



Robocall Database Mitigation Plan.

Our NOC team works 24*7 monitoring traffic using different automatic and manual tools, in order to identify patterns that are consistent with robocalls. This information can assist in the traceback process to identify the source of illegal calls. Once the company identifies potential fraudulent, suspicious or, robocalling traffic, we block it so it can be rejected, we blacklist the origination number and issue a report to the customer notifying that the route is being fully blocked as a preventive measure and it will be re-opened once he confirms that the customer was removed. Once we have this confirmation, the customer is re-opened with the minimum capacity so that we can keep a strict audit of his traffic.

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocalls that use our service to originate calls. In order to accept a new interconnection, Telintel investigates about: Company's physical business location. Contact person(s). Company's reputation in the industry. We also ask the company for their incorporation letter so that it can be verified against the information they are sharing in the interconnection form and we reject all companies using generic domains as @gmail.com, @outlook.com, etc. This helps to identify, filter and, avoid interconnecting those companies that represent a high percentage of probability to send robocalls. Once the company is interconnected, we issue an official notification with the following information:

* We do not allow missed calls * Fraud, spam and scam traffic is not allowed * We will have to issue reports with your name and company name to the authorities in case we find any spam/scam traffic over our routes * Wangiri is also considered as fraud and is not allowed on our routes

Please be aware that, in case we find any of this traffic over the route, your account will be immediately suspended.

We have also implemented Inbound shield policies by querying local databases in the USA for verifying if the caller id is reported as high risk calling number or spoofed number (we carry out these queries using the Transnexus ClearING platform).

in order to open a new company, we ask for the following details:

- FUS - 499 Filer ID#
- W9 - TIN#
- Robocall Mitigation Database (RM ID) #
- FCC Registration Number (FRN)#
- Traffic profile description
- Legal company name
- Legal address of the company
- Web Page
- LinkedIn profile

The company is fully investigated by our legal team, taking into account all the above details plus the company's creation year in order to assign a trustability percentage. Once the company is interconnected, we share the following information:

1. ANIs must be legitimate, conforming, US ANIs, meaning +1npanxyyyy.
2. The ANI must conform to the LERG (reference NPA-NXXes in the LERG 6 file)
3. The ANI cannot, under any circumstances, be text (e.g. asterisk)
4. The ANI must not be spoofed, in other words, we must be able to return a call to the ANI and get something other than a recording.
5. Calls to a DNIS on the National DNC may be subject to penalties.
6. Calls originating from bona fide US government ANIs, such as the Social Security Administration, may be subject to fines or even imprisonment and therefore, are not accepted.

Required traffic stats:

Short Duration Percentage (SDP): Less than 45% Percentage of completed calls (ASR): Greater than 25%

Important

We are fully committed to our customers and providers and we only do/offer clean and legal termination. Therefore, the SCAM traffic is completely unacceptable. Calls from Amazon, Solar, Apple, Energy companies, Social Security, Medicare, Student loan, and Government entities among others are treated as an offense and the company sending this traffic will be immediately reported to the authorities for them to take action. In addition, we will report your company name and Account Manager's name in forums and social media.

Apart of the previous message, we daily monitor the traffic and inform the customer if we find any suspicious activity or traffic profile coming through our network so they can take immediate action and remove the traffic and customers from our routes.

Best regards,

Telintel Team

1500 Weston Road, Suite 200-29, Weston FL, 33326

www.telintel.net