation program.

FLHSI provides origination and termination voice service. All calls that originate on its network are subject to a robocall mitigation program. FLHSI has fully implemented STIR/SHAKEN and other robocall mitigation efforts. FLHSI is not a foreign voice service provider. FLHSI does not sell services of international call originators using North American Number Plan Numbers.

Avoiding Originating Illegal Robocalls As Part Of The Robocall Mitigation Program, Know Your Customer Practices, and Monitoring to Block Illegal Traffic

FLHSI has implemented meaningful protections to avoid originating illegal robocalls as part of its robocall mitigation program. For example, FLHSI has established and implemented comprehensive Know Your Customer ("KYC") policies for any new and existing subscribers. The objective of the KYC policy is to prevent FLHSI from being used, intentionally or unintentionally, for spoofed or illegal traffic. As part of FLHSI's KYC procedures, each new and renewing customer are reviewed to ensure they are still eligible to use FLHSI's services. The customer provide the following information (1) a physical business location; (2) a corporate email address; (3) a working phone number; (4) meeting in person; (5) contractual acceptance of FLHSI Acceptable Use Policy

At the outset of initiating FLHSI's services, customers must agree to FLHSI's Acceptable Use Policy, which are designed to combat robocalls before service is deployed. Customers agree that they are responsible for all communications transmitted via their account and FLHSI reserves the right to terminate any and all services if FLHSI believes, in its sole discretion, that the customer has breached any obligation of the AUP. The AUP expressly forbid the customer to use FLHSI's services in a manner that would violate any applicable laws, rules or regulations, including those laws, rules or regulations governing telemarketing, unsolicited calls, and limitations on the use of automated or prerecorded calling technology, including the Telephone Consumer Protection Act, the Federal Trade Commission's Telemarketing Sales Rule, and applicable state laws. FLHSI also reserves the right to impose limits on any customers' usage of its services or to terminate its services, notwithstanding a customer's purchase of an unlimited minute plan, if FLHSI believes, in its sole reasonable

discretion, that such usage, including the total number of calls made and/or minutes used by a customer is not consistent with normal, fair, and reasonable use of FLHSI's services.

Once services are initiated, FLHSI engages in active fraud monitoring on its own network and, as a VoIP provider that relies on underlying providers for PSTN connectivity, works with its underlying service providers to combat robocalls. FLHSI considers the following types of voice calling and text messaging as fraudulent traffic: (1) All traffic deemed invalid per Commission rules; (2) traffic sent with the intent to steal or harm; and (3) traffic sent with the intent to harm through impersonating or masquerading identities. FLHSI reserves the right to protect itself, its networks, and the public, by stopping fraudulent traffic from traversing its networks. FLHSI's customers who send traffic that the telecommunications industry, government authorities, and FLHSI consider to be fraudulent, are at risk of having their traffic blocked—either by FLHSI or any downstream service provider. The following specific types of illegal activities also violate FLHSI's Acceptable Use Policy: (1) unlawful robocalls; (2) domestic toll fraud; (3) international toll fraud; (4) communication that is illegal, exploitative, abusive, harmful, unwanted, deceptive, inappropriate, or objectionable including, content or communications which FLHSI determines (i) is false or inaccurate; (ii) is hateful or encourages hatred or violence against individuals or groups or encourages terrorism or violent extremism; (iii) could endanger public safety, (iv) describes, features or promotes graphic violence and gore, or (v) the sale or promotion of prohibited substances or goods (5) phishing scams (IRS, SSA, vacations, student loans, etc.); and (6) text messaging SPAM. Further, through reports generated by Call Detail Records and pattern trends, fraud information sharing through industry organizations, and third-party notifications and complaints, FLHSI is able to identify and combat potential unlawful robocalling.

FLHSI also employs methods to identify and prevent the origination of illegal traffic, including monitoring traffic volumes and the identification of high cost destinations globally. If traffic is directed towards unusual or suspicious areas, FLHSI may monitor it and promptly alerts and collaborates with customers. Suspicious calls that terminate in such areas are blocked or flagged. When it is confirmed that calls are fraudulent, FLHSI works diligently to shut down these unlawful calls as soon as possible, including the possibility of terminating the customer account associated with the activity.

Know Your Upstream Providers

FLHSI only accepts traffic from providers that at a minimum satisfy the following requirement:

- Accepting traffic from domestic Voice Service Providers only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Foreign Voice Service Providers or Foreign Intermediate Providers that use NANP resources that pertain to the U.S. in the caller ID field to send voice traffic to residential or business subscribers in the U.S., only if that foreign

provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

- Accepting traffic from Gateway Providers only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.
- Accepting traffic from Non-Gateway Intermediate Providers only if that Non-Gateway
- Intermediate Provider's filing (a) appears in the RMD, (b) shows that the Non-Gateway Intermediate Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action

*Commitment To Responding To Traceback Requests & Internal Efforts To Effectuate
Tracebacks To Combat Robocalls*

FLHSI is committed to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

The person within FLHSI responsible for addressing all robocall mitigation-related issues, is: Robert Berlin, VP operations, 321-205-1100, email: rob@flhsi.com

FLHSI also has in place internal traceback procedures. Carriers and service providers are encouraged to send any request for fraud investigation or tracebacks to Fraud team fraud@FLHSI.com. Once such a request has been received, the FLHSI fraud team will open an internal case and gather information associated to the number, including the customer or company name, address, and any information about the business and telephony usage. FLHSI will relay all relevant information back to the carrier or service provider. In the case of proven fraud (or even spam or scam calls), FLHSI will block the number originating the calls or text and, depending on the findings about the customer, also block the customer and terminate its account.

Plan Update Process

FLHSI ensures that its plan is up to date and will apply all required changes to be compliant with Commission requirements.

This Robocall Mitigation Plan describes the specific measures that FLHSI has implemented as of March 2, 2026. FLHSI continually evaluates the efficacy of its measures to combat bad actors and takes appropriate steps to improve these measures when needed.