

We have a few tools available to help mitigate unwanted robocalls.

Reports -> Spam Report

This is a report on repetitive ANI with risk assessment that you can click and investigate further with user submitted comments and recordings available from external sources.

Click the ANI to get a popup with information showing the source(s) of the calls. You can click on the ANI in the popup to reveal links with more info. From this popup, you can choose to either block the ANI at the customer level (ANI/DNIS block tab in the account) or system-wide (System -> Blacklist).

The screenshot displays a 'Spam Report' interface. On the left is a table with three columns: 'ANI', 'Count', and 'Risk'. The first row is highlighted in blue. A red arrow points to the first 'ANI' value, '+12107961430'. To the right, a popup titled 'ANI Activity - %2B12107961430' is open. It contains a link to copy the ANI to the clipboard and a list of links to 'More info' for three different sites. A red arrow points to the 'More info - Site 2' link.

ANI ↗	Count	Risk ↗
+12107961430	60	MEDIUM
+12292102620	52	HIGH
+12628008457	82	MEDIUM
+12702666856	140	HIGH
+13307783031	76	HIGH
+14075536988	197	HIGH
+14105411462	62	HIGH
+14105550102	224	HIGH
+14694818569	137	HIGH
+14752522020	85	HIGH
+15125228876	62	HIGH
+15126416323	320	HIGH
+15126867316	72	HIGH

ANI Activity - %2B12107961430

Click here to copy [+12107961430](#) to clipboard

Action

For more information on +12107961430, click a link below

- More info - Site 1
- More info - Site 2
- More info - Site 3

Customer peer groups

In the trunks, you can set custom routes by ANI and/or by customer's media IP to an outbound trunk. What we suggest is to create an account called BLOCKER with a peer group set to BLOCKED and route these calls to it, which will get immediately rejected.

The screenshot shows the Asterisk Manager GUI. At the top, there's a 'Peer Group' section with a dropdown menu set to '11 - TEST', and buttons for '+ Add', '+ Delete', and 'Save'. Below this is a sidebar with navigation links: 'Common Settings', 'Inbound Settings', 'Outbound Settings', 'Block Vendors', 'Custom Routing' (which is highlighted), and 'Watchdogs'. The main area is titled 'Fixed Routes' and contains a table with columns 'actions', 'Route Group', and 'M'. A modal dialog box titled 'Fixed Route' is open, showing fields for 'Name' (set to 'known robodial media'), 'Codes' (set to '10.2.0.99, 64.7.101.2'), 'Match' (a dropdown menu with 'Dial Number' selected, and 'ANI' highlighted), 'Choose Account' (empty), and 'Peer Group' (empty). At the bottom of the dialog are 'Submit' and 'Cancel' buttons.

System -> Blacklist

Here you can manually add ANI you do not wish to route.

Any account -> Blocked ANI/DNIS tab

Same as the system blacklist but only applies to the account.

System -> Watchdogs

or

any account -> Peers -> Watchdogs tab

Here you can create watchdogs that will watch various metrics, including repetitive ANI (ANI tab), and take action. You can choose to temporarily or permanently block repetitive ANI per your configured criteria.

These are some of the tools available that can be used to help mitigate that type of traffic.