



Tele Fusion Network Inc operates as a VoIP service provider, specializing in facilitating Business-to-Business (B2B) communications. We exclusively cater to corporate clientele, offering a range of Voice over Internet Protocol (VoIP) solutions and services. Our primary focus is on serving businesses, providing them with reliable and efficient telecommunications infrastructure to support their operations and communication needs.

A Robocall Mitigation Program is a set of strategies, technologies, and policies designed to reduce the volume of unwanted and potentially harmful automated phone calls, commonly known as robocalls. Below is a description of our program in respect of Robocall Mitigation:

Knowing our Customer:

For every customer, it is mandatory to furnish a physical business address, along with official business registration documentation. Additionally, we require the name and contact details of at least one accountable individual associated with the business. A crucial prerequisite is that the business must maintain an online presence through a dedicated website, and the provided contact email address must correspond to the business domain. Our services are open to businesses registered in any country worldwide.

Payment for our services is exclusively accepted via bank transfer. We meticulously cross-check and verify all submitted information to ensure compliance and legitimacy. We reserve the right to decline service to any customer presenting suspicious or questionable credentials.

Call Authentication Protocols:

Implementing call authentication protocols like STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using tokens) to verify the legitimacy of incoming calls. This technology allows phone carriers to verify that the caller ID information hasn't been spoofed.

Caller ID Verification:

Implementing systems that verify caller ID information against authenticated databases to detect and block spoofed or illegitimate caller IDs.

Call Blocking and Filtering:

Utilizing call blocking and filtering technologies to identify and block known robocall numbers, spam patterns, and suspicious calling behavior. This can involve using blacklists, whitelists, and algorithms that analyze call patterns to identify potential robocalls.



Call Diagnostic Report Analysis:

We conduct weekly assessments of each customer's traffic, analyzing various metrics such as the number of call attempts, answer seizure ratio, average call duration, and the fraction of calls shorter than 60 seconds. Our aim is to identify any indications of automated dialing and significant deviations from the customer's typical usage patterns.

Upon detecting anomalies in the traffic data, we promptly engage with the customer to seek a comprehensive explanation. Failure to provide a satisfactory resolution within 7 business days leads to the suspension of the customer's service. This proactive approach ensures the integrity and security of our services while maintaining transparency and accountability with our clientele.

Partnerships and Collaboration:

Collaborating with other stakeholders in the telecommunications industry, law enforcement agencies, government regulators, and technology vendors to share information, coordinate efforts, and develop best practices for combating robocalls.

Traceback Request:

We are committed to promptly addressing all traceback requests. Upon receiving a traceback request, we initiate a thorough analysis of the initiating customer's Call Detail Records (CDRs) for the preceding 30 days. This analysis allows us to identify any irregularities or discrepancies. Subsequently, we engage with the customer to provide a detailed explanation of any anomalies found in the CDRs, as well as addressing the specific traceback example. If a satisfactory explanation is not received within 72 hours, the customer's service is suspended as a precautionary measure.

Furthermore, if a customer becomes the subject of three traceback requests within a span of 90 days, they are permanently banned from our platform, unless the traceback examples are unequivocally demonstrated to be legal and compliant with our policies and regulations. This stringent approach underscores our commitment to maintaining the integrity and security of our services.

Continuous Monitoring and Improvement:

Continuously monitoring robocall activity and adapting mitigation strategies to address emerging threats and evolving tactics used by robocallers.

Legal and Enforcement Actions:

Supporting legal and enforcement actions against robocallers, including civil penalties, criminal prosecutions, and coordination with law enforcement agencies to disrupt robocall operations.