



## SPOOFING CALLER ID

---

by Al Weigand  
Tacoma, WA  
[aweigand@abilita.com](mailto:aweigand@abilita.com)

Recently there was a comment from a consultant who had a client who was receiving recorded solicitations to their cell phone with a bogus Caller ID of 407-000-6938. I'm sure that many of you share my opinion that the spoofing of the caller identification information represents a gross misapplication of telecom technology and must violate some regulatory rules. I thought I would delve a bit deeper into this topic and offer my opinion on what is happening and what recourse might exist.

First, it is important to understand that the public switched telephone network is really comprised of two distinct networks - a voice network that carries the actual conversation, and a packet data network that controls call setup, tear-down and all of the data necessary for network features like Caller ID, Calling Name and 800 services. This data network is known as the SS7 or "signaling system 7" network. Originally, access to the SS7 network was limited to exchange carrier switches and databases (i.e., calling name database and 800 database) but was extended to PBXs in order to offer Caller-ID and other advanced signaling services to enterprise customers via an ISDN PRI trunk. The advent of voice-over-IP networking and the Session Initiated Protocol (SIP) has extended the visibility of the signaling information to any VoIP device with a proper connection to the network.

When placing a call, the originating switch will populate caller information in two distinct data packets that traverse the SS7 network. The first, and most critical, is the automatic number identification, or ANI. ANI identifies the true billing telephone number of the originating line, is not usually displayed to a called line and typically cannot be manipulated by an end user as it is populated by the serving CO switch. However, in the VoIP world it is possible to originate a call that has a user-defined ANI, which may be arbitrary. ANI information is sent to 911 centers (PSAPs) and can be delivered to PBXs over an ISDN PRI. The delivery of ANI to a called party is typically an option on an inbound 800 line to a call center operation, but it may also be visible to an IP device connected via a SIP trunk.

The second packet of number information sent with every call is the Caller ID. This is the number that will be displayed to the called party when the call arrives at the destination. The Caller ID (CID) can be blocked, either by invoking a feature code when the call is originated (per call blocking) or by subscribing to a privacy feature (per line blocking). However, neither feature actually removes the CID information from the call, but instead sets a privacy signaling flag that indicates to the terminating office that the CID is not to be delivered to the called party.

CID can be manipulated, changed, or spoofed by a switch that is connected to the signaling network. This can be a central office switch, a PBX with an ISDN PRI trunk, or a VoIP switch with a SIP trunk connection.

In the case of the recorded solicitations, the bad guys are most likely using their own VoIP switch that is SIP- connected, and inserting a bogus CID in each outbound call. The traditional

local exchange carrier typically does not screen for valid CIDs and will not block them, and the VoIP carriers are even less inclined to impose any limitations on a user.

'Clearly the technology exists to create a spoofed Caller ID. However, the FCC does have an opinion on the blocking or spoofing of CID by telemarketers and addresses this issue very specifically at <http://www.fcc.gov/cib/consumerfacts/callerid.html> :

"Federal Communications Commission (FCC) rules prohibit telemarketers from blocking Caller ID information and require them to pass accurate caller ID numbers. FCC rules specifically require that a telemarketer:

- transmit or display its telephone number, and, if possible, its name or the name and telephone number of the company for which it is selling products or services.
- display a telephone number that you can call during regular business hours to ask to no longer be called. This rule applies even to companies that already have an established business relationship with you.

For violations of these rules, the FCC can seek a monetary fine. If the violator is not an FCC licensee, the FCC must first issue a warning and the telemarketer may be fined only for violations committed after the warning. "

From this, we can conclude that if the aforementioned calls are telemarketing calls, then they are in violation of the FCC rules.

Now for the seedier side of the deal. Those less scrupulous and less technical operators and individuals who want to spoof their CID can use a commercial third party provider. Here are four that you can readily find on the web: Spoofcard, Telespoof, Spoofel, and Itellas. All of these services, as well as Google, operate as call re-originators meaning that the spoofing service provider places the actual call to the desired target number, and bridges the outbound call to the originator's line. During the process they substitute a fake CID that is delivered to the far end. The originator either dials an access number and inputs his desired destination and spoof ID, or initiates the process over a web interface where the service provider places calls to both the originating and terminating line and bridges them together.

Unfortunately, spoofing CID in this way is not illegal - as long as it not done by a telemarketer. Congress has tried two or three times to introduce bills to outlaw all spoofing, but they have never been passed. Florida had passed a CallerID anti-spoofing act, but it was struck down in July of 2009 as being unconstitutional since it effectively regulated interstate commerce (read more here: <http://www.prweb.com/releases/2009/07/prweb2681224.htm>).

Spoofing does have its legitimate users, mostly law enforcement officers who want to disguise themselves during investigations or abused spouses who want to maintain privacy about their location.

So, what can you do about this situation when your home or business is being plagued by telephone solicitors who are spoofing their CID? Sadly, not an awful lot.

If you could identify a telemarketer who is spoofing their CID, you would have a clear violation of FCC rules, and possibly a violation of the National Do Not Call Registry. You could then file a complaint with the FCC or the DNC registry. However, it is unlikely that you will be able to clearly identify the bad guys here since anyone going to such lengths to disguise themselves is probably running a scam and is clearly not going to reveal their true identity during a conversation - if you can even converse with a human.

If the calls continue and can be classified as "harassing" then you could file a police complaint and involve the local telephone service provider in an attempt to identify the caller. You might consider using \*57 to trace the call - but you will find that the results will be useless since this feature captures the inbound (spoofed) caller ID instead of the ANI, and will cost you between \$1 and \$5 per activation.

If the problem grows to larger proportions, the telco can enable a trap and trace feature on the line that will record all incoming and outgoing call information. This information will not be shared with you, but can be used by law enforcement. Unfortunately, many times the information gathered in this manner will indicate only a trunk group and not the actual calling party ID or the ANI, depending upon the level of sophistication of the LEC. Capturing the actual ANI requires an SS7 monitoring tool that not all LECs have available or will utilize for this type of complaint. If by chance the ANI can be captured, then it may turn up a third party spoofing provider (see the list above) or it may turn out to be a spoofed ANI. If the issue is significant enough, law enforcement can obtain a subpoena and compel a third-party spoofing provider to reveal the originating telephone number, but in the case of a spoofed ANI, identifying the bad guy gets a lot more complicated.

One other possibility is to utilize TrapCall; a service that un masks blocked Caller IDs and, ironically, is owned by the same company that runs SpoofCall. TrapCall is primarily targeted at cell phones. In this scheme, an inbound call to a cell phone is forwarded to TrapCall, who un masks the CID and then re-originates the call back to the called party, inserting the un masked CID in place of a blocked ID. Since this service utilizes a standard 10-digit phone number and not an 800 number (see the TrapCall FAQs), it is most likely an IP-connected provider who is pulling the CID (or even the ANI) from the SIP signaling message. Privacy takes another hit from technology even though unmasking a blocked CID seems to violate another FCC rule [http://epic.org/privacy/caller\\_id/fcc\\_final.html](http://epic.org/privacy/caller_id/fcc_final.html) which says:

"No common carrier subscribing to or offering any service that delivers calling party number may override the privacy indicator associated with an interstate call. Carriers must arrange their CPN-based services in such a manner that when a caller requests privacy, a carrier may not reveal that caller's number or name, nor may the carrier use the number or name to allow the called party to contact the calling party. The terminating carrier must act in accordance with the privacy indicator unless the call is made to a called party that subscribes to an ANI or charge number based service and the call is paid for by the called party."

The hitch here is that this rule specifically prohibits "common carriers" from overriding the CID privacy indicator. Unfortunately the folks providing these services do not meet the strict definition of common carriers, so for the moment they can operate with impunity.

Bottom line - until the federal government enacts legislation to ban or regulate CID spoofing, and includes all providers, not just carriers, the problem will continue to exist and most likely grow more annoying.