

Sage Network & Communications

Carrier 1

The handling policies submitted under our carrier's robocall mitigation program are as follows:

- Software introduced to monitor outbound voice traffic in real-time to prevent the origination of illegal robocalls.
- The software provides detailed reporting identifying suspected illegal robocalls and alerts Our carrier if our carrier originates any calls where the calling number is:
 - Invalid
 - Unallocated
 - On a Do Not Originate list
 - In the FCC consumer complaint database
- Sage's carrier will immediately investigate any identified calls to determine if the caller was attempting to originate unlawful robocalls. If we determine that the caller was attempting to originate unlawful robocalls, then we either warn them to stop or terminate their service as appropriate.

Carrier 2

Classifications of the customer base for attesting to the customer identity with assurance that it will not present as a robocaller is as follows:

- Enterprise Business class who source DIDs directly from carrier are labeled "A" – best qualification and assurances
- Enterprise Business class who source DIDs from other than Carrier are labeled "B" – slightly lower but good assurance non-robocaller
- Residential – "A"

Carriers receiving traffic with "A and B" tokens in the header will treat the calls as safe for transit.

Carrier relies substantially on the official FTC Official Do Not Call Registry, Version 1.4. This registry is updated daily.

Additionally, Carrier augments the daily DNC registry with data from customers and underlying carriers who request a DID to be listed on the internal DNC and calls blocked for termination.

If the intended call resides in the public DNC list, we do not route the call but instead: (1) play and audio

message advising the number is prohibited; and (2) send a “SIP 487 request terminated message.”

We are in the process of implementing YouMail Carrier Products which will allow us to mitigate traffic in a real-time basis utilizing its multi-sourced database of potential suspicious or illegal DIDs.

We will provide a variation of the implementation you see in the diagram below the You Mail’s Real-time Mitigation Options section of the document.

Rather than an interface to the SBC, we can allow your infrastructure to query and store a local cache of YouMail data. Carrier queries may be every hour and/or every five minutes for up to the minute data.

The YouMail solution combines a live call sensor network with AI algorithms to identify telephone numbers (TN) that are originating fraudulent calls. The YouMail threat database maintains a continuously updated list of TN fraud sources and their associated campaigns. It features a REST API for integration into a network (Carrier) switch for real time robocall blocking.

All network engineers working within any of our underlying carrier partners routinely send inter-carrier notices/alerts when they “suspect” fraud. This is standard industry practice. Carrier’s internal practice is to remove the number and place on internal DNC; this process is real-time across all carriers; content is constantly changing and refreshed.