**ATIS-0x0000x**

ATIS Standard on

**SMS Unwanted Message Mitigation Landscape**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

Abstract text here.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

The mandatory requirements are designated by the word *shall* and *must,* 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, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| December 7, 2022 |  | Outline | Ben Campbell |
| February 6, 2023 |  | Added more text to overview and architecture sections. | Ben Campbell and Harold Salters |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

This Technical Report describes the landscape of actions that service providers can take to mitigate lllegal, fraudulent, or otherwise unwanted SMS text messages. We describe example message deliver architectures, existing countermeasures, methods used by bad actors to send unwanted messages, existing countermeasures, and provide a gap analysis. This document is entirely description of the existing landscape; nothing herein should be interpreted as normative or otherwise prescriptive.

This document is limited to SMS messaging. It does not look at RCS messaging or over-the-top messaging services. As SMS texting has evolved to include, at least in the consumer’s perception, the routine use of Multimedia Messaging Service, we include MMS where applicable.

## Purpose

As the implementation of various regulatory measures and mitigation techniques have begun to reduce unwanted “robocalls”, more bad actors are moving to other modes of communication, such as SMS text messaging. IP-NNI has begun discussions about mitigation of unwanted text messages. This document is intended to document the current landscape of unwanted text delivery techniques and service provider countermeasures to serve as a basis for future discussion. While it describes perceived gaps It does not attempt to design new mitigation solutions.

[Note: This version of the report is not complete. We contribute it to enable early discussion of the problem statement and SMS delivery architecture description]

# Normative 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.

ATIS-0x0000x, *Technical Report*.[[1]](#footnote-1)

ATIS-0x0000x.201x, *American National Standard*.

# 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/> >.

## Definitions

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Overview

## The “Robotexting” problem

The term “Robotexting” refers to automated sending of fraudulent, illegal, or otherwise unwanted SMS messages. The FCC reported that robotext-related complaints have soared in the last few years. In October 2021, the FCC Chairwoman announced the agency would commence a rulemaking. On September 27, 2022, the FCC released a NPRM on this topic in CG Docket No. 21-402 (FCC 22-72), seeking comments on the potential mandatory blocking of illegal text messages and on the potential application of Caller ID authentication to text messages.

This report documents the current landscape for SMS delivery and currently available robotext countermeasures.

Editor’s note: Separate illegal automated messaging from legitimate automated messaging. Add discussion of non-automated fraudulent messaging.

## Recent Statistics

There is a paucity of network-level statistics on fraudulent, illegal, or otherwise unwanted SMS messages. To date, some 3rd party app providers have used incoming texts to the handsets of their subscribers to extrapolate statistics for the US market as a whole. The extrapolation criteria they use may not be clearly defined between handsets in the market and overall population figures, nor are time intervals clearly specified.

[Note: We hope to add more here as information becomes available]

## Objectives

The objective of this report is to educate the IP-NNI task force, industry participants, and policy makers about SMS delivery architectures and currently available mitigations to the robotext problem. It does not seek to design new countermeasures or establish new requirements.

# Example SMS Delivery Architectures

## Types of SMS delivery

### Application to Person (A2P)

Application to Person (A2P) messaging refers to automated messages sent from a business to a person. A2P messaging commonly involves a messaging application hosted by a Messaging Application provider or CPaaS provider, which forwards messages to an aggregator for delivery to consumers. Typically, A2P messages are application originated and mobile terminated.

### Person to Person (P2P)

Person to Person (P2P) messaging refers to messages sent from one human to another. Typically, P2P messages are Mobile Originated and Mobile Terminated.

### Mobile Termination

Mobile Termination refers to the delivery of a message from a Short Message Service Center (SMSC) to a mobile device, typically via the TSPs mobile network.

### Mobile Origination

Mobile Origination refers to message submission from a mobile device to an SMSC, typically via the OSPs mobile network.

Editor’s note: Mobile origination, mobile termination, and application origination are concepts to be considered for potential removal at a later point.

### Application Origination

Application Origination refers to the submission of messages by an application other than the native messaging application on an end-user device.

#### CPaaS Applications

Enterprise senders commonly use CPaaS applications to send large numbers of A2P messages.

Editor’s note: Generalize this concept to messaging service provider.

#### Email-to-SMS Gateways

Most wireless SPs offer Email-to SMS gateway services, where a sender can send an email to a gateway that converts and forwards it as an SMS towards a mobile recipient. Email-to-SMS is in common use by legacy applications. Many public service and community organizations use Email-to-SMS gateways to send messages to community members.

### Short Codes

Historically, most A2P messaging has used registered short codes in Sender ID fields. Short codes in the US are coordinated by the CTIA short code registry. Short code registrants must be vetted and must agree to follow published best practices.

### 10 Digit Long Codes (10DLC)

More recently, SPs have started to allow A2P messages to be sent with 10-digit “long codes” (effectively, TNs) in the Sender-ID fields. Unlike short codes, 10DLCs do not have a centralized entity to enforce best practices.

Editor’s note: Add call out to toll-free.

## Application to Person (A2P) Example Architecture



Figure A2P Example Architecture

Figure 1 shows an example delivery architecture for A2P messages. In this example, messages are Application Originated and Mobile Terminated.

An enterprise sender uses an automated messaging application hosted at an A2P Messaging Application or CPaaS provider. The application sends messages through an aggregator to an SMSC at the TSP. When the mobile recipient is available, the SMSC forwards the message to the mobile recipient’s end-user device.

## Person to Person (P2P) Example Architecture



Figure P2P Example Architecture

Figure 2 shows an example delivery architecture for P2P messages. In the example, messages are mobile originated and mobile terminated.

A mobile user sends an SMS to another mobile user. The message is submitted to the SMSC at the OSP. When the recipient is available, the SMSC sends the message towards the recipient, potentially via an SMS Hub, which forwards the message to the mobile recipient via an SMSF, MME, or IP-SM-GW depending on the network type.

[Open Question: Is the SMSC at the OSP or TSP for Mobile Origination?]

# Robotext Issues

## Common Unwanted Message Types

### Spoofed Sender Numbers (compare/contrast voice call spoofing with robotext spoofing)

### Non-Spoofed impersonation

### Link attacks

#### Malware

#### Unsolicited Advertising

### Phishing Attacks

## Message Insertion Techniques

### Gray Routes

#### International

#### P2P channel abuse

#### SIM boxes

### Disposable (a/k/a “burner”) TNs

#### Snowshoeing

### Email Gateways

### Insufficient Application Security

### Compromised Credentials

# Countermeasures

## Monitoring and Blocking

## Anti-Spoofing countermeasures

## Forensic analysis

## Sender authentication and TN verification

## Message Branding – Rich Sender Data

## Email gateway countermeasures

## Best Practices

## Others?

# Gap Analysis

# Conclusions

1. This document is available from ORGANIZATION at <website>. [↑](#footnote-ref-1)