Illegal Robocall Free with Trusted Caller ID

Louis Taff

Louis Enterprises, LLC

1. Introduction

1.1 Goals

This document is an entry (Proposal) in the U.S. Federal Trade Commission (FTC) 2012-2013 public challenge competition ("the Competition") for a method to prevent the completion of illegal and/or fraudulent calls placed by machines ("robocalls"). The stated goal of the Competition is "to create solutions that will block illegal robocalls on landlines and mobile phones." The primary goal of this entry is to create such a solution. A secondary goal is to create an enhanced solution that will give phone subscribers choice as to how robocalls are handled. Rather than block such calls, they may wish to decide for themselves whether to answer any given call after being presented with information that the call may be an illegal robocall. Our third overarching goal is to dramatically decrease or eliminate illegal robocalls altogether by making illegal robocalling uneconomic – it simply won't pay. We limit ourselves to calls that at least partly use the Public Switched Telephone Network (PSTN) and/or the Public Land Mobile Network (PLMN).

2. Overview of Proposal

We use a multi-pronged approach. Mostly, our Proposal is based the trustworthiness, or lack of it, of Calling Party Number information that, when presented to called parties, is termed Caller Identification or Caller ID, or simply CID. If the CID of an incoming call is intentionally falsified ("spoofed"), the call may be an illegal robocall or other call that the telephone subscriber would rather not answer. If the CID is genuine and the call is an illegal robocall, the calling number can be captured to use for screening of future calls and for legal action against the caller.

Therefore, one can say that our Proposal is based on (re)establishing ***trust*** in caller ID information. Briefly, the PSTN/PLMN switch receiving a call origination will classify any user-provided Calling Party Number as genuine or spoofed using its subscriber records for the originating facility. These records are accurate because the same switch must also route calls *to* the facility. When the terminating switch is about to deliver the call, the switch will know, through our proposals, if CID information about the call is trusted. If the CID is both trusted and not spoofed, the switch will deliver the call normally. If it is spoofed or not trusted, the switch will, at the subscriber's option, either block the call or identify the call to the subscriber as having an untrusted CID so that the subscriber can choose whether to answer.

In summary, we propose the following technical developments to stop illegal robocalling.

A. Create a new software feature for telephone switches with which a telephone subscriber can report illegal robocalls. After receiving and hanging up on such a call, a subscriber would dial a new "vertical service code" (such as "*99") to report it. The call's particulars would be recorded for use by government agencies in pursuing legal action against the owners of the CID. If the CID was not spoofed, action against the number's owner should be straightforward. If it was spoofed, captured information may help prevent future such calls by leading to the call's carrier(s).

B. Carriers must implement software in their switches to "screen" customer-delivered Calling Party Numbers ("CPNs") and must correctly populate the "Screening Indicators" in CPN Information Elements in common-channel signaling messages.

C. A new signaling parameter, "Trust" for Screening Indicators, must be implemented in SS7 signaling messages to show that a Screening Indicator is trusted.

D. A new database of *carrier* "Trust" must be established, and managed and maintained by a disinterested party. The database will register whether or not the Screening Indicators for each *carrier* are to be trusted.

E. When a carrier receives a call from another carrier, it must examine the SS7 signaling messages for the CPN Information Element and possibly modify it based on the carrier Trust database.

F. When a (Class 5) switching office delivers a call, if the CID is spoofed or, possibly, untrusted, it should block the call or take alternative action as specified by the subscriber, possibly requesting DTMF input from callers.

G. We propose new methods for presentation of terminating calls with untrusted CIDs to subscribers.

H. We suggest that private operators of VoIP gateways ensure that they keep careful records of their customers' registrations for service and a history of their call-detail records.

I. Carriers should implement in their switches the ability to provision for each ISDN facility a list of "auxiliary" calling-party numbers that will pass CPN screening to allow for certain non-fraudulent spoofing.

The remainder of this Proposal discusses the rationale behind these developments and how they stop illegal robocalls. We acknowledge that parts of our Proposal may have been suggested elsewhere, but have not seen this unique and comprehensive combination approach before. To our knowledge, the cross-carrier propagation and possible modification of Trust is entirely new, as is our proposal for Blocked Call requirements, presentation of spoofing information to subscribers, and provisioning of "spoof-able" numbers (E, F, G, I).

3. Characteristics of Robocalls

3.1 Call Volume

We note firstly that in principle it is not possible to distinguish between a call originated by a person and one originated by a machine. We conclude that one of characteristics of illegal robocalls is the sheer *volume* of calls. However, volume by itself is not a unique signature of illegal robocalls since:

1) a large volume of calls may constitute *legal* robocalls,

2) a low-volume but perhaps highly targeted robocall campaign may escape detection, and

3) illegal robocallers may find ways to disguise the volume of calls. They may randomize the order in which they call various geographic areas, or send different calls through different routes such that any single calling path may not carry sufficient calls to trigger a detection mechanism, or use multiple geographically dispersed robocalling devices, or a combination of these.

3.2 Falsified Calling Party Identification

CIDs are a more promising method through which to identify illegal robocalls because the CIDs of such calls are highly likely to be spoofed. If the CID of any illegal call, robocall or not, were not fake, then the origin of the call would be relatively easy to trace to its originator and the legal process would be able to intervene. Additionally, we assume that there is no reason to obscure the CID of *legal* robocalls. Therefore, we feel that the method most likely to correctly predict a given call to be an illegal robocall is to identify its CID as spoofed. Calls whose CIDs are spoofed for legitimate purposes are discussed in Section 8.

3.3 *Development A*: New Feature Code and Database

This leads to one prong of an attack on illegal robocalls. Phone companies should implement a complaint registration feature whereby a subscriber receiving a call he or she believes to be illegal may hang up, lift the receiver, receive dial tone and dial a feature code ("vertical service code") that will register the last call received as a possible illegal call. This is similar to actions taken to add a caller to a list for a feature such as Selective Call Rejection. This new feature

would record in a database the date, time, called number, CID, and any available information about the carrier(s) that took part in the call's delivery (such as the Transit Network Selection information element, if any, in the signaling Initial Address Message). Future calls to the subscriber with this CID should be blocked, perhaps after a confirmation check.

The database would be analyzed, perhaps by sorting on the CID field. *Valid* CIDs could be traced and, if found to be the source of illegal robocalls, legal action taken against their owners. For *spoofed* CIDs this technique may or may not lead back to a working phone number. If information is available on the *carrier*(s) of calls with spoofed CIDs, they can be labeled as untrusted (they carried a spoofed CID without labeling it as such) as described below in more detail.

4. Robocalls and Caller Ids

4.1 Analog Lines, T1 Carriers

On call originations from analog lines and digital (PBX) trunks, CIDs are provided by the switch from *telco-provisioned* records of the phone numbers associated with the lines and trunks. Therefore, it is essentially not possible for a call from an analog line or digital trunk to present a spoofed CID. (We exclude spoofing by calling parties inserting a modem signal on the line *after answer* to add characters to the CID device at called party end.)

4.2 Wireless Originations

Illegal robocalling from wireless (cellular) phones means large numbers of actual cell phone calls being made that meet the definition of illegal robocalling. We are unaware of this having occurred and feel it is an unlikely scenario. First, the costs of such calls would outweigh any financial benefit to the caller. Second, spoofing would be technically difficult to achieve, as the origination number of a cell phone call is available to the Mobile Telephone Switching Office (MTSO), and therefore would difficult to spoof directly. We do not consider wireless originations further.

4.3 ISDN Originations

Customer Integrated Services Digital Network (ISDN) equipment has digital signaling capability over special signaling channels ("D channels") on ISDN Basic and Primary Rate Interface (BRI) and (PRI) facilities. The equipment uses the standardized D-channel Q.931 protocol that employs signaling messages to establish and disconnect circuit-switched calls. The various signaling message types may each contain one or more standardized "Information Elements" of data..

One of these Information Elements (IEs) is termed the "Calling Party Number" or CPN. When the ISDN equipment *receives* a call whose signaling contains a CPN IE, it may extract the information and display it as the calling party number. When the equipment *originates* a call, it may populate a CPN IE. The network receives this Q.931 CPN IE and uses it, *usually without checking its validity*, to populate a CPN IE of an inter-switch common-channel signaling message sent with the Q.763 Signaling System 7 (SS7) protocol. The CPN IEs of the Q.931 and Q.763 protocols are similar but not identical. The SS7 Q.763 protocol message in turn is used to set up a call through the network to the target number. If the originating ISDN equipment does not transmit a Q.931 CPN IE during call setup, the network may populate a Q.763 CPN IE with its own provisioned data. At the switch to which the target (called) phone is connected, the Q.763 CPN IE is received and analyzed and the switch may present its data to the terminating subscriber as the CID.

The first key point of this subsection is that the network does not control the digits with which the customer premises equipment (CPE) populates the CPN IE. The CPE may transmit any content that has been programmed, and this content will be transmitted to the terminating subscriber as the CPN. If the CPN is not a number that the receiving subscriber can dial to get back to the calling party, the CPN is (by definition) spoofed. Therefore, an originating subscriber needs only a BRI or PRI interface and appropriate programmable equipment to spoof a CID on a call.

The second key point is that the originating switch (i.e., the switch that terminates the originating BRI or PRI interface) has an opportunity to validate or "*screen*" (check) the CPE-provided Q.931 CPN IE against its provisioned records before using it to populate a Q.763 CPN IE. These provisioned records are those used to route and deliver *incoming* calls. Therefore, as noted, "valid" usually means that if the recipient of a call actually dials the received CPN to make a return call, that call will terminate at the device that originated the first call. The CPN IEs in both the Q.931 and Q.763 protocols support a "screening indicator" field that shows whether the CPE-provided CPN passes validation against the

switch's provisioned records. This was designed to allow an originating switch to report spoofing to downstream switches. Most service providers appear not to perform this validation or correctly populate the screening indicator.

4.4 Originations on VoIP Equipment

VoIP transports digitized voice signals over a data network via the Internet Protocol. Two phones anywhere in the world can be connected for a VoIP conversation via connected data networks without the call ever touching the PSTN. To connect VoIP traffic to the PSTN requires converting Internet Protocol voice and signaling to that used by the PSTN and vice versa with a device called a VoIP Gateway- the gateway connects VoIP calls with PSTN circuit-switched calls.

If the gateway receives a VoIP origination, the origination signaling (using, e.g., Session Initiation Protocol, or SIP) contains a PSTN number to call. If the gateway interface to the PSTN is an analog line or T1 trunk, the PSTN switch will originate a call and populate an SS7 CPN IE with provisioned (non-spoofed) data for the CPN as in 4.1. The gateway will remain on the call until disconnect, converting between the packetized VoIP voice and analog or digital voice signal on the PSTN.

If the gateway interface is a BRI or PRI, the situation is analogous to section 4.3; the gateway will populate its Q.931 CPN IE with whatever number has been programmed. Typically, it will use the number received in incoming VoIP call signaling. Therefore, an ISDN VoIP gateway is similar to an ISDN PBX in its ability spoof calling numbers. Spoofed CIDs may arrive in call-origination signaling, so the gateway itself need not be programmed for them.

Carriers may themselves offer VoIP service to customers. In this case, a gateway function is still needed, but it is operated by the carrier. Its interface to the rest of the carrier's network may be a PRI operated by the carrier or some other kind of trunk arrangement. A gateway operated by a carrier can screen any user-provided CPNs against provisioned data in the gateway itself – again, needed to route incoming calls.

4.5 Robocall Paths

Some variety of the paths through which robocalls reach a phone **A** connected to a local phone company is shown in Figure 1. Robocaller **C**, coincidentally connected to the same switch as **A,** might reach **A** directly via **C-B-A**. Indirect paths, requiring SS7 signaling, include **C-D-B-A** and via a tandem switch **C-D-E-B-A**. A more extensive path from robocaller **M** connected to another local exchange carrier and involving multiple interexchange carriers might be **M-L-K-I-H-E-B-A**. Finally, a robocaller **J** directly connected to an interexchange carrier may use path **J-I-H-E-B-A**. To reach an angry mobile customer, any of the three robocallers could take a path ending in **H-F-G**. PRI equipment (typically PBXs) can interface to Class 5 switches, but can also connect to interexchange carriers directly ("direct connection," sometimes called "bypass"). Direct connection is typically used by enterprises to avoid (bypass) LEC charges on long distance calls. It might also be used by an illegal robocaller (connection **I-J** in Figure 1).

5. Spoofed *vs*. Accurate CIDs

We address here how a service provider can identify spoofed CIDs within its network. We noted above that signaling standards support an indicator to flag spoofed CIDs. These standards appear not to be correctly supported by at least some public networks. Our Proposal exploits and extends these existing standards to identify possibly spoofed CIDs.

The Calling Party Number (CPN) IE "Screening Indicator" mentioned previously is a two bit wide field that provides data about the actual CPN digits, and can have four values in its two bits:

00 – User provided, not screened

01 – User provided, screened and passed

10 – User provided, screened and failed

11 – Network provided.

Here, "User provided" means the originating party sent the CPN in the call setup signaling.

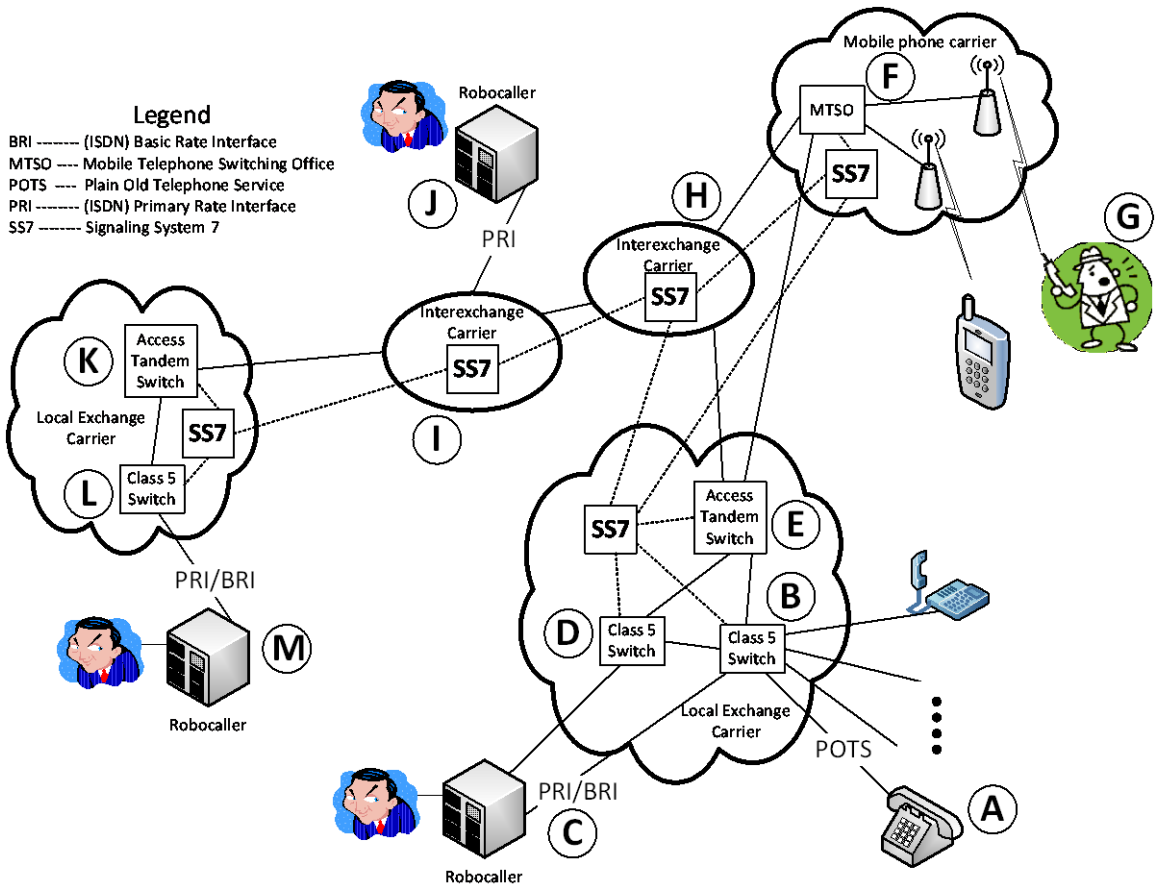

Figure 1. Network architecture for sources of robocalls.

5.1 *Development B*: Screening In-Network Originations

On call originations from analog lines or T1 Carrier, the service provider should populate the CPN IE with either the directory number of the line/trunk, if one exists, or its Billing Number (BN) if it is part of a multiline hunt group and has no directory number of its own. If the directory number and billing numbers are different, it is a subscriber option or service-provider policy as to which of the two will be used as CPN. Since the CPN is populated from the service provider's own records, it is network provided and its screening indicator should be 11.

Devices such as digital or VoIP PBXs may deliver calls to the network over an ISDN BRI or PRI. CPN information elements transmitted with the call-setup signaling for these calls are populated by the subscriber. If the network receives an ISDN call with no CPN, it can proceed as though the call were received on an analog line. If, however, it receives a CPN, the CPN is by definition User-Provided. The service provider can choose to check the CPN against its records (i.e., "screen" it). If the CPN is not checked, its screening indicator must be set to 00; at the terminating end, the CID will probably be flagged as untrusted because the originating user might have spoofed the CPN.

If the CPN is screened and matches a number assigned to the interface, the screening indicator should be set to 01. If the CPN is screened and does not match a number assigned to the interface, the screening indicator must be set to 10.

Thus, for our **Development B** we propose that on a customer ISDN call origination, the originating network node "screen" any user-supplied CPN and correctly populate the "screening indicator" bits in signaling messages. If the user-provided CPN matches a provisioned CPN, the CPN passes the screen; if not, it fails. If no CPN is passed, the switch uses a provisioned CPN and sets the screening indicator to Network provided. The codes to label the four possible outcomes would be as given above, modified by setting a new "Trust" indicator as described in Sect. 7.3 to "Trusted".

5.2 Issues for VoIP Gateways

VoIP phones connecting to VoIP gateways pose special problems, as illustrated in Figure 2.

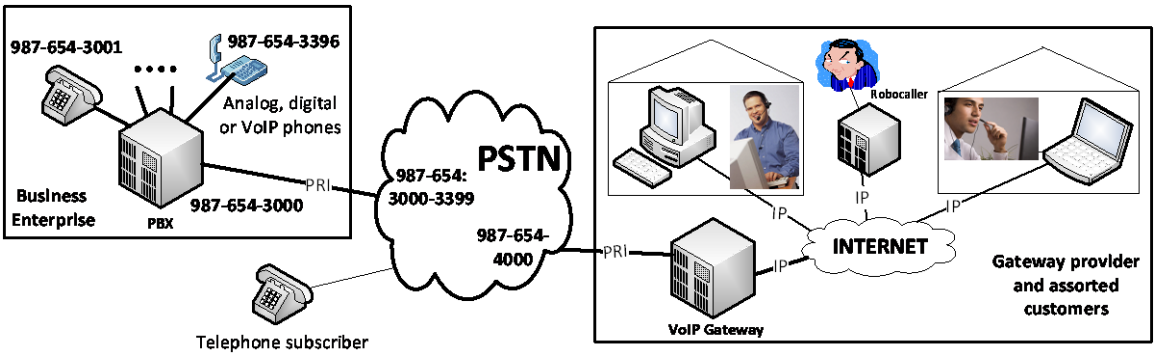

Figure 2. Phone number provisioning for a PBX and a Gateway.

5.2.1 PBX-Like Arrangements

Business/enterprise arrangements that are topologically equivalent to left side of Figure 2 are typical. Whether each phone is analog, digital or VoIP, its calls to the PSTN are sent with a CPN that will pass screening because the PSTN is provisioned for the set of numbers assigned to the interface. This is a standard PBX arrangement. As a variation on this, Skype operates a PSTN-to-Skype service called Skypein, somewhat reflecting the left side of Figure 2. Skype reserves blocks of PSTN numbers and rents them to Skype users. Non-Skype callers dial a PSTN number and reach a Gateway. The Gateway originates a VoIP call to the Skype user's current IP address and bridges the call legs.

5.2.2 Originations without a PSTN number

The right side of Figure 2 shows a VoIP Gateway operator with various customers making VoIP originations intended to terminate on the PSTN. These callers have no PSTN numbers assigned at the Gateway. Any CPN they might specify on outgoing calls may or may not be a real PSTN number that may or may not belong to them. If allowed by a gateway operator, callers may connect to a gateway anonymously (except for their IP addresses) and spoof any CIDs they wish. The robocaller, for example, might make unlimited calls with spoofed CIDs that called parties have no way to return, or even to trace. The one caveat is that the Gateway operator will no doubt have a mechanism to bill the callers.

If, however, the PSTN screens calls as specified in the beginning of this section, the network switch will detect that the gateway is not provisioned for any user-provided numbers and set the Screening Indicator to "failed" on any such calls. The terminating switch will detect the Indicator and block the calls.

If caller-provided CIDs are *not* sent to the gateway with call originations, the gateway itself or the network would use the gateway provisioned billing number as the CPN. The PSTN would transport the calls and deliver them, as they would have a legitimate CPN. The called parties would see the Gateway number as the calling party.

This is the case, for example, for calls made by users of Skype who want to call a PSTN number ("Skypeout" service). These callers pre-register with Skype, giving billing information such as a credit card number. Called parties soon recognize the Skype Gateway CID of these calls and answer them. However, according to Wikipedia,[1] "Skype users can assign a caller ID number in order to prevent their Skype-Out calls being screened by the called party." Because Skype users could choose the caller ID numbers maliciously, we see little alternative to treating these CIDs as spoofed.

A problem occurs when, as in Figure 2, a robocaller does not spoof its calls, but uses a Gateway (and its CPN) for large numbers of illegal calls. This is addressed in the following section.

5.2.3 *Development H*: Registration of VoIP Users

A Gateway customer or owner may send illegal robocalls through the gateway without spoofing the calls' CIDs. Our method of screening spoofed CIDs will not prevent these calls from completing. Here we must depend on reports by call recipients of the bad actions (see sect. 3.3 above: *Development A*: New Feature Code and Database). The robocall

reports will contain complaints of illegal calls with the gateway's own number as the calling number. Legal action might be taken against the owner of the gateway.

Fault, however, may lie not with the gateway owner but with one of the owner's customers. Hence, as *Development H*, the owner must be able to show enforcement authorities call-detail records of the gateway and to identify the customer that made the calls. Therefore, gateway owners need to do careful record keeping. They need to be able to produce information (credit account number, etc.) that can lead to a physical address at which any customer can be found.

5.3 Actions on Out-of-Network Originations

Each call entering a service-provider's network from another network must have its SS7 CPN IE examined at its point of entry, and the new Trust indicator (see Sect. 7) must be modified if necessary. All network nodes (e.g., Class 5 switches) that deliver calls to terminating subscribers would consider the Trust indicator when evaluating the screening indicator bits and take appropriate actions.

5.4 *Development F*: Actions on Terminations

When a call is to terminate (be delivered) to a subscriber, the delivering node must examine the CPN information to determine if it is trusted. The CPN IE will contain a new Trust indicator for the screening indicator. If the screening indicator is trusted, the values of the CID are those given at the beginning of Sect.5.

For screening codes 01 and 11 the network node delivers the call normally. The CID may or may not be sent to terminating subscribers with CID service, depending on the Presentation Restriction indicator. Presentation Restriction (whether or not the CID may be sent to the terminating subscriber) has no bearing on whether the CID is valid. The subscriber might reject the call if Presentation Restriction is on (Anonymous Call Rejection) even if the CID is trusted.

For codes 00 and 10 the network node invokes one of the actions proposed in section 6.

If the call originated outside the service-provider's network, the trustworthiness of the screening indicator will have been flagged as per Sect. 7. If the node receives an untrusted screening indicator, it should probably treat the CID as though the indicator were 00.

6. *Development G*: Identify Spoofing for Subscribers

6.1 Calls with Unacceptable CIDs

Calls with Screening Indicators 00 and 10 might receive services patterned on Custom Local Area Signaling Services (CLASS), such as spoofed call rejection (block the call) with optional announcements to calling parties, selective spoofed call acceptance, etc. Depending on the screening indicator and CPN content, the service provider may classify a call into one of multiple categories: verified, unsure, known bad provider, etc. A display to the subscriber (see below) may reflect these categories. In one common case, a CID displays "Out of area," often an illegal telemarketer or robocall. If a call's screening indicator is untrusted or 00 *and* its CPN IE is blank or does not conform to a phone-number format, we suggest that it be treated as "10".

The CLASS feature set is based on the *availability* of CID under the assumption that the CIDs are trusted. Additional services based on the *trustworthiness* of CID can be analogous to those based on CLASS. Selective call acceptance for specific numbers, selective call rejection for others, general call rejection for calls whose CID fail certain trust levels and possibly other services could be available to those harassed by false CIDs.

6.2 Blocking: Spoofed Call Rejection Feature.

This Challenge does not give requirements for a call rejection feature except to "Block" illegal robocalls. Here we propose requirements for the feature. When a call arriving for a subscriber is to be blocked by Spoofed Call Rejection:

1) Play an announcement on the backward voice path (to the caller) identifying why the call did not go through. If the call was a robocall, the announcement will probably not be heard by a person. If the call was from a person, the

announcement should contain sufficient information for the person to understand what happened. The announcement might additionally contain information for the caller on how to avoid the current unpleasant situation – such as to use another phone network, since at least one of the following has occurred:

a) the CPE they are using spoofed the CID,

b) the network they are using did not screen the call,

c) the network they are using is untrusted with respect to CPNs,

d) the network they are using routed the call over at least one untrusted interexchange carrier.

2) This announcement is an opportunity to introduce another feature, "dial-through". Human callers might be given an opportunity to dial a DTMF code to prevent blocking. One issue with this is that illegal robocallers may soon develop the ability to automate dial-through DTMF tones to ring the target phones. To avoid this, the code might have more than one digit, possibly of the terminating subscriber's choice.

3) Return answer supervision. I.e., answer the call at the network Class 5 switch long enough to ensure that a charging record is made, that the originator of the call will pay for it, and that any transit networks will pay their "forward" networks for carrying the terminating call. This departure from convention may require renegotiating interconnect agreements among carriers. We acknowledge our ignorance of the complex and controversial topic of intercarrier compensation.2 Thus, call "completion" rates for illegal robocalls should increase (no more no-answers), increasing the robocallers' bills, but the number of calls answered by humans should decrease dramatically.

4) Release (disconnect) the call. The terminating subscriber is unaware that anything happened.

6.3 Presentation of Spoofed CIDs

Some subscribers may choose *not* to block illegal robocalls, but to be "warned" prior to answering them.

For subscribers without a CID display, spoofing could be signaled through one or more new ringing cadences; this would alert the subscriber to something abnormal about the call.

For the roughly half of U.S. subscribers[3] with a CID display, a possibly-spoofed CID could be identified through one or more additional characters in the information sent for Caller-ID display, such as a question mark leading and/or trailing a number or name. Multiple levels of distrust of the CID (possibly spoofed, definitely spoofed) could each have a unique flag. New ringing cadences could be used for these subscribers also.

On analog lines in the U.S., calling number delivery is transmitted in the interval between the first and second rings. Specifications for the service, including the information content, are available from Telcordia (formerly Bellcore) in document GR-31-CORE, part of the extensive LSSGR (Local Switching System Generic Requirements) package; associated Calling Name Delivery requirements are in GR-1188. GR-1188 (issue 3) contains requirements for a new 60 characters Extended Name field; this number of characters could support a detailed description of the weakness of a CID. LSSGR documents are not widely available due to their significant cost. We have used a suitable substitute, British Telecom (BT) Supplier Information Note, BT SIN 227, issue 3.5, available at: www.sinet.bt.com/227v3p5.pdf. The character set specified is IA5 (International reference Alphabet #5), the ASCII code in the U.S. - all printable characters on a standard keyboard. Therefore, to identify a CID as possibly spoofed to a subscriber, the service provider has a wide choice of characters. Human factors specialists and/or a market study can determine the most customer-friendly characters to use. Subscribers with CID displays who have not been subject to spoofed CIDs may find the new flag characters confusing. We suggest that this "identify possible spoofing" feature be provisioned separately from the basic Caller ID feature. Only customers desiring spoofing protection need then have it assigned and active.

On digital lines, including mobile phones with digital service, spoofed CID presentation could be done by simply relaying the Calling Party Number IE, including the screening indicator, to the subscriber. This would allow intelligent CPE to identify a questionable call and behave according to the user's preference.

7. Database of Trusted Networks

If a call originates outside a service provider's network, then the provider has only the call-associated CPN IE information provided by the delivering network to determine trustworthiness of the CID. Generally, this information is

insufficient because of possibly inadequate measures taken by the originating network or a transit network. We have informally heard[4] that some service providers either carelessly or willfully violate the terms of their interconnection agreements with other providers and deliver CIDs that are not trustworthy.

7.1 *Development D*: "Trust" Database Proposal

Therefore as a component of this Proposal, we propose a new feature to be deployed by telephony service providers to determine if the networks to which each provider connects are trustworthy[5]. CIDs of calls originating in other networks might be spoofed but not be flagged as spoofed. Risky networks would be flagged through a *database* that associates a *trust* level with each network from which a provider receives incoming calls. The database would indicate if the Screening Indicators of CPN IEs received from each network are trusted. The value of trust for a CID for a terminating call is the trustworthiness of its Screening Indicator, which is that of its originating network, and is simply looked up in the database. Initially we propose only two values – trusted or untrusted.

The network terminating a call generally has no knowledge of what upstream networks the call traversed, and therefore whether the Screening Indicator is to be trusted even if it is so marked. Therefore, trust must be tracked along a call's path. If network A passes a call to network B as a transit call which passes it to network C, *Network B must update the CPN IE of the transit call signaling to reflect the trustworthiness of network A* as recorded in the trust database. If network A is trusted, network B should do nothing with the CPN IE. If network A is untrusted, network B must set the Trust indicator in the CPN IE to untrusted. Network C must do the same – i.e., it must update the CPN IE depending on the trust database record of network B. This is the only way a downstream network can learn if the CPN IE is to be trusted. Hence, to gain trust or remain trusted a transit network must relay trust information. If *any* network along the path is untrusted, the CPN IE will show untrusted.

Note that a trusted network may still deliver spoofed and untrusted CIDs. "Trusted network" simply means that the screening indicators for CIDs are correctly marked as trusted or not. The terminating network must examine the screening indicators to determine how it wishes to treat the CIDs.

With this system, if a trusted network delivers a spoofed CID, it either was not screened (e.g., a call originated on a switch not yet upgraded with screening capability, so the Trust indicator would *not* be set) or it failed screening (so the Trust indicator *would* be set). If a detectably spoofed CID is sent with its indicator set for "screened and passed" or "network provided" and its Trust indicator set, then the sending network is by definition untrusted. It will soon find all of its calls rejected or otherwise getting second-class-citizen treatment.

We expect that sizing of and lookups in this database will not be technically difficult. Any one SS7 node needs to use only as many database entries as there are different networks with which it interfaces. Even if this number were in the thousands, a memory-resident database should not be a problem.

Finally, we merely speculate that the database might be developed to contain other dimensions of trust also, such as records of complaints about carrier fraud.[6]

7.2 Database Maintenance

A principal issue, then, is how this trust database is populated, and on what basis its contents are to be changed. We know of no technical method existing at this writing by which CPNs of calls incoming from another network can be rigorously validated as "belonging" to their respective switches – i.e., remotely checking the screening - (except by actually dialing the CPN). Unfortunately, therefore, it appears that the database cannot be populated automatically but must be maintained manually. The database maintainer must rely on complaints about falsified CIDs.

The next question is, "who is the database maintainer?" One answer is that each carrier can maintain its own database. This allows each carrier to build up its own reputation for quality and integrity. Another answer is that one or more private companies might maintain their own versions of databases and sell their maintenance services to carriers. Database updates would be distributed periodically to subscribing carriers.

Yet another answer is that a single database could be maintained industry wide by a non-profit or government agency such as the FTC or FCC. To ensure "acceptance" of the idea, use of the database could be mandated. Use of a truly neutral maintainer should avoid possible questionable practices such as intentionally "untrusting" a carrier for competitive or other reasons.

To devise an algorithm to keep track of trust for a carrier, we would suggest that, initially, trust be based on the carrier's record. We suppose that a carrier might clean up its act by systematically marking calls originating on its own network and interconnecting carriers as trusted or not. If no "bad CID" complaint is received about a carrier for some interval, that carrier is trusted. When some number of reports are received about spoofed CIDs whose screening indicators were incorrect, that carrier's trust is revoked, possibly after the reports are verified. The database maintainer(s) can devise clever algorithms for how to revoke and re-establish trust based on a network's history.

Database maintenance must be done with appropriate care. Accidental or malicious corruption of the database could have unfortunate implications for callers who happen to use a carrier whose database record is erroneously marked as untrusted (their calls may be rejected by recipients), not to mention the carriers themselves.

Once a network starts screening CPNs for all its originating calls, all its "own" CIDs should be trusted. However, if it acts as a transit network for a call from another network that is untrusted, its only ways to retain its trusted status are either to mark the CPNs from the transit network as untrusted or to stop carrying that other network's calls.

7.3 *Development C*: Transmitting Trust on SS7

We illustrate here how a network node receiving a call can relay trust information to the next network node – either in its own network or in another if it is acting as a transit network. The precise choice of how a Trust indicator is transported is not critical to the use of Trust in handling CIDs at the terminating switch. We propose an extension to the signaling protocol(s), exploiting spare bits in the Calling Party Number Information Element in the SS7 signaling protocol. At some future time the standards bodies may choose to adopt a similar convention

In Q.763, the first octet of the Calling Party Number parameter field contains a bit signaling whether the number of address signals (digits) is odd or even ("O/E" bit) and seven bits indicating the "Nature of address." Of these seven bits, the least-significant three are used for signaling the type of number and some bits are spare:

Calling party number parameter – octet 1								
7	6	5	4	3	2	1		
0	0	0	0	0	0	0		spare
0	0	0	0	0	0	1		subscriber number (national use)
0	0	0	0	0	1	0		unknown (national use)
0	0	0	0	0	1	1		national (significant) number (national use)
0	0	0	0	1	0	0		international number
0	0	0	0	1	1	0		spare (set differs slightly between ANSI and Q.763)
1	1	0	1	1	1	1		
1	1	1	0	0	0	0		reserved for national use
1	1	1	1	1	1	0		
1	1	1	1	1	1	1		spare

We propose using some of the spare codes (0000101 – 1101111) as a flag to indicate Trust. We suggest simply mapping the standard bits onto "1100000" for this purpose. Then if the most significant bits are masked off, the remaining codes are the standard ones. These codes are spare in both the ANSI and ITU protocols.

To enable a smooth transition to this scheme and to distinguish between networks that support this new standard and those that do not, we propose that the new bits mean "Trusted" as opposed to "Untrusted." Coming from an originating switch, the code without these new bits means that the screening indicator is untrusted: the switch has not been upgraded to screen CPNs and set these bits properly.

7.4 Transmitting Trust on Other Protocols

To transmit Trust to ISDN CPE or to network equipment interfaced via ISDN, we note that the ISDN CPN IE supports the Screening Indicator in extension octet 3a. This octet has two bits for the Screening Indicator, three spare bits, two

bits for a Presentation Restricted indicator and one bit for an extension indicator. We suggest that bit three, adjacent to the Screening Indicator, can be used to flag "Trusted." Alternatively, a trust code identical to that used in SS7 could be reserved as one value of the spare 3-bit field.

For `protocols used on IP networks such as Session Initiation Protocol (SIP) and H.323, we suggest that experts in protocol interworking propose ways to support this trust indicator.

7.5 *Development E*: Operating with the Trust Indicator

With a protocol mechanism adopted, a network SS7 node receiving a CPN for a call from another network will then look up that other network in its trust database. If the database returns "untrusted," the node, when it relays the call, must then clear the "trusted" flag field. If the database returns "trusted," the node should do nothing. In this case a trusted upstream network may already have cleared the indicator if it received the call from an untrusted network.

We expect that compliance with the Trust indicator from multiple networks will happen when calls from untrusted networks start showing up with all their CIDs marked as "possibly spoofed." Presumably, non-spoofing customers will apply pressure to get their CIDs marked as trusted. Alternatively, a government mandate could prove convincing.

Note that even if a call originates on a trusted network, it may transit an untrusted one. If it then terminates on a trusted network, its CID will be untrusted, even if the transit network does not modify the CID or trust indicator. To best serve its customers, the originating network can deliver its calls preferentially to trusted transit networks. This should increase motivation for transit networks to get with the program.

We note in passing that a network that screens CPNs could block spoofed-CPN calls "at the source" and terminate the call. This depends on all carriers being trusted – some are not, and may launch spoofed-CPN calls. Additionally, this would not give recipients the opportunity to choose to answer the calls if they desire. We do not propose this solution.

8. Special Cases

8.1 Exceptions

In certain calling situations, spoofed calls may be desirable, both by the calling and called parties. We list here some situations and the technical means to achieve the desired effects.

1) Outbound call centers calling for clients, using clients' numbers (possibly toll-free – 800, 877, etc.) as CPNs. Technically, this configuration may be similar or identical to that of a robocaller.

2) Business owners calling from mobile phones may want their business numbers displayed as CIDs.

3) Organizations that operate private facilities between distant locations. A caller in city X may call a party in city Y by using private facilities between X and Y, then exiting the private facilities in city Y to make a local call. The caller may want the CID from city X to appear.

These cases can be addressed by provisioning in the phone network. The switches to which these services, phones, and/or PBXs are connected must list the numbers to be "spoofed" as *valid* for the affected BRIs/PRIs. For our Development I, the phone company must establish a process to provision the numbers and to change them that is both expedient and rigorous in ensuring absence of fraud. After such provisioning, the "spoofed" CPNs will pass screening.

4) Answering services that answer incoming calls and forward them to clients; they desire to use the incoming CID as the outgoing CPN.

One cannot know in advance what CIDs will call clients, so the CPNs cannot be provisioned in switches. This is a good case to allow spoofing based on a "promise" of the subscriber (the answering service) to provide an accurate CID. Clayton[7] notes that this was tried in the UK for VoIP calls, but abuse followed. However, this case may be as simple as not assigning spoofed-call checking to clients; however, the clients will be susceptible to spoofed illegal robocalls.

5) Law enforcement needs to make spoofed-CID calls.

6) Other legitimate callers, such as some kinds of shelters, need to make spoofed-CID calls.

These special situations probably need a unique feature specifically designed for them. The feature would allow any number to be spoofed with no way for the receiving end to detect the spoofing. Legal safeguards and a detailed audit trail, available through legal process, need to be implemented.

8.2 International Originations

Calls from international locations arrive on an international interexchange carrier; in principle, they should be treated no differently than calls carried by a domestic interexchange carrier. The international carrier has the responsibility to ensure that CPNs of calls it carries are appropriately screened at their origins. If it cannot, it must mark the unscreened CPNs of internationally arriving calls as untrusted. If it cannot do this, it will be untrusted, and some of its calls may be unanswered or blocked.

The foregoing notwithstanding, we note that international gateways have an opportunity to do screening. If a call from an international origin has a CPN conforming to a North American Numbering Plan number, the CPN is spoofed. The gateway SS7 node can itself alter the screening indicator for such a call to "10" and Trusted. Situations such as international outbound telemarketing centers need to be treated as in the previous section, by network provisioning.

8.3 Spoofing Services

Spoofing services, accessible to their customers through, e.g., toll-free numbers, will be identifiable through this new feature. Their outgoing calls will fail screening – the "user-provided" CPN will fail screening against the billing number of the spoofing service. Unless such a service qualifies for exception status, its calls will be blocked or identified as spoofed to called parties, as will any call with a spoofed CPN.

8.4 Possible Issues

Illegal robocalling is not a trivial problem, and it would be foolish to imagine that a short proposal can even identify all the issues that will arise, much less resolve them. We have noted a few issues needing consideration.

1) Interactions. Any new feature introduced on a telephone switch needs to be examined for how it is to interact with existing features. Some existing features relevant to this proposal include:
    a) Call forwarding – several variations such as "all calls," "busy/no-answer," etc.
    b) Call waiting.
    c) Voice mail.
    d) Custom Local Area Signaling Services. These assume trusted CIDs; they need to use the new Trust indicator.
    e) Number portability.
2) Future extension to services such as ENUM.
3) Can carriers allowing CPN spoofing be penalized somehow through the intercarrier compensation system?
4) Illegal robocallers might exploit originations from non-SS7-equipped switches that cannot provide CPNs. However, FCC data8 as early as 2007 indicate that only 24 of 12347switches nationwide are not SS7 equipped.

9. Evaluation and Conclusion

We feel our Proposal meets or exceeds all requirements of the Competition.

9.1 Does It Work?

We feel it does.

9.1.1 Success Rate

- How successful is the proposed solution likely to be in blocking illegal robocalls? Will it block wanted calls? An ideal solution blocks all illegal robocalls and no calls that are legally permitted. (For example, automated calls by political parties, charities, and health care providers, as well as reverse 911 calls, are not illegal robocalls.)

This solution will block any robocall with a spoofed CID or, if desired, identify the CID as spoofed. *Legal* automated calls with valid CIDs will *not* be blocked. Otherwise-legal robocalls with spoofed CIDs *will* be blocked. In the unlikely event an illegal robocaller uses a valid CID, some such calls will not be blocked. If subscribers immediately dial a (new) code to register the CID, subsequent calls to the same subscriber with the same valid CID will be blocked or identified as a robocall and authorities can start legal proceedings.

9.1.2 What Phones Are Protected?

- How many consumer phones can be protected? What types of phones? Mobile phones? Traditional wired lines? VoIP land lines? Proposals that will work for all phones will be more heavily weighted.

All consumer phones will be protected – wired and mobile – as long as the carriers implement our proposed solution. Calls through a LEC or CLEC to VoIP landlines should get the same protection as any other phone.

9.1.3 Supporting Evidence

- What evidence do you already have to support your idea? Running code? Experiments? Peer-reviewed publications?

The success of existing call screening features based on Local Area Signaling Services supports these claims.

9.1.4 Methods of Circumvention

- How easy might it be for robocallers to adapt and counter your scheme? How flexible is your scheme to adapt to new calling techniques? How have you validated these points? Remember that the real test of a security system is not whether or not you can break it; it's whether or not other people can.

Once this method is implemented and in place, the only way an illegal robocall can complete will be to have a valid CID. For these calls we depend on recipients to report the calls and on enforcement authorities to stop them.

9.2 Is It Easy to Use?

We feel it is.

- How difficult would it be for a consumer to learn to use your solution?

Use of the solution is simple, both for called parties and for callers. Once provisioned, a consumer need do nothing. They should just stop getting illegal robocalls. They may, but need not, report any illegal calls they get with a valid CID via the new dialed-code feature. If they choose to see CIDs, they may need to understand some new characters that will appear on their Caller ID display. Legal callers will hear nothing new and need not change their behavior in any way.

- How efficient would it be to use your solution, from a consumer's perspective?

Use of this solution is highly efficient for consumers – they have nothing to do except report the rare illegal robocalls they get with valid CIDs. Most callers will not be aware of the solution, in contrast to a one-size-fits-all "dial-through" feature invoked on every call that would block legal robocalls, may confuse some callers, would work only with DTMF calling phones, and typically gives instruction in only one language. Dial-through, if used in our Proposal (see 6.2), is targeted to a few callers with an unfortunate choice of service providers.

- Are there mistakes consumers might make in using your solution, and how severe would they be?

Consumers with Caller ID displays who have chosen to be sent all calls might misinterpret new characters sent to identify invalid CIDs. This could result in their answering an illegal robocall or in not answering a legitimate call for which at least one carrier is untrusted.

- How satisfying would it be to use your solution?

We feel consumers will get great satisfaction from using this solution. Either the illegal robocalls will simply stop, or a consumer may choose to see Caller ID displays of CIDs that are spoofed, and smugly decline to answer the calls. A choice not to answer will not complete the call, unfortunately, so the robocaller may not be charged.

- Would your solution be accessible to people with disabilities?

This solution is accessible to anyone who can use a phone.

9.3 Can It Be Rolled Out?

We feel it can.

- What has to be changed for your idea to work? Can it function in today's marketplace? (E.g., Does it require changes to all phone switches world-wide, and require active cooperation by all of the world's phone companies and VoIP gateways, or can it work with limited adoption?) Solutions that are deployable at once will be more heavily weighted, as will solutions that give immediate benefits with even small-scale deployment.

Naturally, changes will be incremental. Any network introducing our solution will immediately reduce illegal robocalling from within itself. As its neighbor networks adopt our solution, reductions in illegal robocalls will accelerate. Perfect functioning of our solution at some future time for every phone in the nation requires its eventual adoption by any local exchange and inter-exchange carrier that can host a robocaller. Carriers that do not adopt these changes may, after a suitable introduction period, find themselves labeled as untrusted and lose traffic accordingly.

- Is deployment economically realistic?

This is a difficult question because it is unclear if ***any*** solution is economically realistic. One must ask who benefits economically from deploying a solution. The major players, the carriers, must pay for network upgrades, then will *lose* traffic, hence revenue. This loss is probably the single largest economic impact of solving this problem, other than that of the robocallers themselves. Equipment suppliers may make some profit by developing solutions. Telephone subscribers benefit first because illegal robocalling scams such as was recently stopped by the FTC[9] will be curtailed or stopped, and second by not spending time answering illegal robocalls. These benefits are hard to quantify.

We see a few options to overcome this troubling issue. First, one can ask consumers to pay (e.g., a monthly fee) for the "block illegal robocalls" feature. This option may be a tough sell because i) Caller ID delivery is typically a premium service and subscribers pay extra for it, raising a legitimate expectation that the phone company, through its published tariffs, has an obligation to ensure that caller ID information is accurate, and ii) the calls are *illegal* – consumers may feel it is up to law enforcement to stop them and why should *they* pay? A second option is to mandate implementation. Carriers would be required to provide the feature free to any subscriber who asks. The costs would be hidden and borne by everyone through increases in residential phone rates. The precedent here is that blocking of Caller ID delivery is mandated and free. A third option, probably the most satisfying, is to force the robocallers themselves to fund whatever solution is chosen through fines and penalties for their illegal behavior.

The foregoing discussion does not address what may be the intent of this question – what does our solution cost? We estimate this roughly based on our experience in planning the development of switching features. Our proposal is a software solution requiring several significant software developments and deployments:

1) Feature developments in switches that interface with customers:
   a) On originations, screening of customer-provided CPNs and setting Screening Indicators.
   b) Ability to provision multiple numbers to pass CPN screening (see 8.1).
   c) New terminating treatments for calls with new Trust indicators and spoofed CIDs.
   d) A new "*99"-like feature to enable customers to report possible illegal robocalls.
2) Development in common-channel signaling points that interface with other networks. CCS message content (the CPN IE) must be examined and modified if from untrusted networks.
3) A database, possibly nationwide, for the new vertical service code ("*99"-like) feature must be developed and a protocol for communication with it must be worked out.
4) A Trust database, possibly nationwide, must be implemented, including a protocol for distributing its contents to SS7 signaling points. Algorithms for revoking and restoring Trust for carriers need thinking through.

Development of these features will probably run $3-5M for any manufacturer doing them all; we estimate a total cost between $20-50M for development and deployment, or no more than about $0.50 for each of the nation's over 114,000,000[10] phones.

Additionally, there is the cost of operation and maintenance of the two databases we have proposed. We cannot give authoritative estimates here, but note that these costs could be directly subsidized by the savings they will effect for regulatory and law enforcement agencies in quickly identifying and gathering statistics on illegal robocallers.

Finally, there is a hidden cost in processing capacity of switching equipment. New features use existing capacity and may detract from busy-hour capacity. In some situations this may require installing additional equipment.

- How rapidly can your idea be put into production?

Based on our experience in switching-system development, we expect deployment between six months and one to two years after a decision is made to proceed.

9.4 Our Three Goals

In summary, we feel we have achieved our three goals:

We have created a solution that will block illegal robocalls on landlines and mobile phones while allowing legal robocalls to complete normally.

We have proposed to allow individual subscribers to handle illegal robocalls themselves if they desire.

In blocking the calls and proposing a financial disincentive to make blocked calls, we have a way to cause illegal robocalls to possibly cost more than they return to illegal robocallers. Perhaps this will end the problem.

9.5 Addendum – Note on FCC report

In closing, we note that our Proposal would resolve several of the concerns expressed[11] by the FCC Chairman regarding Call Identification Information.

---

[1] http://en.wikipedia.org/wiki/Caller_ID_spoofing

[2] See http://transition.fcc.gov/wcb/ppd/IntercarrierCompensation/, also, e.g., Congressional Research Service, CRS Report RL 32889: http://digital.library.unt.edu/ark:/67531/metacrs9128/m1/1/high_res_d/RL32889_2005Apr28.pdf

[3] http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=282
http://business.highbeam.com/435358/article-1G1-56079651/caller-id-use-soars-among-all-income-levels

[4] See discussion thread in comp.dcom.telecom or telecom digest 23 Nov. 2011, MSNBC/NYT: Caller ID Forging. We acknowledge use of some information in this thread.

[5] After our ideas were worked out, we discovered a previous related but less comprehensive suggestion for transmitting trust. See: http://massis.lcs.mit.edu/telecom-archives/archives/back.issues/recent.single.issues/archive2.php?volume=28&issue=154.

[6] International Interconnection forum for services over IP (i3 Forum), "Fraud classification and recommendations on dispute handling within the wholesale telecom industry," Release 1.0, April 2012. www.i3Forum.org

[7] Richard Clayton, "Can CLI be trusted?," J. Information Security Tech. Report, 12, #2, June 2007, pp74-79. Available as a preprint at http://www.cl.cam.ac.uk/~rnc1/cli.pdf

[8] See http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-287688A12.pdf , linked by http://transition.fcc.gov/wcb/iatd/monitor.html

[9] See http://www.ftc.gov/opa/2012/12/cubanexchange.shtm.

[10] http://quickfacts.census.gov/qfd/states/00000.html

[11] Julius Genachowski, Chairman, Federal Communications Commission, Report DA 11-1089, Caller Identification Information in Successor or Replacement Technologies, June 22, 2011.