Cloud Communication providers may offer similar services that seem the same. The reality is many do not provide the same level of Security and Compliance you should expect from a cloud provider. In this time of constant attacks and ransomware events, it is critical that your organization determine if your provider meets the leading industry requirements for compliance and security. Phoneware and our upstream service provider Saddleback Communications have the implemented the industry's highest level of compliance and security standards to protect our customers.

We see your business basically as an extension of our own business. Uptime and protection of data are our top priority. To this end we have implemented the industry highest compliance standards to protect our customers, their data and telecommunications integrity.

COMPLIANCE – Phoneware and Saddleback Communications are fully compliant with the following requirements:

- **HIPAA -** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
- **CPNI -** The Federal Communications Act and the FCC's rules require telecommunications interconnected providers of Voice over Internet Protocol (VoIP) services, to protect "customer proprietary network information," or CPNI. CPNI includes some of the most sensitive personal information that carriers and providers have about their customers as a result of their business relationship (*e.g.*, phone numbers called; the frequency, duration, and timing of such calls). To protect consumer privacy, the FCC rules require carriers/providers to file reports, annually, to certify their compliance with the CPNI rules.
- **PCI DSS -** The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card companies The Payment Card Industry Security Standards Council (PCI SSC) manages the ongoing evolution of the Payment Card Industry (PCI) security standards with a focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands.
- **SOC 1, 2 -** SOC 1 report is designed to address internal controls over financial reporting. SOC 2 report addresses a service organization's controls that are relevant to their operations and compliance. There are five main principles of SOC2 Compliance; these are. 1 – Security Including two-factor authentication, intrusion detection, network and application firewalls. 2 – Privacy Access control, encryption, two-factor authentication. 3- Confidentiality Encryption, access control, network and application firewalls. 4 – Process Integrity Quality Assurance, process monitoring 5 – Availability Security Incident Management, Disaster Recovery, Performance Monitoring.
- **ISO 7001** - The ISO certification validates whether a set of specific standards and requirements are being met, or not. This certification outlines different requirements for the maintenance, implementation, and establishment of an information security management system. It considers future improvements, along with data handling and assessment of information security risks that matter on an organizational basis.

- **NIST 800-53** - NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology. This is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Modernization Act of 2014 (FISMA) and to help with managing cost effective programs to protect their information and information systems

SECURITY – Phoneware and Saddleback Communications have gone to great lengths to ensure the greatest possible security of our networks:

- **Metaswitch SBCs** – Phoneware and Saddleback Communications have deployed geo-redundant Metaswitch Perimeta Session Border Controllers (SBCs). Among Perimeta's many functions, they are inherently configured with Fraud protection capabilities that block the majority of fraudulent Session Initiation Protocol (SIP) User Agents at the edge of the Voice Network, before they ever get to the Metaswitch softswitch. Metaswitch uses SRTP/AES and TLS with SHA 256 for Encryption and when operated in FIPS Mode, these SBC's meet the FIPS 140-2 standard required for NIST. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3657
- **Arbor DDoS Protection** – Phoneware and Saddleback Communications have deployed Arbor Edge Defense (AED). These inline security appliances are deployed at the network perimeter between the internet router and firewall, to protect the network from DDoS and other attacks.
- **Palo Alto Firewalls** – In 2019, Phoneware and Saddleback Communications upgraded to Palo Alto Networks Firewalls at their Data Centers and in their Central Offices, protecting the core network and UCaaS over-the-top services. These are the highest rated firewalls in the industry; in 2019 they were named a leader in the Gartner Magic Quadrant for Network Firewalls for the 8th consecutive year.
- **Redshift Networks UCTM** – Redshift Networks is a carrier-grade VoIP/SIP security, threat intelligence analytics and Fraud-detection technology. RedShift's Unified Communications Threat Management (UCTM) solution provides Phoneware and Saddleback Communications with a Defense in Depth (DID) security architecture to protect against VoIP and SIP security attacks. UCTM provides real-time visibility into Phoneware and Saddleback Communications' VoIP network, enabling the carrier to immediately detect and automatically mitigate security attacks and fraudulent events. UCTM also helps Phoneware and Saddleback Communications protect its customers from Toll Fraud, confidential information compromise and telephony Denial of Service (DoS) threats.
- **Toll Fraud Prevention** – Phoneware and Saddleback Communications have additional customized programs that help detect and automatically block potential Toll Fraud. This includes international Toll Fraud, domestic Toll Fraud, SIP PS Brute force attacks and Comm Portal brute force attacks.

Phoneware and Saddleback Communications leverage national geographic dispersed datacenters to provide our solution in a Geo-Redundant manner to ensure the highest level of redundancy and uptime. CPNI verification can be found on the FCC web site: https://apps.fcc.gov/eb/CPNI/

PCI attestation and HIPAA Business Associates Agreements can be provided as required. Datacenters SOC reports can be provided to attest to the highest level of industry security available per request.

HIPAA compliant and provides Business Associate Agreements for Covered Entities and Business Associates.

Compliant with FCC requirements for protecting Consumer Proprietary Network Information.

An information security standard for validation of controls around cardholder data to reduce credit card fraud.

Our data centers complete the SSAE 16 SOC1 and SOC2 type II audits with a nationally recognized accounting firm.

Internationally recognized best practice framework for an information security management system.

U.S. Gov. security and privacy controls requirements for the transmission, storage, and processing of information