

onecom

Robocall Mitigation Plan

Robocall Mitigation Plan

This Robocall Mitigation Plan has been developed to demonstrate our commitment to preventing illegal and fraudulent robocalls, in accordance with the applicable regulations set forth by the Federal Communications Commission (FCC).

Current Situation:

While our own network does not currently implement the STIR/SHAKEN framework, we utilise our upstream provider, Bandwidth (RMD0017042060) to ensure calls are appropriately signed and verified.

Bandwidth has fully implemented STIR/SHAKEN in its network and provides us with STIR/SHAKEN-compliant services for all US-bound calls.

Mitigation Strategy

Numbering Sourcing: We obtain US telephone numbers exclusively from T1 provider Bandwidth, which is a registered and reputable telecom provider in the United States. By maintaining a single trusted source of numbers, we significantly reduce the risk of fraudulent or spoofed calling activity originating on our platform.

Upstream Compliance: All US-originating calls are routed through Bandwidth, which applies STIR/SHAKEN signing. Bandwidth has confirmed that it meets the FCC's requirements for caller ID authentication and has provided assurances that every call passed through its network is signed, verified, and compliant.

Traffic Monitoring and Reporting:

- We proactively monitor call patterns and usage metrics to identify irregular or potentially suspicious activity, including sudden spikes in call volumes or short-duration calls.
- If we detect or are notified of suspected illegal robocall traffic, we immediately investigate and take corrective action, such as suspending the relevant accounts or terminating the offending call traffic routes.
- We cooperate fully with Bandwidth, industry partners, and law enforcement agencies in sharing information that aids in mitigating illegal or abusive calling activities.
- Onecom terms of service do not allow customers to resell services, Immediate restrictions applied when abuse or irregularities occur.

Customer Onboarding and Vetting: We employ a thorough onboarding process for all new customers, working only with registered organisations, obtaining the required identifications and clear usage cases for their call traffic. By vetting customers before activating their services, we reduce the likelihood that our network will be used to originate illegal robocalls.

Responsibilities

The Account management / Cloud support and consultancy staff are responsible for verifying and monitoring systems which includes reviewing any inconsistencies and abnormal activity.

Conclusion

Our company recognises the seriousness of robocalling threats and is committed to maintaining a secure and compliant voice service environment. By partnering with a reputable provider, Bandwidth, strictly vetting our customers, and monitoring traffic for suspicious activity, we believe our approach effectively addresses the FCC's Robocall Mitigation Plan requirements despite our own network's current lack of STIR/SHAKEN implementation.

Point of Contact for Traceback Requests and Questions

Onecom Support

Cloudsupport@onecom.co.uk