Anti-Scam and Anti-Spam Call Policy

Purpose and commitment

We are committed to maintaining the integrity of our telecommunications network and ensuring the trust, safety, and security of our customers. This policy outlines our zero-tolerance stance against the misuse of our telephony services for fraudulent activities, including scam and spam calls.

Definitions

Scam Calls - unsolicited calls intended to deceive, defraud, or mislead the recipient, often for financial or other unlawful gains.
Spam Calls - unsolicited bulk calls, including robocalls, telemarketing, or phishing attempts, conducted without the recipient's prior explicit consent.

Zero tolerance for misuse

We strictly prohibit any activity involving scam or spam calls. Upon detection, immediate remedial actions will be taken, which may include service suspension or termination, as well as legal action where applicable.

Prohibited conduct

The following activities are strictly prohibited:

- Initiating Scam Calls: using our services to deceive or defraud individuals or entities.
- Sending Spam Calls: engaging in bulk unsolicited communications for advertising, marketing, or other purposes without recipient consent.
- Caller ID manipulation (Spoofing): altering or misrepresenting caller identification details to deceive or mislead recipients.

Detection and prevention measures

To combat scam and spam calls, we implement:

- Automated detection systems
  - Advanced algorithms and machine learning models to identify fraudulent call patterns.
  - Continuous updates based on evolving threats and scam methodologies.
- Call traffic monitoring
  - Analysis of call traffic for irregularities, such as high call volumes from a single source or rapid sequential calls.
  - Supplementing automated systems with human review for accuracy.
- Customer reports
  - A reporting mechanism for customers to flag unsolicited or suspicious calls.
  - Investigations into reported cases, with escalations to regulatory authorities as needed.
- Industry and consumer group collaboration
  - Sharing intelligence on scam and spam activities with industry peers, upstream providers, and consumer protection organizations.
  - Participation in industry initiatives aimed at reducing fraudulent telecommunication practices.
- Regulatory and law enforcement engagement
  - Cooperation with regulatory bodies and law enforcement agencies to exchange information and take action against offenders.

Enforcement actions

Violations of this policy may result in:

- Service suspension: immediate suspension of services upon detection of misuse.
- Service termination: permanent termination for severe, repeated, or egregious violations.
- Legal recourse: referral to law enforcement for prosecution and compliance with regulatory requirements.

Customer reporting and feedback

Customers are encouraged to report suspicious or unsolicited calls through our support channels. Reports will be thoroughly investigated, and necessary actions will be taken. Customer feedback is essential for enhancing our protective measures.

VoIPcloud Wholesale
Floor 26, 188 Quay Street,
Auckland Central
Auckland, 1010
P +64 9222 4699
E support@nz.voipcloud.online

Policy amendments

This policy is subject to periodic review and updates to address emerging threats and regulatory changes.