

Updated Policy and Background Effective 02.25.2025

The company is a reseller only (no facilities or soft switches) of various voice communications services and relies on the underlying carriers from whom services are procured to route traffic. The company does not route, assist in routing, originate or terminate any voice traffic whatsoever, nor does the company operate an IP network over which calls are routed.

The company does not knowingly or willingly engage with any customer whose business involves Robocall traffic origination. This is a serious issue; QuantumShift is committed to protect consumers from unwanted, illegal and annoyance-type phone calls. Full vetting of prospective business clients (no residential clients served) is undertaken early on when prospecting and discussing services. Measures taken include verifying the identity of the individual responsible for making decisions related to the company's telecommunications needs, and gathering information such as contact name, e-mail address, telephone number, and business location address. Customers are subject to the company's credit verification procedures. The company additionally undertakes a "Buyers' Journey" with its prospective customers for purpose of comprehensive analysis of their technology needs, which includes call patterns and usage data and an audit of customers' and prospects' existing telecommunications environments. While the company does resell voice services, such as POTS lines and POTS alternative solutions, the company's main stronghold as a reseller is within the IP and software space (e.g., Dedicated Internet circuits, broadband, and its proprietary software platform). The company oftentimes undergoes a thorough and lengthy due diligence process which entail vendor questionnaires prior to a client formally engaging with the company. It is the company's position that such due diligence, coupled with audits of clients' existing environments and the Buyers' Journey further enhances the robustness of the company-client relationship by ensuring each party has the opportunity to thoroughly vet one another's practices, particularly in the areas of data integrity and security policies, and gain a comprehensive understanding of customer usage trends.

Over the last two (2) years, the company's resell of traditional TDM-based technologies has notably decreased, and it is anticipated this trend will continue into the foreseeable future as underlying carriers continually close central offices and retire switches. As a result, the company continues to support its client base in transferring to alternate technologies, which often includes IP-based services. Additionally, fraud monitoring contractual language is in the company's agreements with underlying carrier partners.

Monitoring

Although the company does not have facilities or a network upon which throttling or verifying voice traffic is possible, the company receives monthly Call Detail Records (CDRs) from its underlying facilities-based partners (i.e., the incumbent local exchange carrier in a particular location), to assist the company in facilitating billing its end user customers. The company uses such CDR data not only to bill end users, but to track and monitor trends which would alert it to potential or suspected fraud or Robocalling activity. The company has a dedicated billing, cost assurance, and software development team who regularly come into contact with and review this data.

The company attests it will cooperate in all aspects of any investigation pertaining to any of its downstream end customers with respect to suspected Robocalling activity, up to and including issuing notifications to any to underlying service provider to suspend service if necessary.

The company attests it does (and will continue) to regularly monitor the Robocall Mitigation Database for purpose of ensuring its downstream vendors responsible for providing access to voice services are in compliance with WC Docket No. 17-97 and any subsequent rulings, and it will not knowingly engage in business relationships with any voice service provider not in compliance, or one that is not in the Database.

Traceback

The company is committed to responding and cooperating with any traceback requests it may receive from law enforcement agencies, the Federal Communications Commission, and the Registered Traceback Consortium, and

shall cooperate with any such entities in investigating any Robocalling activities. The company and its customers are contractually bound to one another with regard to cooperation in Traceback requests; language to that effect is in each service order the company's customer signs when procuring voice services.

Jenna Brown

VP, Compliance & Contract Management

February 25, 2025