

**EXHIBIT TO CERTIFICATION OF BRAZOS WIFI
FOR ROBOCALL MITIGATION DATABASE**

To Whom It May Concern:

Indicated below are the robocall mitigation measures employed by Brazos WiFi. Brazos Wifi implements the features on their network and traffic. Brazos WiFi certifies that its software follows required traceback standards. Brazos WiFi will continue to implement new robocall mitigation software measures as they become available.

Methods and Efforts Employed to Avoid Carrying or Processing Illegal Robocalls

- No intermediate “transit” traffic is allowed on our network. Only traffic sourced from customers that treat Provider as its “Provider of Record.”
- All ANIs and DNISs are tracked and documented from customer through vendor delivery, including all voice “hops” and stored for 90-days.
- All originating and termination numbers are profiled by our patented (USPTO 10348584) traffic analytics engine for irregular behavior including, but not limited to:
 - High Volume / Short Duration Traffic
 - Calls with immediate hang ups
 - Calls from numbers that exist on a known robodialer list.
- Automated filtering for both inbound and outbound traffic to our voice network.
- Provider commits to respond fully and in a timely manner 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.
- We conduct a monthly review of our measures in an effort to combat new techniques that scammers use to compromise the PSTN in the US.
- Provider maintains an Acceptable Use Policy (AUP) that subscribers must sign before being permitted to use Provider’s network. Provider’s contractual terms with subscribers specify that Provider may take action up to suspension or termination of service for violation of the AUP. Among other things, the AUP prohibits:
 - providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
 - violating any applicable law;
 - violating applicable industry accepted guidelines; and
 - using Provider’s service to engage in or in connection with fraudulent activities.
- Provider works with its upstream carrier to detect a calling pattern consistent with illegal robocalls. If such a call is detected, Provider will identify the party that is using our network to originate those calls and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party’s ability to originate calls on our network.

Commented [JD1]: The bullet points in this section should be reviewed for accuracy, and anything that is inapplicable should be removed.

- When traffic analysis indicates the presence of likely illegal robocalling, B&B follows certain procedures on investigating such subscribers. The procedures established include but are not limited to:
 - checking recent and past call detail records and benchmark against expected trends;
 - checking recent and past account activity and purchases;
 - investigating if any system issue generates the strange behavior;
 - verifying that the call originating path is valid; and
 - contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.
- New customers requesting an excessive number of call paths will be screened for legitimate call usage needs.
- New and existing customers with an excessive number of call paths shall receive Robocall outreach and education materials.
- Caller ID and call records are reviewed when the service is installed to verify legitimate caller ID information.
- Know Your Customer: Provider has a “Know Your Customer Team” comprised of multiple employees. This team conducts “know your customer” tests before it allows a party to become a new customer. Among other tests, the team will investigate the type of service being sought by the prospective customer and review the potential customer’s website to ensure that it has functional links and is not using fictitious names. Provider’s fraud department also will determine whether potential customers have a concerning number of prior ITG traceback requests and may also reach out directly to contacts throughout the industry to ask whether the prospective customer is problematic. Provider’s Know Your Customer Team will research whether the prospective customer is located overseas (which can be a potential fraud indicator), and whether the FCC or the FTC have sent the prospective customer of individuals associated with the customer letters identifying them as involved in robocalling or spoofing. Additionally, Provider’s fraud department will ensure that a prospective customer is registered in the FCC’s robocall mitigation database (and does not withdraw such registration) if the customer is classified by the FCC as a “service provider.” Any information that is provided to Provider is compared to public information available either on the customer’s website or through other internet-based resources.
- Network Tools: Provider uses the following network tools to combat illegal robocalls:
 - Randomizer: Utilized for customer traffic which is sent to Provider via a Least Cost Routing (“LCR”) engine. Based on calling party telephone number analytics, an announcement is played to the calling party that requires the calling party to enter two randomly generated digits to complete the call. If the correct digits are not entered, the call will not proceed (machine generated calls presumably are unable to enter the randomly generated digits).
 - Automatic Number Identification (“ANI”) Management: Utilized for customer traffic which is sent to Provider via an LCR engine. ANI Management is used to identify and block originating telephone numbers from sending calls that are believed to be unlawful based on repeat attempts to reach the Provider network.

- Proactive Blocking: Applied to all traffic. Per rules adopted by the Commission in FCC 17-151, Provider blocks calls from phone numbers on Do-Not-Originate (“DNO”) lists from US Telecom SOMOS and Neustar. In certain circumstances, Provider also blocks calls that originate from invalid, unallocated, or unused numbers. Provider’s customers may also place certain of the inbound-only telephone numbers they use on the DNO list.
- No Treatment: This treatment is applied to lawful robocalls so that they can complete. Call types include debt collections, political calls, surveys, non-profit, emergency notifications, and other lawful call types.
- Whitelist: Provider “whitelists” telephone numbers that it knows originate legitimate calls (i.e. are valid). For example, some law enforcement and emergency calls originate from numbers where the entire telephone number is composed of zeroes. While appearing to be an unallocated number, Provider knows based on call history that the call is originating from a federal law enforcement agency or a local police department. Such calls also originate from older or misconfigured PBXs (private branch exchanges). Another example would be collection calls by Bank of America or calls to known numbers used for emergency county-wide or municipal alerts.
- Teaming with Others: Provider works with other companies to stop unlawful robocalls. For example, Provider has worked with “YouMail.” From services that YouMail provides to its own customers, YouMail creates a near real-time feed of telephone numbers being used unlawfully (typically associated with the “IRS” or similar scams). Provider then monitors these numbers to take potential action. If Provider recognizes that calls are being carried on its network that are originating from these numbers, then DNO treatment (as described above) will be applied. Provider also regularly works with the Internal Revenue Service directly on complaints.
- Contract Termination: Provider typically has contractual rights that allow it to terminate customers that violate relevant law, including violations of the Telephone Consumer Protection Act. When appropriate, Provider enforces these rights. Subject to applicable laws that may prevent it from doing so, Provider may also terminate accounts if it discovers that any of the entities or individuals associated with a customer account have been named by the FCC or the FTC as an illegal robocaller or have failed to respond to traceback requests. As a gateway provider, Provider does not have a direct relationship with a party that may be originating unlawful robocalls. Accordingly, when Provider suspects it has identified unlawful calling, in addition to taking the steps identified above, it may also contact the party sending Provider the calls (i.e., Provider’s carrier/provider customer), and request that they work to investigate their customers (e.g., to identify the party sending them the calls, determine whether the calls are unlawful, and then to eliminate the source of the calling). At the same time, Provider is aware of the need to balance any blocking and termination efforts with the goal of preventing the blocking of legitimate calls, particularly those that have a bearing on public safety or health (e.g., a school system sending an alert or law enforcement).

Traceback Requests.

Brazos WiFi certifies that its software follows required traceback standards. Brazos WiFi commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, regulators, and the industry traceback consortium.

STIR/SHAKEN Implementation.

Brazos WiFi has implemented STIR/SHAKEN to all egress traffic. STIR (Secure Telephony Identity Revisited) and SHAKEN (Secure Handling of Asserted information using toKENs) is an industry framework that is being developed to prevent the completion of calls where the originating provider does not own or is not authorized to use the Caller ID associated with the call (a “spoofed call”). STIR/SHAKEN uses digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. The expectation is that the certificate technology will enable the called party to verify that the calling number is accurate and that it has not been illegally spoofed.

Commented [JD2]: Everything in the next two sections should be applicable to Brazos WiFi