ATIS-0300114

ATIS Standard on -

Next Generation Interconnection Interoperability Forum (NGIIF) Next Generation Network (NGN) Reference Document Caller ID and Caller ID Spoofing

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0300114

ATIS Standard on

Next Generation Interconnection Interoperability Forum (NGIIF)
Next Generation Network (NGN) Reference Document
Caller ID and Caller ID Spoofing

Alliance for Telecommunications Industry Solutions

Approved September 18, 2019

Abstract

This document outlines Caller ID, the issue of Caller ID spoofing, and impacts related to consumers and the network, existing regulatory conflicts, and consumer educational needs.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

K. Riepenkroger, NGIIF Co-Chair (Sprint)

R. Ryan, NGIIF Co-Chair (Comcast)

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Caller ID and Caller ID Spoofing

1 Scope, Purpose, & Application

1.1 Scope

This document discusses Caller Identification (Caller ID) services, Caller ID spoofing issues, and operational impacts of illegitimate Caller ID spoofing.

1.2 Purpose

The purpose of this document is to offer operational strategies that enhance the integrity of legitimate Caller ID.

1.3 Application

This document is a standalone document. Additionally, there is a full suite of Next Generation Network (NGN) reference document guidelines available in ATIS-0300104, *Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability.*

2 Informational References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0300104, *Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability*.[1]

IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*.[2]

U.S. Senate Committee on Commerce, Science, & Transportation. *Stopping Fraudulent Robocall Scams: Can More Be Done?* Hearings, July 10, 2013.[3]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/>.

[2] This document is available from the Internet Engineering Task Force (IETF). <http://www.ietf.org>

[3] This document is available from the U.S. Senate Committee on Commerce, Science, & Transportation at <

https://www.commerce.senate.gov/public/index.cfm/hearings?ID=C1EEC086-3512-4182-AE63-D60E68F4A532 >.

"Truth in Caller ID Act of 2009." (47 U.S.C. 609 note).[4]

GR-31-CORE, *CLASS Feature: Calling Number Delivery*.[5]

ATIS-1000067, *IP NGN Enhanced Calling Name (eCNAM)*.[1]

GR-1188-CORE, *CLASS Feature: Calling Name Delivery Generic Requirements*.[5]

"Communications Act of 1934." (47 U.S.C. § 151).[4]

"Telephone Consumer Protection Act of 1991 (TCPA)," (47 U.S.C. § 227).**Error! Bookmark not defined.**

U.S. House. 113th Congress, 1st Session. H.R. 3670, *Anti-Spoofing Act of 2013*, 2014.[6]

M3AAWG. *Best Practices to Address Online, Mobile, and Telephony Threats*, June 1, 2015.[7]

"Telemarketing Sales Rule (TSR)," 68 Federal Register 4580 (Jan. 29, 2003), (16 C.F.R. Part 310).[8]

"Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994," (15 U.S.C. §§ 6101-6108).[8]

"Federal Trade Commission Act of 1914" (15 U.S.C §§ 41-58, as amended).[8]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < https://glossary.atis.org >.

3.1 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
Caller ID	Caller Identification
CNAM	Calling Name
CND	Calling Number Delivery
CPE	Customer Premise Equipment
CPN	Calling Party Number
eCNAM	Enhanced Calling Name
FCC	Federal Communications Commission
FTC	Federal Trade Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
M3AAWG	Messaging Malware Mobile Anti-Abuse Working Group

[4] This document is available from the U.S. Government Publishing Office at < https://www.gpo.gov >.

[5] This document is available from Telcordia Technologies at < http://telecom-info.telcordia.com >.

[6] This document is available from the Library of Congress at < http://www.loc.gov >.

[7] This document is available from the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) at < https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf >.

[8] This document is available from the Federal Trade Commission (FTC) at < http://www.ftc.gov >.

MIME	Multipurpose Internet Mail Extensions
NGIIF	Next Generation Interconnection Interoperability Forum
NGN	Next Generation Network
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switching Transition Network
RFC	Request for Comments, an IETF publication
SHAKEN	Signature-based Handling of Asserted Information Using toKENs
SIP	Session Initiation Protocol
SP	Service Provider
TCPA	Telephone Consumer Protection Act of 1991
TDoS	Telephony Denial of Service
TN	Telephone Number
TSR	Telemarketing Sales Rules
VoIP	Voice Over Internet Protocol

4 Caller ID Services

Caller ID is the marketing name for a Calling Number and/or Calling Number+Name service offered by Service Providers (SPs). While there are many terms used to refer to this service, (e.g., Calling Line Identification Presentation and Calling Line Identity/Identification), Caller ID is defined in the ATIS Telecom Glossary as “a network service feature that permits the recipient of an incoming call to determine, even before answering, the number from which the incoming call is being placed.”

These services were originally offered to Plain Old Telephone Service (POTS)/Time Division Multiplexing customers. With the migration to Internet Protocol (IP)-based networks, similar services were implemented using new signaling protocols.

4.1 Types of Caller ID Services

4.1.1 Calling Number Delivery (CND)

CND is an incoming feature that allows business or residence customers to have the calling party’s number (CPN), data, and time of the incoming call delivered to their customer premise equipment (CPE) during the silent interval between the first and second rings. If the calling party’s number is “anonymous” or unavailable, an indication of each will be displayed on the customer’s CPE. CND is a POTS service described in GR-31-CORE, *CLASS Feature: Calling Number Delivery*.

4.1.2 Calling Name (CNAM)

CNAM provides the name associated with the CPN of an incoming call. The name is retrieved from a database and is delivered to the customer’s CPE during the silent interval between the first and second rings (along with the number if the customer subscribes to both services). If the CPN is anonymous or unavailable, then name information will not be provided, and an indication of anonymity or unavailability will be displayed on the customer’s CPE. The length of the display field for the name is 15 characters. CNAM is a POTS service described in GR-1188-*CORE, CLASS Feature: Calling Name Delivery Generic Requirements*.

4.1.3 IP-Based Identity Services

In the NGN, the calling name and number may be delivered via SIP INVITE.[9]

4.1.4 Enhanced Calling Name (eCNAM)

Enhanced Calling Name delivers an extended name, longer than 15 characters, along with additional data elements about the originating party. The IP-based service and method of delivery (via SIP INVITE) are described in ATIS-1000067, *IP NGN Calling Name (eCNAM)*. Delivery of more data about the caller could help protect and empower the called party as he/she manages incoming calls.

5 Maintaining the Integrity of Caller ID

Technological changes have allowed callers to manipulate Caller ID, i.e., Caller ID spoofing. The *Truth in Caller ID Act*[10] makes it illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.

This clause discusses potential techniques for maintaining Caller ID integrity that are under consideration by multiple industry forums. Currently there is no technical solution to certify the legitimacy of the Caller ID; however, this clause points out techniques that are being developed within the industry and discussed in various industry groups: certification and verified tokens.

5.1 Certification

Work under the Internet Engineering Task Force (IETF) has been completed on “Authenticated Identity Management in the Session Initiation Protocol (SIP)”, RFC 8224. Figure 5.1 is an example of a basic use case for a SP implementation for Caller ID certification.[11] The complete details on the authentication and verification in the context of SHAKEN are defined in ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN).*

Originating Service Provider Certificate Management is detailed in ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management.*

[9] ATIS-1000067, *IP NGN Calling Name (eCNAM)*.

[10] The *Truth in Caller ID Act 2009* amends Section 227 of the *Communications Act of 1934* (47 U.S.C. § 227).

[11] IETF RFC RFC8224, *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*.

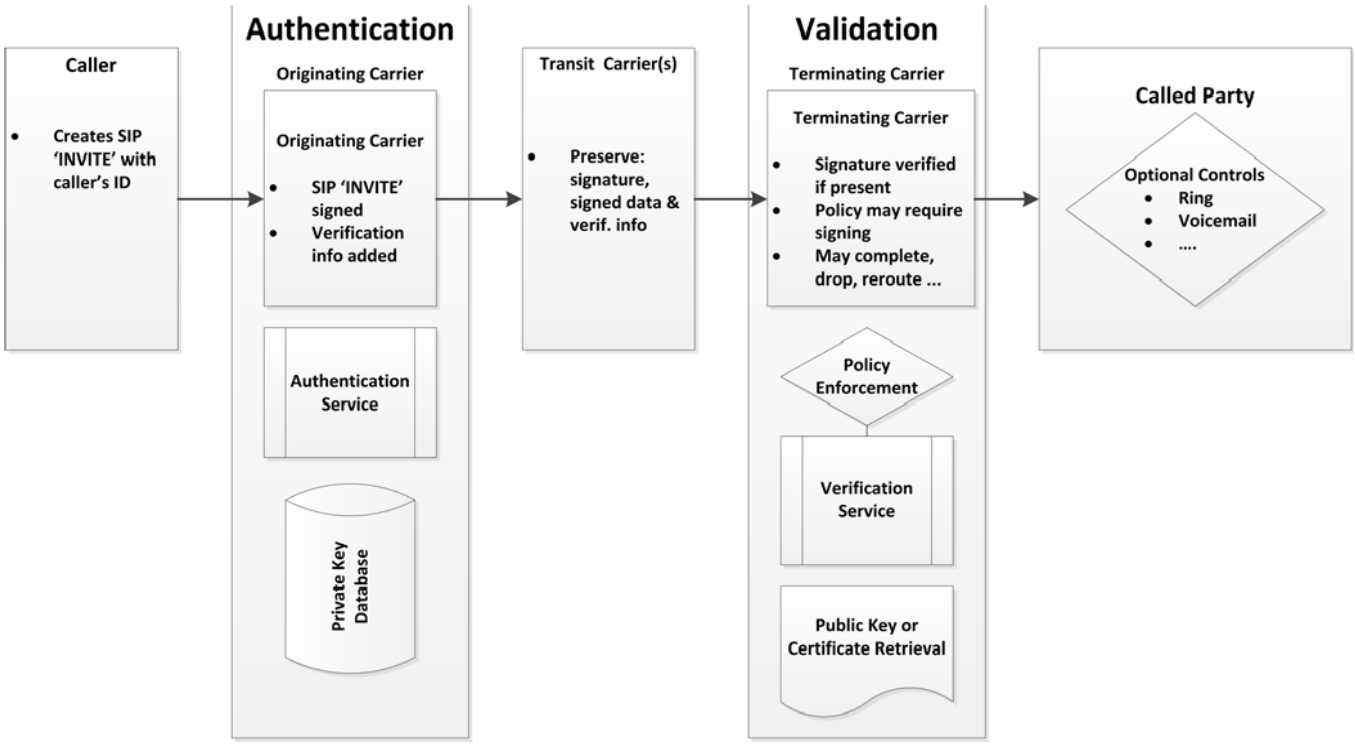

Figure 5.1: Basic Use Case for Service Provider Implementation for Caller ID Certification

6 Table Relationship between Caller ID Spoofing & Robocalls

Robocalling/voice broadcasting is the most common form of an autodialer service. It is typically used for calls related to sales, marketing, or polls, but robocalling may also be used to scam consumers or for other illegitimate purposes. Not all robocalls are spoofed; and not all spoofed calls are robocalls (as shown in Figure 6.1).

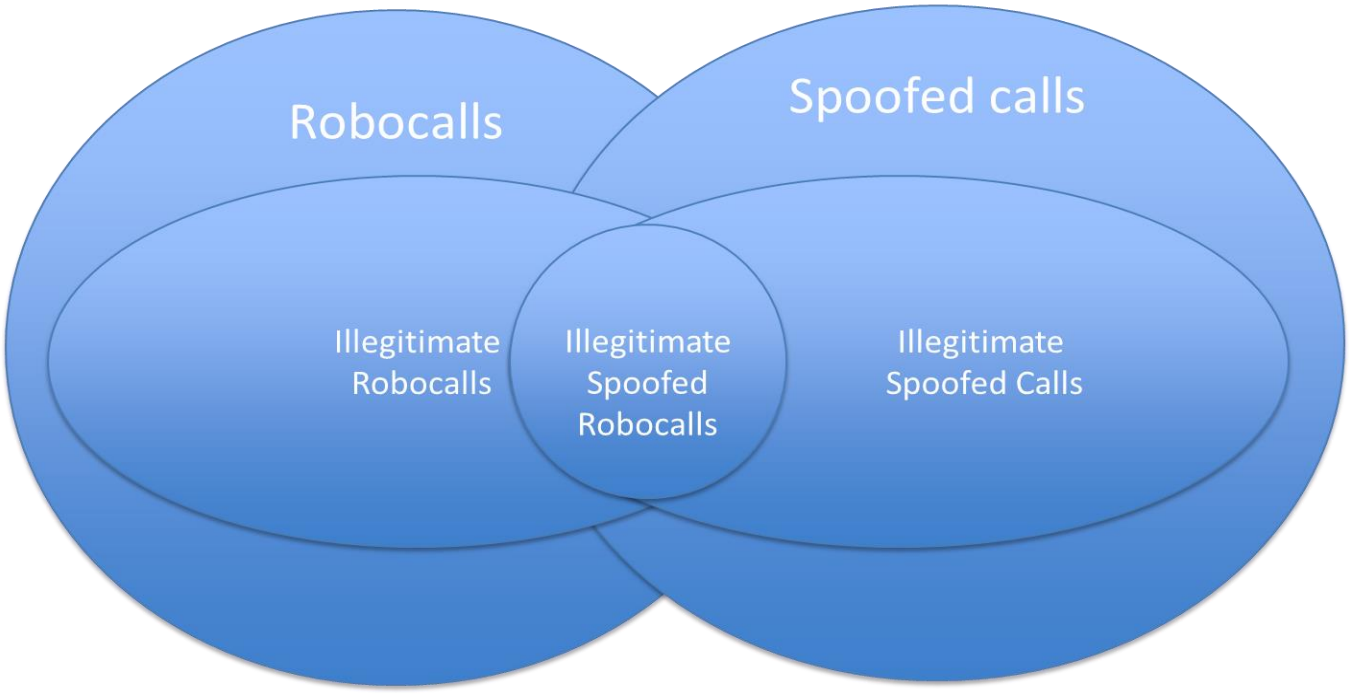

Figure 6.1- Types of Spoofed and Robocalls

7 Examples of Caller ID Spoofing

The *Truth in Caller ID Act* prohibits spoofing, or deliberately falsifying the telephone number (TN) and/or name relayed as the Caller ID information to disguise the identity of the caller ***for harmful or fraudulent purposes***. However, the *Truth in Caller ID Act* only applies to the United States. The following are some examples of potential illegitimate Caller ID activities involving spoofing:

- Reflection spoofing - i.e., spoofing the called TN in the Caller ID.
- Random number generators providing spoofed TN.
- Calling patterns that may be indicative of illegitimate spoofing:
  - Same TN with many calls to different numbers within a short period of time.
  - Same TN sequentially calling large blocks of TNs.
- Phantom traffic - i.e., calls terminating in which the Caller ID information has been stripped or altered potentially creating billing issues.
- Local or long distance spoofed TNs resulting in call backs to the TN (i.e., individual or business) that was spoofed.
- Spoofing the TN, then hacking into the user's voice mail account and gaining access to the user's voice messages. Neighbor spoofing - i.e., Same NPA-NXX as the called number.
- Unallocated, unassigned and invalid TN spoofing.
- Prank numbers (e.g., 911-NXX-XXXX) or other malicious activity.
- Use of random spoofed TNs for the purpose of Access stimulation for parties that benefit from toll-free TN revenue.

7.1 Comparative Call Types Where Spoofing May Occur

Examples of the impacts of spoofed robocalls are identified in Table 8.1, *Robocall Matrix* in ATIS-0300105, *Autodialer Reference Document*. In addition to this table, Table 7.1 provides examples of the impacts of spoofing.

This table is for illustrative purposes and should not be considered an all-inclusive list.

Table 7.1 - Types of Calls Where Caller ID Spoofing May Occur

	Uses	Low, Medium, High - Risk and Impacts		
		Consumer Impact		
		Potential to Block E911 Calls		Network Congestion
Legitimate Uses	Domestic Violence Shelters	low	low	low
	Hospital Call Back	low	low	low
	Doctor's Offices	low	low	low
	Answering Services	low	low	low
	9-1-1 Call Back	low	high	low
	Telemarketers	low	med	med
	Newspaper Reporters	low	low	low
	Certain Businesses and Government Announcements	med	med	med
Illegitimate Uses	Illegally Changed/ Deleted/ Augmented Caller ID	low	high	low
	International Revenue Sharing Fraud	low	low	low

Table 7.1 Legend

- High: Has high potential of experiencing the risk or impact.
- Medium: Has medium potential of experiencing the risk or impact.
- Low: Has low potential of experiencing the risk or impact.

7.2 Spoofing a U.S. Number from an International Location

From an enforcement perspective, both the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) have indicated the major challenge they encounter with combating international illegitimate spoofed calls and robocalls is that even if law enforcement manages to identify the call source, the FCC and FTC lack jurisdiction to pursue the initiator of the international call.[12]

One-ring scams are a frequent form of illegitimate spoofing from an international location:

"Wireless consumers receive robocalls from phone numbers with area codes that spoof domestic numbers but are actually associated with international pay-per-call phone numbers. These robocalls usually disconnect after one

[12] Both FCC and FTC testimony to the Senate indicated that much of the challenge in effectively combating fraudulent robocalls from an enforcement standpoint is that the calls are often originating overseas and even if they manage to find the source, they are powerless to go after them. For reference, see a provision in H.R. 3670, the *Anti-Spoofing Act of 2013*, as passed by the House in September 2014. A provision in H.R. 3670, the *Anti-Spoofing Act of 2013*, as passed by the House in September 2014, addresses the requirement that the call spoofing prohibition applies to VoIP providers that enable only outbound calls.

ring, not giving the consumer time to answer the call and tempting them to return the call. Customers who return these calls drive extra traffic to these foreign carriers, and the scammer may receive a portion of the terminating charges (or possibly premium charges) that the foreign SP collects from the wireless customer's carrier."[13]

8 Impacts of Caller ID Spoofing & Robocalls

Caller ID spoofing and robocalls can impact SPs' networks and their consumers. This can pose serious network and financial impacts to SPs, resulting in improper sizing of network growth and millions of dollars in lost revenue.

8.1 SP Impacts

Currently, SPs have no real-time visibility into the possible spoofing of calls transiting their network. At the time of the call, an SP has no way to determine whether such a spoofed call is illegitimate or legitimate. The SP may only see the call that is processing on their network. After the completion of the call, SPs have investigated techniques that can positively identify whether a call has been spoofed.[14]

Illegitimate Caller ID spoofing can have undesirable impacts to SPs, such as:

- Improper sizing of network growth;
- Increase in consumer complaints;
- Increase in call center contacts;
- Potential billing issues.

8.2 Network Congestion

SPs' networks are engineered to minimize network congestion conditions which could impact the ability of the consumer to make and receive telephone calls. The engineering of these networks is based on the theory that the future behavior of the network will be similar to past behavior and include a small margin for network growth. SP network congestion will occur whenever actual conditions exceed these assumptions and an alternate route is not available. The magnitude and scope of the network congestion depends on the magnitude and scope of the associated event. Table 1 illustrates the potential for illegitimate Caller ID spoofing to negatively impact SPs' networks and cause network congestion.

8.3 Blocking E911 Calls

Illegitimate Caller ID spoofing of a Public Safety Answering Point's (PSAP) legitimate TN could result in undesirable impacts, including a total telephony denial of service (TDoS) for the PSAP. Such events could occur if a number of the called parties return the call to the PSAP. This could be prevalent when a PSAP's 911 trunks are limited in size. The operational problem is exacerbated in the event of a true emergency situation wherein legitimate 911 calls fail to reach a PSAP due to a TDoS attack or loss of service event. This hinders SPs' ability to fulfill the legal requirement of restoring all emergency services impacting national security in a timely fashion.

8.4 Consumer Impacts

Illegitimate Caller ID spoofing is often used for activities that have an undesirable impact on consumers, such as:

- Identity theft;

---

[13] M[3]AAWG. *Best Practices to Address Online, Mobile, and Telephony Threats*, June 1, 2015, p. 48 < https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf >.

[14] U.S. Senate Committee on Commerce, Science, & Transportation, *Stopping Fraudulent Robocall Scams: Can More Be Done?* Hearing, Testimony of Kevin Rupy, Senior Director, Law and Policy, United States Telecom Association, July 10, 2013 < http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=46937fbc-0560-4bd7-8cb8-6401a88543bf >.

- Financial loss;
- Loss of confidence in SP;
- Loss of confidence in telecommunication services;
- Safety concerns.

Since Caller ID spoofing is not always illegitimate, consumer education is important to minimize confusion and help understand potential impacts.

8.5 Personnel & Consumer Education from SPs

Call Spoofing Best Practices for Consumer Interactions:

- Provide education to SP personnel on Caller ID, the legitimate use of call spoofing [as allowed in the *Telephone Consumer Protection Act of 1991* (*TCPA*)], as well as the issues associated with the illegitimate use of call spoofing.
- Ensure processes, as well as training, are well documented and in place for front-line personnel to be equipped to easily address concerns regarding call spoofing raised to them by customers.
- Areas to be considered for this coverage on call spoofing are the front-line business office or other in bound call centers, online access for customers, and repair and technical support in in bound centers.
- Call center personnel are best prepared to address Caller ID spoofing concerns with the appropriate processes, training, and documentation, allowing personnel to offer customers an explanation of spoofing and options they can make use of to address Caller ID spoofing.
- Consumer education could be initiated in SP communications (inserts in monthly bills), email alerts and website pop-ups.

Potential Documentation for Consumer Training:

- A simple understandable explanation as to what Caller ID spoofing is, such as “Caller ID spoofing is the practice of using technology to display a different person’s name and number information on Caller ID units when making a call.” It is important for customers to know that there are legitimate uses for Caller ID spoofing, such as domestic violence safe houses, hospital rooms, newspaper reports, law enforcement, and doctor’s cell phones. Telemarketers and call centers will also show a telephone number different from the calling number to provide consumers with an appropriate call back number. It is important to provide information that the misuse of call spoofing happens when the calling number changes the Caller ID to a random number or the dialed number in order to increase the probability that the call will be answered.
- SPs will want to consider in the training that it is not possible currently for the SP to prevent callers from spoofing Caller ID information, and, if appropriate, advise that the SP does not sell customer names and numbers to third-parties.

SPs may also want to advise their customers of various services available to them (e.g., no solicitation service, *57,[15] selective call rejection, third-party applications, online account management, etc.). SPs should advise customers that calling parties that spoof Caller ID generally use specialized Internet software, and a spoofed call can originate outside the customer’s SP’s network or is not carried on the customer’s SP’s network. As a result, spoofed calls are, in those cases, untraceable and SPs face difficulty in working to stop them.

Scripted documentation provides front line personnel the best opportunity to correctly address customers’ concerns and provide them with options that may help reduce the impacts of the robocalling issues. Options will vary by SP, and any costs should be discussed with the customer. Here are some options to consider:

[15] This is a landline, switch-based Class feature.

1. **Change of TN**. Not everyone is eager to change their phone number, but this can be a useful solution for some consumers.
2. **Use a calling feature to block incoming calls**. SPs may offer a variety of privacy-focused calling features depending on SPs' service offerings that customers might find useful.
3. **If appropriate, offer to trace the harassing calls**. It is usually difficult to trace spoofed calls. However, if that is appropriate and is done, SPs may then have other information that leads them to further investigate the harassing calls, including working with law enforcement.
4. **Get a non-published (private) listing**. If the consumer uses a SP that publishes their TN in a print or web directory, the consumer may wish to request a private listing where the name, address and phone number are not included in the printed or web directory and aren't available through Directory Assistance.

Some SPs may have specified Annoyance Call Bureaus or security teams to address issues such as these. Customers who continue to have concerns after their contact with front line personnel or online resources can be referred to that group for additional assistance depending on SPs' specific processes. Customers may be asked to share any relevant information such as the dates/times they received spoofed calls and other appropriate specificity for the investigation of the calls. Annoyance Call Bureaus or security teams can provide valuable efforts to address these concerns, such as:

- Provisioning and monitoring call tracing equipment on customers' telephone services.
- Tracking, translating, and identifying call sources through central office switching locations, network monitoring, and analysis systems.
- Utilizing billing, address, and facilities systems to identify call sources when possible.
- Working directly with long distance, local exchange carriers, wireless, and various other communication SPs and annoyance call bureau departments nationwide and in Canada.
- Working with law enforcement on releasing identified party information.
- Contacting identified parties on behalf of customers where appropriate to resolve problems ranging from life threatening or harassing calls to computer generated and auto-dialed calls, spoofing, blast faxes, and any other annoyance call types identified by customers.
- Communicating with customers regarding billing, tariff requirements relating to areas such as *57 activity, and FCC regulations.

8.6 Consumer Education from Other Sources

There are many sources other than SPs that provide information to educate consumers on Caller ID and Caller ID spoofing, such as the following government agencies and consumer groups:

- FTC: http://www.consumer.ftc.gov
- FCC: https://www.fcc.gov/spoofing
- Better Business Bureau: http://www.bbb.org
- Consumer Union: http://consumersunion.org
- The National Cyber Security Alliance: http://www.staysafeonline.org
- Federal Bureau of Investigation: https://www.fbi.gov/scams-safety/be_crime_smart
- Internal Revenue Service: http://www.irs.gov

9 Regulatory Environment

This clause describes various FCC rules and regulations, as of the date of publication of this document, with the intent to assist with investigating and/or mitigating some of the issues addressed herein. Noted references are not

all-inclusive, do not intend to provide legal guidance and, based on date of this document, may have been subsequently revised. State commissions may also have issued rules and regulations on the subject addressed by this document.

9.1 FCC

9.1.1.1 Telephone Consumer Protection Act (TCPA)

Congress has empowered the FCC to enforce the *Communications Act of 1934*, including the *TCPA*, and the agency's implementing rules and orders, in several ways. For example, the FCC's most powerful tool to enforce compliance with the law is to revoke a license for non-compliance or deny issuance or renewal of the license. The FCC more commonly enforces the *TCPA* and its other rules and orders by imposing monetary penalties.[16]

9.2 FTC

The FTC was specifically directed under the *Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994* to adopt rules prohibiting deceptive and abusive telemarketing acts or practices, including "unsolicited telephone calls which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy." The body of regulations adopted by the FTC to implement the *Telemarketing and Consumer Fraud and Abuse Prevention Act* is known as the *Telemarketing Sales Rule* (*TSR*). The FTC was also empowered generally to address unfair or deceptive acts or practices in or affecting commerce, which the *Federal Trade Commission Act of 1914* declares unlawful.[17] However, the FTC's jurisdiction does not extend to common carriers, which are subject to the regulatory authority of the FCC. For reasons described below, pertaining to both common carrier and privacy obligations, those companies must complete phone calls.

When the *TCPA* was passed in 1991 to address telemarketing robocalls, its primary function was to protect the privacy and public safety interests of telephone subscribers by placing restrictions on automatic dialers, fax machines, and unsolicited automated calls. The *TCPA* amended Title II of the *Communications Act of 1934* to add a new section (§227) entitled "Restrictions on the Use of Telephone Equipment". The nature of the technology being used in 1991 is well-illustrated by the following consumer complaint: "The automated calls filled the entire tape of an answering machine, preventing other callers from leaving messages." Except for amendments to expand the reach of §227 to offshore callers and to prohibit Caller ID spoofing, the robocall provisions of the law remain largely as they were enacted in 1991, but they have become increasingly ineffective.

The original phone network was a "closed" system, meaning that voice services were generally provided by local exchange carriers and long-distance companies through only the Public Switching Transition Network (PSTN). These companies were providing what is called "plain old telephone service" (POTS). When Congress passed the *TCPA* in 1991 to address robocalls, autodialing systems, and certain fax machine problems, and even when it acted again three years later to deal with unsolicited telemarketing calls, wireless communication was only beginning to emerge and even dial- up Internet access was not yet a reality for mass consumer use. Today's communications services are provided not by the historical closed PSTN but by a "network of networks". Voice service is now available from a diverse technical heritage: the PSTN, Voice over IP (VoIP) SP, Internet SPs, cable companies offering phone service, competitive local exchange carriers and wireless SPs, along with "over-the-top" VoIP services (which use existing broadband networks).

A typical mass-calling event will usually transit multiple networks (encompassing both the PSTN and the Internet) before finally reaching the consumer.[18]

---

[16] U.S. Senate Committee on Commerce, Science, & Transportation. *Stopping Fraudulent Robocall Scams: Can More Be Done?* Hearing, Statement of Eric J. Bash, Associate Chief, Enforcement Bureau, Federal Communications Commission, July 10, 2013 < http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=de5998a2-82c0-48cb-827c-819be06776c5 >.

[17] *Federal Trade Commission Act of 1914* (15 U.S.C §§ 41-58, as amended).

[18] U.S. Senate Committee on Commerce, Science, & Transportation, *Stopping Fraudulent Robocall Scams: Can More Be Done?* Hearing, Testimony of Kevin Rupy, Senior Director, Law and Policy, United States Telecom Association, July 10, 2013 < http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=46937fbc-0560-4bd7-8cb8-6401a88543bf >.

The FTC's Robocall Summit on October 18, 2012, made clear that convergence between the legacy telephone system and the Internet has given rise to massive unlawful robocall campaigns.[19]

Each of these SPs must ultimately connect to the PSTN because the reliability of their service to their own customers depends on their ability to deliver any call to anywhere.

- The FTC coordinates with various partners to bring law enforcement "sweeps", i.e., multiple simultaneous law enforcement actions that focus on specific types of telemarketing fraud.[20]
- The FTC does not have criminal law enforcement authority.[21]

In 2003, the FTC responded to enormous public frustration with unsolicited sales calls and amended the *TSR* to create a "National Do Not Call Registry."[22] [23]

10 Conclusion

This document has outlined Caller ID, the issue of Caller ID spoofing, and impacts related to consumers and the network, existing regulatory conflicts, and consumer educational needs. The impacts to the network are felt regardless of whether it is the PSTN, NGN, or hybrid PSTN/NGN. Industry and regulator efforts to identify and eventually implement mitigation techniques for illegitimate Caller ID spoofing are underway and will continue to be monitored by the ATIS NGIIF.

[19] U.S. Senate Committee on Commerce, Science, & Transportation. *Stopping Fraudulent Robocall Scams: Can More Be Done?* Hearing, Prepared Statement of the Federal Trade Commission, July 10, 2013 < http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=aacf57ff-1b70-45c5-9ef1-837ebea0a911 >.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Federal Register 4580 (January 29, 2003), 16 C.F.R. Part 310. The FTC issued the *TSR* pursuant to the *Telemarketing and Consumer Fraud and Abuse Prevention Act*, 15 U.S.C. §§ 6101-6108.