



10.23.2024

Robocall Mitigation Plan

The Maynard Group is committed to combating Robocalling and other forms of telecommunications fraud. We take responsibility for technology and services that we provide and want to ensure a safe and secure system for our customers and those they communicate with.

Specific Steps to Avoid Illegal Robocall Traffic:

- **Customer Vetting Process:**
 - Our market segment consists of mainly commercial clients. This allows us to ensure that we are only entering business relationships with legal business entities. We research each potential client ensuring they are a legally registered business entity and any information related to address, phone numbers and any other contact information is accurate and up to date.
 - Each potential client is personally contacted and evaluated to ensure that we have a clear understanding of their telecommunication needs and how we can best meet those needs. By doing so we can understand how our telecommunications systems will be used and to help ensure no illegal activity will be taking place.
- **STIR/SHAKEN Implementation and Monitoring:**
 - All originating traffic, be it local, long distance, or international, is routed through upstream carriers which have implemented STIR/SHAKEN call authentication protocols. We monitor our traffic for proper attestation levels and take action if anomalies are detected.
- **Traffic Monitoring and Analysis:**
 - The PBXs that we manage channel and trunk limitations so any over utilization results in failure to pass any calls on. As over utilization is approached we are notified of the event and we can take action to investigate.
 - To investigate we will search Call Detail Records on the PBX itself or if not available we can gather the data from Billing Detail Records from the upstream provider. We can then determine the Calling Party, the Called Party, and timestamps of the calls to determine if the calls were likely made from a robotic source.
 - These PBX's are typically NEC, Avaya, Mitel, Cisco, Zoom, Enswitch, BiCOM and 3CX.
- **Traceback Cooperation:**





- We promptly respond to traceback requests from the FCC, law enforcement, or the Industry Traceback Group to identify and mitigate sources of illegal robocalls.

Compliance with "Know Your Customer" Obligations:

- **Customer Due Diligence:**
 - We perform due diligence on all new and existing customers, including verifying their business legitimacy, contact information, and intended use of our services.
- **Upstream Provider Vetting:**
 - We carefully select and partner with reputable upstream carriers who have demonstrated a commitment to robocall mitigation and have implemented robust call authentication measures.
 - The Upstream Providers that we use are VoIP Innovations, Bandwidth, and Telnyx
- **Ongoing Monitoring:**
 - We continuously monitor customer and upstream provider activity for any signs of suspicious or illegal traffic.

Analytics Systems for Identifying and Blocking Illegal Traffic:

- **Internal Monitoring Tools:**
 - We utilize a combination of internal Call Detail Record (CDR) analysis from the PBX or Upstream Providers; server resource utilization tools native to the software of Operating Systems; and network monitoring tools to detect unusual calling patterns, high volumes of calls, and other indicators of potential robocalling activity.
- **Upstream Provider Tools:**
 - Upstream providers provide us with a variety of tools to limit and notify us based on the traffic we provide. VoIP Innovations and Bandwidth are able to automatically block traffic that exceed specified parameters we deem suspicious.
- **Third-party Analytics Systems:**
 - The Maynard Group does not currently utilize any third-party analytics tools beyond those provided by our upstream providers.
- **Blocking Illegal Traffic:**
 - We will block illegal traffic by deactivating individual extensions, tenants or systems.
 - We may also take the step of removing the offending entities access to trunks that allow outbound traffic.
 - If the source is illicitly accessing our system resources from outside our network we will also block their IP address.

Traceback:

- As part of our dedication to the mitigation of robocalling and toll fraud, we will respond to any traceback requests made from the FCC, law enforcement, or the Industry Traceback Group in a timely manner. When notified of any occurrences of robocalling or toll fraud on our network, we will take immediate action to prevent any further violations.





By implementing these comprehensive measures, The Maynard Group, aims to proactively prevent illegal robocalls, protect our customers, and contribute to a safer and more secure telecommunications environment.

