Robocalling

Robocalling is the number one consumer complaint to the FCC. The FCC and telephony carriers have taken several steps to combat unwanted robocalls. These efforts fall into 2 general categories: (1) providing a method to verify caller ID through the STIR/SHAKEN regime, and (2) carrier services that attempt to identify robocalls and scams and either warning the receiver or directly blocking the call.

1. STIR/SHAKEN

What is STIR/SHAKEN?

STIR/SHAKEN is a set of technical processes and procedures designed to combat spoofed caller IDs. Robocallers often spoof their caller ID so that it appears that their call is arriving from a number local to the recipient so that the call will more likely be answered.

How Does it Work?

The STIR/SHAKEN regime is rooted in the ability of the originating carrier to "attest" to the right of the caller to use the caller ID sent in an outgoing call. An encrypted digital certificate is attached to the call header, and passed through to the terminating carrier. The terminating carrier can then authenticate the certificate by using the originating carrier's public encryption key. Based on trusting the attestation of the originating carrier, the terminating carrier can then inform the receiver of the call that the caller ID has been verified.

What does it do?

On Android phones, the words "Caller Verified" will show up under the phone number of the incoming call ringing page. On iPhones, verified calls will be indicated with a check mark in the Recent Calls page. STIR/SHAKEN itself does not block any calls, although carriers, cell phone manufacturers, and developers can use this information on their own call blocking apps.

What are limitations with it?

Note also that STIR/SHAKEN verifies only a subset of accurate caller IDs. Caller IDs may be accurate but the originating carrier may not be able to make a full attestation. For instance, if a caller owns a telephone number through one carrier, but makes outbound calls through another carrier, the outbound carrier cannot fully attest to the caller ID, even though the caller has the right to use that number. There are proposals to provide a mechanism for a caller to certify a right to use a phone number to an outbound carrier, but they have not been adopted at this time.

What can Plum Voice Customers do?

Plum Voice Customers that are concerned with the impact that STIR/SHAKEN may have on their outbound calls should ask their customers to whitelist the calling number that they use when placing outbound calls through Plum Voice. The easiest way for end users to do this is for them to add the calling number into the phone's address book or contact list.

When will it take effect?

STIR/SHAKEN was originally pushed as a voluntary system by the FCC that required a series of bilateral agreements between every pair of telephony carriers. AT&T and T-Mobile seem the furthest along in rolling it out. On December 31, 2019, the TRACED ACT[1] was signed, which orders the FCC to require implementation of STIR/SHAKEN generally within 12 months, with some exceptions.

2. Carrier Services to Combat Robocalls

What Services are Carriers offering?

The major cell phone carriers are also voluntarily implementing their own robocalling and spam blocking services, such as Verizon Wireless Call Filter[2], AT&T Call Protect[3], and T-Mobile Scam ID and and Scam Block[4]. These typically offer a free tier of service and then a paid premium upgrade.

What do they do?

Although each carrier's implementation is unique, they typically cross reference an incoming caller ID in real time to a database of known calling phone numbers of robocallers. They will then either label the call with a warning such as “Potential SPAM”, directly block the call, or send it to Voicemail.

How do they work?

Although each carrier’s implementation is proprietary, they typically use some combination of data analytics, network intelligence, and reports from customers to create and maintain a database of calling phone numbers of suspected robocallers. Examples might be suspicious patterns of high volume, short duration calls observed by the carriers, or customer feedback from “Spam” buttons on smart phone call log apps.

What are limitations with it?

There are many legitimate reasons for companies to use robocallers to call consumers, including school closing notifications, weather alerts, and patient reminders. Identifying which calls are legitimate versus spam is an imprecise art that will be both over and under inclusive.

What can Plum Voice Customers do?

The major US cell phone carriers rely in part on third party companies to maintain their database of unwanted phone numbers. In order to ensure your outbound calls are not miscategorized as unwanted or fraudulent calls by the wireless carriers, we highly encourage

---

[1] https://www.congress.gov/bill/116th-congress/senate-bill/151/text
[2] https://www.verizonwireless.com/support/call-filter-faqs/
[3] https://www.att.com/features/security-apps/#FAQ7
[4] https://www.t-mobile.com/customers/mobile-security

you to proactively request whitelisting of legitimate outbound calling use cases from each of the major wireless carriers.

Below are websites where you can submit whitelisting requests:

- AT&T/Wireless/Call Protect/HIYA
  - https://hiyahelp.zendesk.com/hc/en-us/requests/new
- Verizon/Wireless/TNS
  - https://reportarobocall.com/trf/
- T-Mobile / FirstOrion / PrivacyStar
  - https://feedback.fosrvt.com/

When will it take effect?

These services are already in the market. Last June 6, 2019, the FCC[5] gave the phone carriers the right to create implement call blocking systems by default on an “opt-out” basis.

[5] https://www.fcc.gov/document/fcc-affirms-robocall-blocking-default-protect-consumers-0