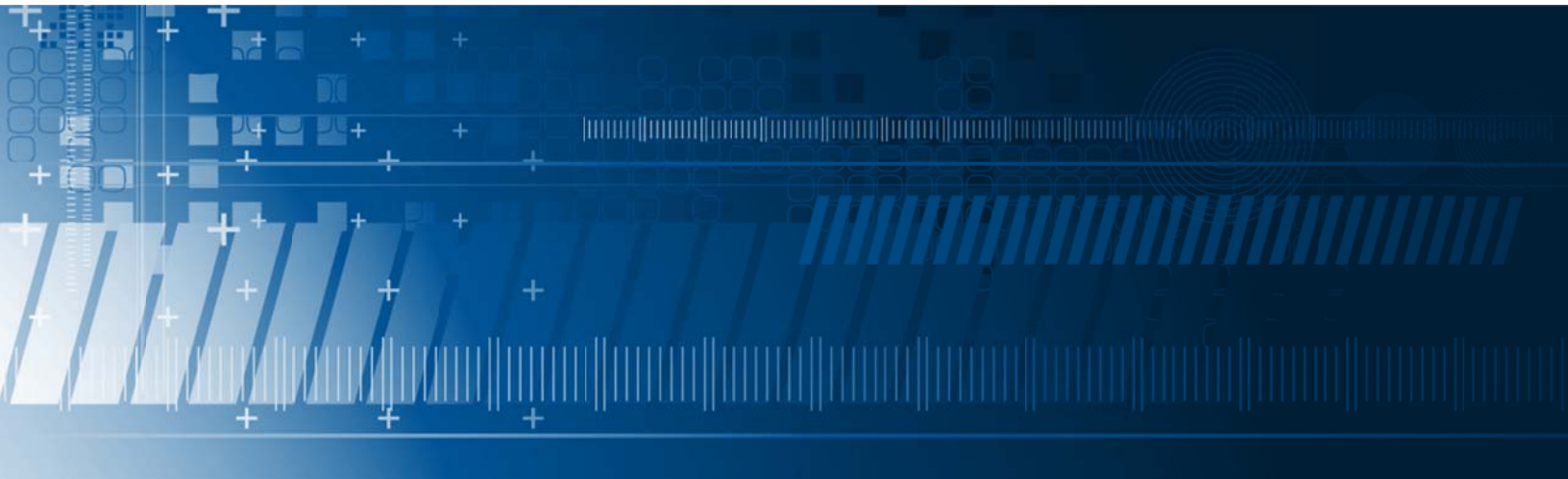
# Calling Party Spoofing Mechanisms and Mitigation Techniques

Alliance for Telecommunications Industry Solutions
April 2016

ATIS-I-0000051



## Abstract

The impact of illegitimate uses of Caller ID spoofing and robocalling presents unique challenges for the industry in addressing consumer concerns with unwanted and fraudulent calls. This paper outlines practical mitigation techniques being developed, and emphasizes Caller ID spoofing is not a static problem that can be solved with a single solution. Rather, a flexible, layered approach (similar to addressing cybersecurity risks) is needed to respond to these evolving threats.

## Foreword

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 and major U.S. contributor to 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

# Contents

# Executive Summary

## Goal

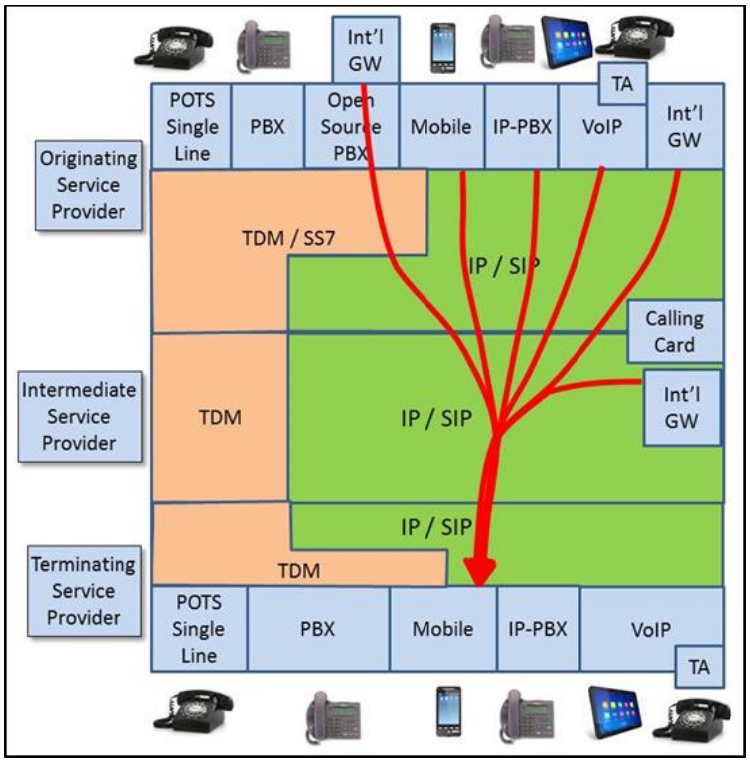
The intent of this paper is to educate and inform the reader regarding the current landscape of Caller ID spoofing and the related issue of robocalling. This document highlights practical mitigation techniques the industry is taking to provide the consumer with meaningful and useful tools.

## Context

The focus of this paper is Caller ID spoofing and its impact on robocalling. Not all robocalls are spoofed, and not all spoofed calls are robocalls. There are also legitimate uses for both robocalls and Caller ID spoofing, so an outright ban would not be appropriate. However, illegitimate uses of Caller ID spoofing increase the impact of fraudulent robocalling and undermine techniques to prevent unwanted robocalls. The end goal is to give consumers the tools to reduce unwanted and fraudulent calls. Mitigating illegitimate Caller ID spoofing will not by itself fully achieve this goal but it will clearly help consumers.

## Calling Scenarios

Voice calls originate and terminate from many different sources and can be transported over two technologies: TDM/SS7 (i.e., "circuit switched"), IP/SIP, or a combination thereof. This creates many possible calling scenarios involving a myriad of technology combinations, so proposing a "solution" for one specific scenario is not realistic. It is more accurate to use the Cybersecurity language of "threat vectors". Mitigation techniques must consider all technology combinations rather than simply focus on the hot problem of the day. Vigilance and flexibility are also needed considering that technology and threat vectors continually evolve. This diagram is complex, but in reality it only provides a very simplified, current picture of the real network complexity that must be considered for every call scenario, 24/7/365.




## Problem Statement

In today's network, terminating service providers do not have the capability to directly verify the accuracy of the calling party number. Signaling information for both SIP and TDM networks includes the calling party number, but this can be spoofed in many ways.

## Mitigation Techniques Currently in Use

A variety of mitigation techniques are already available to help consumers reduce unwanted and fraudulent calls. White lists, black lists, anonymous caller rejection, smartphone apps, voicemail screening, and cloud-based applications are all offered to users by service providers, app developers, and third-party providers. Unfortunately, all of these mitigation techniques rely to some extent on the accuracy of calling party information, which is a primary motivation for the growing illegitimate use of Caller ID spoofing to undermine today's defenses.

## The Way Forward – SIP

The IETF STIR Working Group is developing a mechanism to allow phone numbers to be "signed" at the origin, and "verified" at the termination. ATIS has proposed enhancements to make the approach practical by allowing service providers to perform the "validation" and "verification" on the user's behalf. Approval at the IETF is expected this year, and will set the stage for the following additional steps:

- SHAKEN: Options within protocols could lead to implementations that may not be interoperable. The ATIS/SIP Forum IP-NNI Task Force is developing a profile framework (SHAKEN) setting forth standards to allow for consistent implementation in service provider networks. Completion of this framework is planned for the end of this year.
- Display Framework: A framework is required to allow for the display of validated Caller ID information to end users in a consistent and secure format. The ATIS/SIP Forum IP-NNI Task Force is developing this framework, with the initial deliverable expected by the end of 2016.

## The Way Forward – TDM

No viable mechanism has been proposed to validate and securely transmit real-time Caller ID information in TDM networks. The focus for TDM networks is shifting to forensic analysis, using Call Detail Records (CDR) to trace the call from the termination back to the network of origination to identify the source of fraudulent calls. Today, this is a time-consuming manual process, but the feasibility of automating portions of this traceback process is being evaluated.

## Conclusion

Caller ID spoofing is not a problem that can be fixed with a "silver bullet". If the dike has a leak, a flood can be stopped with a finger, but with a sieve the water simply takes another path. Mandating a single "solution" to Caller ID spoofing would be counterproductive; fraudulent callers would simply adapt to exploit other weaknesses in existing or future infrastructure. Instead a layered approach, similar to that used in cybersecurity efforts, with a range of choices of mitigation techniques, provides the flexibly to respond to an evolving threat. ATIS is playing a key role in developing industry standards for these mitigation techniques in a timely manner.

# Scope & Purpose

## Scope

This white paper will: define, in non-technical terms, Caller ID spoofing and its relationship to robocalling; describe the threat vectors and landscape that make Caller ID spoofing and robocalling problematic; set out use cases for legitimate Caller ID spoofing that must be allowed regardless of mitigation strategies adopted against the practice; enumerate the industry's efforts in developing those strategies; and explain the basic mitigation approaches.

While the paper's principal focus is Caller ID spoofing, it also addresses robocalling, given the close association between these two topics. We encourage the reader to keep this connection in mind, as it entails many aspects, including:

1. Not all spoofed calls are robocalls, and not all robocalls are spoofed; however, there is often a correlation between the two.
2. The ability to illegitimately spoof Caller ID information increases the impact of fraudulent robocalling, and makes techniques to block robocalling less effective.
3. There are legitimate and illegitimate uses of robocalling and spoofing, forcing industry stakeholders to struggle in the development of mitigation techniques for one or both that do not harm valid uses for either.
4. The negative consequences of robocalling span the spectrum from a nuisance to the consumer to potential fraud, as does Caller ID spoofing.
5. The mitigation techniques described in this document can impact robocalling as much as Caller ID spoofing.

## Purpose

The paper educates policymakers and others about the challenges posed by Caller ID spoofing and related robocalling, provides an overview of existing mitigation techniques, and defines the clear need to allow industry to continue developing these techniques given the fast-changing and unknowable aspects of spoofing practices. The paper addresses what the industry is doing with regard to mitigation techniques to attempt to diminish the impact of illegitimate Caller ID spoofing, and may be subject to updates as ATIS learns more about the subject.

# Definitions & Abbreviations

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

For purposes of this white paper, the term "mitigation technique" will be used to describe any method(s), such as products, services, tools, applications, features, or technologies, used to lessen or reduce the frequency, magnitude, or severity of Caller ID spoofing.