

Optus Robocall / SPAM Calls Mitigation Plan

To whom it may concern,

Optus has undertaken the following measures to mitigate robocalls on its network:

- a. Monitoring:
Optus monitors network traffic to assure the service and quality of international traffic.
A non-intrusive CDR based Fraud Management System is in place to alert on traffic case involving intermittent bursts of high activity, suspiciously low call completion rates/short call duration and invalid number ranges.
In addition, our Fraud Prevention Department also monitors and alert on suspiciously high volume traffic and patterns.
- b. Investigation:
Once suspicious traffic has been alerted, Optus will collaborate with customers, carriers and providers expeditiously and in good faith to determine the legitimacy of the traffic. Optus is also committed to respond in a timely manner to AT&T / Verizon/ IDT and FCC licensed international voice calls providers for any trace back request.
- c. Blocking and suspending:
Once fraudulent traffic has been identified, Optus will suspend and block immediately the customer/carrier originating the suspicious traffic.

Optus is constantly working on improving the tools that can help to prevent and detect any kind of fraudulent traffic and Optus management will implement such measures and procedures without undue delays.

STIR/SHAKEN

Optus is currently unable to implement the STIR/SHAKEN protocol as we still have TDM switches in the core and edge of our voice network which prevents the implementation of the feature.

Optus does have a program in place to migrate to a full SIP voice network that will be able to support STIR/SHAKEN.

The current completion date for this program is scheduled for October 2026.

Suspected involvement with illegal robocalling or spoofing

As of September 2025, we can confirm that Optus is not subject to any current commission or other law enforcement agency action in the prior two years with relation to suspected involvement with illegal robocalling or spoofing.