**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 |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

This Technical Report describes the landscape service provider actions to mitigate lllegal, fraudulent, or otherwise unwanted SMS text messages. The report describes example message deliver architectures, existing countermeasures, methods used by bad actors to send unwanted messages, and 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.

## Purpose

As various regulation 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 contribution is an outline of potential topics for future discussion and inclusion.]

# 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

## Recent Statistics

## Objectives

# Example SMS Delivery Architectures

## Types of SMS delivery

### Application to Person (A2P)

### Person to Person (P2P)

### Mobile Termination

### Mobile Origination

### Application Origination

#### CPaaA Applications

#### Email-to-SMS Gateways

### Short Codes

### 10 Digit Long Codes (10DLC)

## Application to Person (A2P) Example Architecture

## Person to Person (P2P) Example Architecture

# Robotext Issues

## Common Unwanted Message Types

### Spoofed Sender Numbers

### Non-Spoofed impersonation

### Link attacks

#### Malware

#### Unsolicited Advertising

### Phishing Attacks

## Message Insertion Techniques

### Gray Routes

#### International

#### P2P channel abuse

#### SIM boxes

### Disposable TNs

#### Snowshoeing

### Email Gateways

### Insufficiently 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)