

Robocalling Mitigation Plan

Effective Date: December 17, 2025

1 Purpose

Brightspeed is committed to protecting its customers against illegal robocalls originating or traversing through our IP and non-IP based networks.

2 Compliance with Regulatory Rules and Framework

- Traffic carried over the Non-IP network: The Federal Communications Commission (FCC) implemented requirements, pursuant to Section 47 C.F.R. §64.6304(d) of the Rules, on a suite of industry standards subsequently adopted, creating an Internet Protocol (IP) call authorization framework. The Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN referenced as STIR/SHAKEN), does not function on portions of a carrier's network that rely on technology that cannot initiate, maintain, and terminate SIP calls ("non-IP calls"). The deadline for implementing STIR/SHAKEN of June 30, 2021, is subject to a continuing extension of the FCC's requirements, provided that a carrier:
 - is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standard group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution¹; and
 - commits to continuing support for establishing an effective solution.

Brightspeed meets each of these conditions. The company is a member of the ATIS PTSC Non-IP Call Authentication Taskforce and has committed to continue to work with the industry toward an effective solution to redress robocalling over the non-IP network.

Type of Extension Claimed: Non-IP Network Extension (§ 64.6305(d))

- Brightspeed claims the continuing extension provided under 47 CFR § 64.6305(d) for portions of its network that rely on Time Division Multiplexing (TDM) or other non

¹ <https://www.a+s.org/commi#ees-forums/ptsc/non-ip-call-authen+ca+on-task-force-members/> (last visited January 29, 2024) including Connect Holding II LLC d/b/a Brightspeed.

IP technologies that cannot initiate, maintain, carry, process, or terminate SIP-based calls.

Basis for Exception: Technological Limitation Due to TDM Infrastructure

- The basis for this extension is that Brightspeed operates a voice network that utilizes non-IP TDM-based switching and transmission equipment, which is inherently incapable of supporting SIP signaling protocols required for STIR/SHAKEN call authentication.
- Due to this technological limitation, Brightspeed is unable to implement STIR/SHAKEN on this portion of its network and is therefore subject to a continuing extension under the rules. As required, the company continues to meet its robocall mitigation obligations under § 64.6303(a) for the non-IP portion of its network.
- Brightspeed actively participates in the industry's collective efforts to develop an appropriate non-IP caller ID authentication solution.

Specifically, Brightspeed is a participant in the ATIS Non-IP Call Authentication Task Force, which is engaged in:

- Establishing technical standards for caller ID authentication over legacy TDM networks;
- Testing and piloting feasible non-IP authentication methods; and
- Collaborating with other providers and equipment vendors to identify a scalable, industry-wide solution.

Brightspeed maintains documentation of its participation and is prepared to provide proof of engagement upon Commission request, consistent with the requirements of § 64.6303(a)(2).

- Traffic carried over the IP network: Brightspeed complies with 47 C.F.R. § 64.6301(a) by deploying the STIR/SHAKEN caller ID authentication framework across the IP portions of its network. For SIP calls that originate on Brightspeed's IP network and are exchanged with other providers, Brightspeed ensures caller ID authentication is performed using its own SPC token and certificate. To facilitate this, Brightspeed utilizes ANI Networks and/or Ribbon Communications as third-party signing providers, in accordance with FCC rules, while retaining full responsibility for attestation decisions and compliance.
- **Industry Traceback Consortium ("ITG"):** Brightspeed is committed to responding fully and within 24 hours to all traceback requests from the FCC, law

enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping illegal robocallers that may use Brightspeed services to originate calls.

- **Call Analytics Systems:** Brightspeed currently operates a Time Division Multiplexing (TDM) network, which lacks the technological infrastructure to support real-time, packet-based analytics systems typically used in IP environments. As a result, Brightspeed does not employ analytics tools to identify and block illegal traffic on its TDM network.
- **Analytics:** While analytics are not currently utilized on the IP portion of the network, Brightspeed continues to evaluate these services for potential future implementation to enhance its robocall mitigation capabilities.
- **Third-Party Analytics Vendors:** Brightspeed does not currently utilize third-party analytics vendors. As the company transitions to IP-based voice infrastructure, it will evaluate available analytics providers to enhance its robocall mitigation capabilities in compliance with FCC requirements.
- **Provider's Role in the Call Chain:** Brightspeed provides Voice Service with a STIR/SHAKEN obligation and Non-Gateway Intermediate Provider without a STIR/SHAKEN obligation roles in the Call Chain.

3 RMD Enforcement Action – Two Year Review

Pursuant to the enforcement-related certification requirements adopted in the Sixth Caller ID Authentication Report and Order (FCC 23-18), Brightspeed, hereby certifies that, to the best of our knowledge, information, and belief, Brightspeed has not been prohibited from filing in the Robocall Mitigation Database pursuant to any law enforcement action, including those described in paragraph 42 of the Sixth Report and Order.

This includes, but is not limited to:

- Instances in which a provider has been removed from the Robocall Mitigation Database and precluded from refiling until certain deficiencies have been cured; and
- Instances in which a provider's authorization to file has been revoked due to continued violations of the Commission's robocall mitigation rules.

For the individual compliance status of Brightspeed's operating companies, please refer to **Attachment B**, Section 1: Subsidiaries (Operating Companies), column titled "RMDB Status."

4 Robocall Mitigation Program

Brightspeed has implemented the robocall mitigation program described below for those portions of its network on which it has not implemented the STIR/SHAKEN authentication framework. This Robocall Mitigation Program applies to both roles in the call chain as identified above.

- i. **Network Monitoring Practices.** Brightspeed, within its non-IP network, will proactively monitor its networks for patterns indicative of illegal robocalls. The company will also coordinate with other major providers, the ITG, trusted third parties, and key federal agencies to address and mitigate obviously fraudulent calls. These efforts include, but are not limited to, coordination with the ITG, implementing industry and government principles (i.e., Do Not Originate and Direct Inward Dial blocking) used to mitigate illegal activities, including one-ring scams, and mass robocalling scam campaigns as identified by a trusted third party. Brightspeed will also conduct additional network-level blocking in response to proper requests from the FCC where the entities that are the subject of such FCC requests have failed to undertake the FCC-directed remedial measures.
- ii. **Know-Your-Customer Initiatives.** Brightspeed will adopt “know-your-customer” initiatives to help mitigate the risk that its customers may attempt to use Brightspeed’s network to initiate an unlawful robocalling campaign. Brightspeed will undertake reasonable, good faith efforts to validate the identity of its customers, particularly smaller customers, that may be more susceptible to identify theft and spoofing of their account by third parties engaged in unlawful robocalling activities. These measures include monitoring of financial position and payment performance, performing required or permitted credit checks, and requiring customers to demonstrate they are a legitimate business entity if they are not a Fortune 500 company or other publicly traded company, a local, state or federal government agency or educational institution. Brightspeed will further ensure the vetting of new residential and business customers by gathering personally identifiable information for additional security on each account before activating new service or making changes to existing services.
- iii. **Know-Your-Upstream-Provider Initiatives.** Brightspeed will adopt “know-your-upstream-provider” initiatives to strengthen the “chain of trust” for all upstream providers from which it accepts traffic and that such providers remain in good standing in the Commission’s robocall mitigation database. We commit to cooperate fully with law enforcement or other sources to identify suspected illegal robocalling traffic originating upstream in accordance with state and federal law. Brightspeed employs reasonable policies and procedures to monitor for instances of illegal calls flowing into Brightspeed’s network and escalates any such activities to our Robocall Mitigation Team for investigation and mitigation efforts.
- iv. **Robocall Mitigation Team (“RMT”).** The RMT is an expert based group tasked in combating illegal spoofed, or scam, robocalls within Brightspeed. The team is sponsored by senior leadership from multiple business disciplines and team members are empowered to implement remedial network-level actions, adapt, or create operational policies, and issue “cease-and-desist” notifications to upstream providers. The team monitors industry progress on development and testing for non-IP solutions and addresses STIR/SHAKEN implementation as the Brightspeed network begins transition to VoIP and/or IP SIP based services. Commission Notices and ITG requests are monitored, and affirmative action executed to identify any feasible mitigation on a case-by-case basis.

- v. **Contractual Terms and Other Conditions.** Brightspeed's service agreements contain acceptable use and traffic integrity terms that prohibit the use of Brightspeed's services for unlawful purposes. Network capacity limitations also serve as a check against customers originating large volumes of calls, which may be indicative of illegal robocalling campaigns. Large and wholesale customers may also be subject to a review of their call counts, minutes, and target rates on a destination-by-destination basis. New and existing customers are also provided industry standard calling party hygiene practices designed to assist in preventing originating calls with invalid or malformed calling party information.
- 4. **State Attorneys General Anti-Robocall Principles.** Brightspeed adopts the foregoing principles, which generally call for voice service providers to implement call blocking technology on residential VoIP and mobile networks, to know their customers, to actively monitor their networks for robocall traffic, and to cooperate in investigations that trace the origins of illegal robocalls. Through these steps, Brightspeed will mitigate illegal robocalls and work cooperatively with State Attorneys General in identifying and prosecuting the bad actors that initiate these illegal calls.
- 5. **Continuing Efforts to Address Unlawful Robocalling.** Brightspeed has taken the specific steps set forth above to avoid originating illegal robocall traffic as part of its robocall mitigation program. Brightspeed will continuously analyze the effectiveness of this program and review best practices in this space. Brightspeed reserves the right to modify and/or supplement its robocall mitigation measures to adapt to risks from bad actors and to improve the overall effectiveness of its program for the benefit of its customers.

Last Update: December 17, 2025

ANTI-ROBOCALL PRINCIPLES

(Attachment A)

State Attorneys General and the undersigned voice service providers are committed to stopping illegal and unwanted robocalls for the American people. Therefore, state Attorneys General have engaged voice service providers to gain their support and assistance in combatting this pervasive problem. These Anti-Robocall Principles are the product of this engagement.

Illegal and unwanted robocalls continue to harm and hassle people every day. Consumer fraud often originates with an illegal call, and robocalls regularly interrupt our daily lives. Robocalls and telemarketing calls are the number one source of consumer complaints at many state Attorneys General offices, as well as at both the Federal Communications Commission and the Federal Trade Commission. State Attorneys General are on the front lines of enforcing do-not-call laws and helping people who are scammed and harassed by these calls.

Through law enforcement and technological developments, respectively, state Attorneys General and voice service providers are working to assist consumers and battle bad actors who scam consumers and intrude upon their lives. By implementing call blocking technology, knowing their customers, actively monitoring their networks for robocall traffic, cooperating in investigations that trace the origins of illegal robocalls, and integrating other practices enumerated in the Anti-Robocall Principles, these voice service providers will aid the state Attorneys General in identifying and prosecuting illegal robocallers.

ANTI-ROBOCALL PRINCIPLES FOR VOICE SERVICE PROVIDERS

The undersigned voice service providers declare that they will work with the undersigned state Attorneys General by incorporating, or continuing to incorporate, these Anti-Robocall Principles into their business practices:

- Principle #1. Offer Free Call Blocking and Labeling.** For smartphone mobile and VoIP residential customers, make available free, easy-to-use call blocking and labeling tools and regularly engage in easily understandable outreach efforts to notify them about these tools. For all types of customers, implement network-level call blocking at no charge. Use best efforts to ensure that all tools offered safeguard customers' personal, proprietary, and location information.
- Principle #2. Implement STIR/SHAKEN.** Implement STIR/SHAKEN call authentication.
- Principle #3. Analyze and Monitor Network Traffic.** Analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls.
- Principle #4. Investigate Suspicious Calls and Calling Patterns.** If a provider detects a pattern consistent with illegal robocalls, or if a provider otherwise has reason to suspect illegal robocalling or spoofing is taking place over its network, seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name, terminating the party's ability to originate, route, or terminate calls on its network, and notifying law enforcement authorities.
- Principle #5. Confirm the Identity of Commercial Customers.** Confirm the identity of new commercial VoIP customers by collecting information such as physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business.
- Principle #6. Require Traceback Cooperation in Contracts.** For all new and renegotiated contracts governing the transport of voice calls, use best efforts to require cooperation in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered its network or by identifying its own customer if the call originated in its network.
- Principle #7. Cooperate in Traceback Investigations.** To allow for timely and comprehensive law enforcement efforts against illegal robocallers, dedicate sufficient resources to provide prompt and complete responses to traceback requests from law enforcement and from USTelecom's Industry Traceback Group. Identify a single point of contact in charge of responding to these traceback requests, and respond to traceback requests as soon as possible.

Principle #8. Communicate with State Attorneys General. Communicate and cooperate with state Attorneys General about recognized scams and trends in illegal robocalling. Due to the ever-changing nature of technology, update the state Attorneys General about potential additional solutions for combatting illegal robocalls.

DEFINITIONS OF TERMS IN ANTI-ROBOCALL PRINCIPLES

The following terms are used in the attached set of Principles:

- **CALL AUTHENTICATION:** Call authentication allows a voice service provider to cryptographically sign call signaling information and allows the intermediate and destination providers to validate the signature. Call authentication prevents a caller from disguising its true identity and/or call origination. Call authentication is provided by a set of standards called STIR/SHAKEN, which specifies this functionality for Voice over Internet Protocol (“VoIP”) calls.
- **CALL BLOCKING:** Call blocking consists of technologies or devices that can stop illegal robocalls before they reach the called party. Call blocking can be implemented by various means on a voice service provider’s network or can be activated by the consumer through software applications or other devices or services.
- **CALL BLOCKING TOOLS:** Call blocking tools are devices, software applications, or services that may be pre-installed, downloaded, enabled, or manually programmed for individual use by consumers. Call blocking tools may be offered directly by the provider or made available through third parties.
- **CALL LABELING:** Call labeling passes additional information about an incoming call to the called party beyond the caller’s telephone number and caller ID name. It is typically displayed on the landline caller ID display or the mobile device screen. The information may display something like “spam” or “fraud alert” in text, or it may suggest the likelihood of an unwanted call by color, score, or image. The information may be provided by the voice service provider or by third-party software and services.
- **NETWORK-LEVEL CALL BLOCKING:** Network-level call blocking by the voice service provider stops calls from reaching a consumer’s landline or cellular telephone device without the consumer taking any steps to activate, request, opt-in, opt-out, or enable the blocking.
- **SHAKEN:** Signature-based Handling of Asserted information using toKENs. SHAKEN is an industry standard that defines how voice service providers should implement the STIR technology to ensure that outbound or originating calling party numbers are not illegally spoofed.
- **STIR:** Secure Telephony Intity Revisited. STIR is the name of a standardization working group and is commonly used to label the technology that adds cryptographic signatures to call signaling requests. This technology prevents a caller from providing a calling number to the receiving party that the caller is not authorized to use.

DEFINITIONS OF TERMS (*continued*)

- **STIR/SHAKEN:** STIR/SHAKEN describes a set of technical standards and operating procedures for implementing call authentication for calls carried over an Internet Protocol network. The STIR/SHAKEN framework will enable originating voice service providers to attest to the validity of asserted caller IDs and sign outbound calls with a secure signature or certificate that cannot be faked. The terminating service provider will use the security certificate to validate that the caller ID attestation has not been compromised.
- **TRACEBACK:** Traceback is the process of determining the origin of a call, typically by starting with the receiving party and terminating voice service provider and tracing backwards through the path of the intermediate providers and, ultimately, to the originating voice service provider and the origin of the call. Traceback can be used to find the source of robocalls and, thus, the entities responsible for those calls.
- **VoIP:** Voice over Internet Protocol. VoIP carries voice telephone calls over Internet Protocol networks, either within and between voice service providers or to the end customer.

DISCLAIMER

Failure to adhere to these principles is not in itself a basis for liability nor does adherence to these principles protect or release any party from liability. Compliance with these principles does not relieve any party from its duty to comply with state or federal laws and regulations. Adherence to these principles may take time for the voice service providers to plan for and implement.

AGREED to and SUPPORTED by the undersigned state Attorneys General and voice service providers:

AT&T Services, Inc.

Bandwidth Inc.

CenturyLink

Charter Communications, Inc.

Comcast

Consolidated Communications, Inc.

Frontier Communications Corporation

Shentel

Sprint

T-Mobile USA

Twilio, Inc.

U.S. Cellular

Verizon

Wabash Communications

Windstream Services, LLC

JOSHUA H. STEIN
Attorney General
State of North Carolina

GORDON J. MACDONALD
Attorney General
State of New Hampshire

CURTIS T. HILL, JR.
Attorney General
State of Indiana

STEVE MARSHALL
Attorney General
State of Alabama

KEVIN G. CLARKSON
Attorney General
State of Alaska

MARK BRNOVICH
Attorney General
State of Arizona

LESLIE RUTLEDGE
Attorney General
State of Arkansas

XAVIER BECERRA
Attorney General
State of California

PHIL WEISER
Attorney General
State of Colorado

WILLIAM TONG
Attorney General
State of Connecticut

KATHLEEN JENNINGS
Attorney General
State of Delaware

KARL A. RACINE
Attorney General
District of Columbia

ASHLEY MOODY
Attorney General
State of Florida
CLARE E.

CHRISTOPHER M. CARR
Attorney General
State of Georgia

CONNORS
Attorney General
State of Hawaii

LAWRENCE G. WASDEN
Attorney General
State of Idaho

KWAME RAOUL
Attorney General
State of Illinois

TOM MILLER
Attorney General
State of Iowa

DEREK SCHMIDT
Attorney General
State of Kansas

ANDY BESHEAR
Attorney General
Commonwealth of Kentucky

JEFF LANDRY
Attorney General
State of Louisiana

AARON M. FREY
Attorney General
State of Maine

BRIAN E. FROSH
Attorney General
State of Maryland

MAURA HEALEY
Attorney General
Commonwealth of Massachusetts

DANA NESSEL
Attorney General
State of Michigan

KEITH ELLISON
Attorney General
State of Minnesota

JIM HOOD
Attorney General
State of Mississippi

ERIC S. SCHMITT
Attorney General
State of Missouri

TIM FOX
Attorney General
State of Montana

DOUGLAS PETERSON
Attorney General
State of Nebraska

AARON D. FORD
Attorney General
State of Nevada

GURBIR S. GREWAL
Attorney General
State of New Jersey

HECTOR BALDERAS
Attorney General
State of New Mexico

LETITIA A. JAMES
Attorney General
State of New York

WAYNE STENEHJEM
Attorney General
State of North Dakota

DAVE YOST
Attorney General
State of Ohio

MIKE HUNTER
Attorney General
State of Oklahoma

ELLEN F. ROSENBLUM
Attorney General
State of Oregon

JOSH SHAPIRO
Attorney General
Commonwealth of
Pennsylvania

PETER F. NERONHA
Attorney General
State of Rhode Island

ALAN WILSON
Attorney General
State of South Carolina

JASON R. RAVNSBORG
Attorney General
State of South Dakota

HERBERT H. SLATERY
III
Attorney General
State of Tennessee

KEN PAXTON
Attorney General
State of Texas

SEAN D. REYES
Attorney General
State of Utah

T.J. DONOVAN
Attorney General
State of Vermont

MARK R. HERRING
Attorney General
Commonwealth of Virginia

ROBERT W. FERGUSON
Attorney General
State of Washington

PATRICK MORRISEY
Attorney General
State of West Virginia

JOSHUA L. KAUL
Attorney General
State of Wisconsin

BRIDGET HILL
Attorney General
State of Wyoming

Attachment B: Disclosure of Corporate Structure and Control for Connect Holding II LLC
(d/b/a Brightspeed)

Filing Entity:

Connect Holding II LLC (d/b/a Brightspeed)

Headquarters: 1120 South Tryon Street Suite 700, Charlotte, North Carolina

1 Parent Companies

- Connect Holding LLC: Direct parent of Connect Holding II LLC.
- Apollo Global Management, Inc.: Ultimate controlling entity via funds managed by affiliates of Apollo.
- Mubadala Investment Company: Minority stakeholder via investment in Brightspeed.

FRN	Registrant	Services Provided
31304405	Connect Holding, LLC	Voice/ISP
32802472	Connect Holding II, LLC	Voice/ISP

2 Principals Exercising Management or Control

Name	Title	Role
Michel Combes	Executive Chair and CEO	Executive control over day-to-day operations
Jacky Wu	President, Finance, Technology and Operations	Financial oversight, strategic planning, and Operations
Sorabh Saxena	Chief Information Officer	Technology and systems leadership
Jeff Lowney	President, Business Group	Business unit leadership
Colon McLean	Chief People and Administrative Officer	Organizational and personnel management and legal operations
Marge Jackson	Executive Vice President, Consumer Growth, Sales & Customer Care	Sales and Customer Care
Rui Costa	Executive Vice President, Consumer Products, Marketing & Customer Experience	Consumer marketing oversight, strategic planning
Kristy Harrison	Executive Vice President Operations	Network Operations, Engineering, Field Operations
Daniel McCullough	Executive Vice President, Chief Financial Officer	Financial oversight and strategic planning

3 Subsidiaries (OperaMng Companies)

FRN	Registrant	Services	RMD Status
		Provided	
1677541	Brightspeed of Northern Texas, Inc.	Voice Services	Not Prohibited
1685148	Brightspeed of Texas, Inc.	Voice Services	Not Prohibited
1685429	Brightspeed of Coastal Texas, Inc.	Voice Services	Not Prohibited
1712751	Brightspeed of Southern Texas, Inc.	Voice Services	Not Prohibited
1730886	Brightspeed of Arkansas, LLC	Voice Services	Not Prohibited
1732338	Brightspeed of Northern Arkansas, LLC	Voice Services	Not Prohibited
1743541	Brightspeed of Mississippi, LLC	Voice Services	Not Prohibited
1748466	Brightspeed of Southern Indiana, LLC	Voice Services	Not Prohibited
1768449	Brightspeed of Southern Tennessee, LLC	Voice Services	Not Prohibited
1770122	Brightspeed of Appalachia, LLC	Voice Services	Not Prohibited
1772482	Brightspeed of Eastern Tennessee, LLC	Voice Services	Not Prohibited
1773811	Brightspeed of Western Tennessee, LLC	Voice Services	Not Prohibited
1777036	Brightspeed of South Carolina, LLC	Voice Services	Not Prohibited
1952340	Brightspeed of Eastern North Carolina, LLC	Voice Services	Not Prohibited
2337244	Brightspeed of West Missouri, LLC	Voice Services	Not Prohibited
2342038	Brightspeed of Kansas, LLC	Voice Services	Not Prohibited

2382570	Brightspeed of North Carolina, LLC	Voice Services	Not Prohibited
2390326	Brightspeed of Wisconsin, LLC	Voice Services	Not Prohibited
2595247	Brightspeed of Eastern Kansas, LLC	Voice Services	Not Prohibited
2767283	Brightspeed of Central Michigan, Inc.	Voice Services	Not Prohibited
2774487	Brightspeed of Michigan, Inc.	Voice Services	Not Prohibited
2853711	Brightspeed of Ohio, Inc.	Voice Services	Not Prohibited
2901551	Brightspeed of Indiana, LLC	Voice Services	Not Prohibited
2938843	Brightspeed of Northcentral Ohio, Inc.	Voice Services	Not Prohibited
3936952	Brightspeed of Central Indiana, LLC	Voice Services	Not Prohibited
4085080	Brightspeed of Eastern Wisconsin, LLC	Voice Services	Not Prohibited
4085098	Brightspeed of Northeastern Wisconsin, LLC	Voice Services	Not Prohibited
4140422	Brightspeed of Pennsylvania, LLC	Voice Services	Not Prohibited
4146585	Brightspeed of New Jersey, Inc.	Voice Services	Not Prohibited
4183919	Brightspeed of Virginia, LLC	Voice Services	Not Prohibited
4253373	Brightspeed of East Missouri, LLC	Voice Services	Not Prohibited
4253381	Brightspeed of Central Arkansas, LLC	Voice Services	Not Prohibited
4312153	Brightspeed of South Arkansas, LLC	Voice Services	Not Prohibited
4312211	Brightspeed of South Central Arkansas, LLC	Voice Services	Not Prohibited
4312229	Brightspeed of Central Wisconsin, LLC	Voice Services	Not Prohibited
4312245	Brightspeed of Northern Michigan, Inc.	Voice Services	Not Prohibited
4333688	Brightspeed of Georgia, LLC	Voice Services	Not Prohibited
4333753	Brightspeed of Southern Alabama, LLC	Voice Services	Not Prohibited
4333779	Brightspeed of Illinois, LLC	Voice Services	Not Prohibited
4333795	Brightspeed of Central North Carolina, LLC	Voice Services	Not Prohibited
4547006	Brightspeed of Western Wisconsin, LLC	Voice Services	Not Prohibited
4547014	Brightspeed of Southern Wisconsin, LLC	Voice Services	Not Prohibited
4547022	Brightspeed of Northwest Wisconsin, LLC	Voice Services	Not Prohibited
4547048	Brightspeed of Northern Wisconsin, LLC	Voice Services	Not Prohibited
4547055	Brightspeed of Midwest Wisconsin, LLC	Voice Services	Not Prohibited
4547071	Brightspeed of East Central Wisconsin, LLC	Voice Services	Not Prohibited
4547089	Brightspeed of North Central Wisconsin, LLC	Voice Services	Not Prohibited
4547295	Brightspeed of Northwest Arkansas, LLC	Voice Services	Not Prohibited
5051743	Brightspeed of Southern Kansas, Inc.	Voice Services	Not Prohibited
5051768	Brightspeed of Eastern Texas, Inc.	Voice Services	Not Prohibited
5786223	Brightspeed of Louisiana, LLC	Voice Services	Not Prohibited
5827712	Brightspeed of Alabama, LLC	Voice Services	Not Prohibited
5827787	Brightspeed of Missouri, LLC	Voice Services	Not Prohibited
6160741	Brightspeed of Upper Michigan, Inc.	Voice Services	Not Prohibited
31310576	Connect Parent Corporation	Voice Services	Not Prohibited
32802472	Connect Holding II LLC	Voice/ISP	Not Prohibited
33713272	Brightspeed Broadband, LLC	Residential ISP	Not Prohibited

4 Affiliates

- Apollo Global Management portfolio companies that may share operational, administrative, or advisory connections but are not directly involved in telecommunications.
- Embark Corporation: A legacy entity incorporated into Brightspeed operations.
- Brightspeed-related holding and shell entities used for corporate structure and financial purposes (e.g., Connect Holding, Connect Holding II).