

Robocall Mitigation Program For Swift Services

Executive Summary

This document outlines the Robocall Mitigation Program for Swift services. The program aims to protect consumers from illegal robocalls and ensure the integrity of the telecommunications network. Introduction Robocalls have become a significant concern for consumers,

regulators, and telecommunications providers.

Swift Services is committed to adhering to these guidelines, to protect our customers and the broader telecommunications ecosystem.

Enforcement

If it is determined that a Swift services customer is in violation of its acceptable use policy in any part of its network, Swift services will have legal action against the customer to stop such practices and terminate their service.

Call Verification:

Monitor Call Traffic: Our 24/7 NOC continuously monitor call traffic signs of spoofing or other malicious activities.

Caller id Authentication: Ensure that all outbound calls have valid caller id information.

Know Your Customer

Swift services has procedures in place to prevent new and renewing customers from using our network to originate illegal robocalls.

Swift services vets all residential and business customers, validates their identity, physical location, and contact personal information. Also, personally identifiable questions may be asked to provide additional security.

Consumer Education:

Educational Channels: To inform customers to report robocalls and seek assistance on our website.

Support Channel: Dedicate support channels for customers to report robocalls and seek assistance.

Contractual Provisions with End-users

All new customers acknowledge a statement on the service application which states users are prohibited from originating unwanted calls with the intent to defraud, cause harm, or wrongly obtain anything of value from the called party. If any customer is found in violation of the company's robocall mitigation policy the end users service may be terminated.

Upstream Provider Knowledge

Swift services knows all carriers from which it receives traffic. Lcubevoice has confirmed that all carriers in which Lcube voice exchanges traffic are listed in the Robocall Mitigation Database.

Traceback

Swift services is committed to cooperating with all legal and legitimate industry inquiries to potential invalid or illegal traffic originating from its network.

Swift services will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner within 24 hours.

Robocall Mitigation Database Eligibility

Swift services has not been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling.

Swift services has not been prohibited from filing in the Robocall Mitigation Database (RMD).

Robocall Detection and Blocking:

Real Time analytics: use real-time analytics to detect suspicious call patterns.

Blacklist: Lists are updated on time of known robocall sources and legitimate callers.

Conclusion

Swift services is committed to protecting our customers from illegal robocalls and ensuring the integrity of our telecommunications network. By implementing this Robocall Mitigation Program, we aim to comply with FCC requirements, and contribute to the broader effort to combat robocalls. Our approach combines advanced

technology, consumer education, and regulatory compliance to create a safer and more secure communication environment