**ATIS-0x0000x**

ATIS Technical Report 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**].

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 |
| February 24, 2023 |  | Updated and made proposed edits to sections 1, 2, 4, 5, and 6. Added some spoofing-related information from NPRM responses. Re-style as a technical report and remove normative language boilerplate. | Sarah Delphey , Sean Hoelzle, Harold Salters, and Ben Campbell. |

**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 text messages. We describe example message delivery architectures, methods used by fraudulent message senders, existing countermeasures, and provide a gap analysis. This document is entirely descriptive of the existing landscape; nothing herein should be interpreted as normative or otherwise prescriptive.

This document’s discussion of text messaging refers to SMS (Short Message/Messaging Service) messaging as well as MMS (Multimedia Message/Messaging Service) messaging where applicable. It does not look at RCS messaging or over-the-top messaging services such as Apple’s iMessage or WhatsApp that do not rely on SMS or MMS.

## Purpose

As the implementation of various regulatory measures and mitigation techniques have begun to reduce illegal “robocalls”, fraudulent actors are increasingly using other modes of communication, such as text messaging. IP-NNI has begun discussions about the mitigation of illegal text messages. This document is intended to document the current landscape of illegal text message 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, the SMS delivery architecture, and various techniques used by bad actors.]

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. 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-2)

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 Illegal “Robotexting” Problem

The term “Robotexting” refers to the automated sending of messages. Like automated robocalls, the use of automated methods for sending text messages is not illegal and is very commonly used by legitimate businesses, organizations, and consumers (e.g. automatic text replies while driving). Robotexts are used for sending delivery notifications, two factor authentication codes, and appointment reminders. During the COVID-19 pandemic, text message alerts were used by several state health departments to notify individuals of positive COVID-19 tests.[[2]](#footnote-3)

Illegal robotexting refers to the use of automated sending to transmit text messages that are fraudulent or otherwise illegal. Text messages sent via manual means may also be illegal and are encompassed in the overall discussion of illegal text messages captured in this document. The FCC reported that illegal text-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 text message delivery and currently available countermeasures against illegal texting.

[Note: update/add to this section depending on the adoption of the latest texting order/NPRM in the FCC open meeting on March 16th.]

## Recent Statistics

There is a paucity of network-level statistics on fraudulent or otherwise illegal text 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 text message delivery architectures and currently available mitigations to the illegal texting 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 commonly refers to messages initiated by a business or organizational entity. A2P messaging commonly involves the business or organization obtaining services from a messaging service provider, which transmits messages to a downstream messaging service provider for termination. There are often one or more additional messaging service providers involved in the delivery of the message. The majority of A2P messages are mobile terminated, although there is a significant amount of A2P traffic that does not involve mobile users.[[3]](#footnote-4) The reference to an “application” is misleading as A2P text messages may be sent through automated or manual means, and both A2P and P2P message senders typically utilize a texting application. A2P message senders are subject to registration requirements that do not apply to P2P message senders.

### Person to Person (P2P)

Person to Person (P2P) messaging commonly refers to messages that are not initiated by a business or organizational entity.[[4]](#footnote-5). P2P messages may be initiated through manual or automated means (as in the example of automated text responses) but are most often sent manually.[[5]](#footnote-6)

### Segmentation of A2P and P2P traffic

SPs may segment A2P and P2P message traffic. Some have separate, independent delivery platforms for A2P and P2P traffic. Others use the same platform for both but may label individual messages by type.

This segmentation effectively creates A2P and P2P “channels”, where SPs can apply different delivery policies to each channel.

### 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.

SD Note: I would support generalizing to definitions of origination and termination irrespective of mobile vs. non-mobile user status.

### Application Origination

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

#### Messaging Service Provider

An entity that enables consumers, organizations, or other businesses to send or receive text messages. The messaging service provider might not be (and frequently is not) the provider of the phone number(s) used to send or receive messages or the provider of related inbound or outbound voice services.

#### Email-to-SMS Gateways

Most wireless service providers 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, businesses and consumers sent messages using ten-digit phone numbers without a distinction between A2P and P2P traffic. Registered short codes were the first channel created for the exclusive use of high volume A2P messaging traffic. Short codes in the US are coordinated on an opt-in basis, requiring approval, agreement to follow published best practices, and enablement by each terminating messaging service provider before they can be used to terminate messages to that service provider’s users. Additional organizations facilitate short code resources such as iconectiv and the CTIA short code registry.

### 10 Digit Long Codes (10DLC)

Historically, businesses and consumers sent messages using ten-digit phone numbers without a distinction between A2P and P2P traffic. More recently, documents such as the CTIA Messaging Best Practices and contractual updates proliferated upstream from mobile carrier interconnection agreements have attempted to define, identify, and separate traffic sent from 10-digit “long codes” (10DLC). 10DLCs are effectively local phone numbers) in the Sender-ID fields as either A2P or P2P. Traffic that originates from any messaging service provider other than a major mobile carrier that shows a local phone number in the sender ID field is automatically considered to be A2P, and therefore as coming from a business or organization, unless the message sender is able to submit an application through its originating service provider and obtain specific approval from major wireless carriers to be given an exemption to be treated as P2P and therefore not subject to registration requirements and additional per-message fees.

### Toll Free Messaging

Toll free messaging was established based on the desire of businesses and organizations to text-enable their existing toll-free business numbers. Like short codes, toll-free phone numbers are exclusively used for A2P messaging.

## 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 Service Provider or. 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.

Some SPs use an SMS/MMS Intercarrier gateway for A2P 10DLC message traffic. This leads to an alternate path where the Aggregator sends messages via an SMS/MMS Intercarrier gateway (Similar to P2P message traffic).

## Person to Person (P2P) Example Architecture



Figure P2P Example Architecture

Figure 2 shows an example delivery architecture for P2P messages.

In this example, 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/MMS Intercarrier Gateway, 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 Number

The term “spoofing” is commonly used to describe electronic communication sent with a false identity, or more generally, impersonation attacks. When referring to text messaging, the term “spoofing” is usually used to describe messages sent with a fake Sender Number. This report uses that meaning, and further distinguishes spoofing from other types of impersonation attack that do not use a fake Sender Numbers.

While spoofing is common with voice calls, it is uncommon with text messaging. There are several reasons for this:

* Access to the intercarrier SMS/MMS Gateway for P2P Messaging is limited to trusted partners, and those trusted partners can only originate messages from numbers they are authorized to use. There are already protections in place at the intercarrier gateway to ensure that an message service provider (for example) can’t submit a message from a number belonging to another messaging service provider.
* While messaging ownership of a mobile number can be overridden using the OSR (Override Services Registry), access to such changes in the OSR is tightly controlled and must be performed or authorized by the carrier owner.
* In SMS/MMS technology the sending number during mobile origination is inserted by the network, and not the sending device. Therefore, the source of a mobile originated message cannot be easily manipulated.[[6]](#footnote-7) For non-mobile messages, sending numbers are verified by the originating provider or at a minimum, verified by the intercarrier gateway as being associated with the sending originating or intermediate service provider.
* As there is no “caller ID” lookup for incoming texts, spoofing is generally not an effective impersonation tactic, since the name of the impersonated entity (the holder of the number) would not appear on the consumer’s device.[[7]](#footnote-8)[[8]](#footnote-9)
* While spoofing is uncommon, fraudulent message senders often seek out service providers or secondary black market account sellers that provide access to messaging-enabled phone numbers with little or no required information or oversight.

Instances of text “spoofing” are more typically associated to unauthorized SIM swaps, whereby a bad actor takes control of a number temporarily.

[Open Question: Do protections against Sender Number Spoofing for SMS apply to MMS?]

### Non-Spoofed impersonation

Businesses often use 10-digit numbers to communicate with customers. This has become even more common place with the rise of 10DLC. As discussed in 6.1.1, spoofing is uncommon. Non-spoofed impersonation is when a legitimate phone number sends messages pretending in the message content to be someone else ( e.g, a bank, IRS, or doctor’s office), usually for the purpose of obtaining personal information.

Non-spoofed impersonation assumes that the recipient may not recognize that the sender number does not match the identifying information in the message content. This is a major factor in the success of impersonation attacks.

### Link attacks

A “Link Attack” is a malicious text message that attempts to trick the recipient into following a URL, often as part of a phishing attack to obtain the recipient’s account login or personal information. Link attacks often involve impersonation, but not always.

#### Malware

A Malware link attack includes a URL that links to a malicious web site. That site may attempt to install malware on the recipient’s device, or otherwise take harmful actions.

#### Unsolicited Advertising

An unsolicited advertising link attack involves sending marketing messages without the (where required) prior consent from the recipient. Messages typically include a URL that links to a web site with advertising content or a sales offer. The message content may not be relevant to the linked material, but rather serves to trick the recipient into viewing the advertisement Where the advertised product or service is potentially legitimate, message senders are often affiliate marketers seeking to drive traffic to a partner’s webpage using an affiliate link. The party offering the product or service (“seller”) compensates the message sender based on the number of page views or converted sales, and the seller may or may not be aware of or complicit in the message sender’s practices.

Unsolicited Advertising Link Attacks using unrelated message content that appears benign have become a common way for bad actors to attempt to circumvent filters or policies regarding unsoliticed advertising.

#### Phishing Attacks

A Phishing attack is an impersonation attack that attempts to trick the recipient into revealing authentication credentials or other sensitive personal information. Phishing attacks via SMS are sometimes called “Smishing” attacks.

Phishing commonly involves link attacks. But they may use other approaches to convince a recipient to reveal sensitive information. For example, they may ask the recipient to call a phone number, where an accomplice attempts to trick the victim into revealing information.

## Message Insertion Techniques

### Gray Routes

#### International

#### P2P channel abuse

#### SIM boxes

### Phone Number Cycling

Bad actors commonly exploit services that provide free or very inexpensive TNs without strong customer qualification practices as a platform to launch attacks. When the attacks are eventually traced to the TN, the attacker simply moves on to use a new TN. TNs used in this fashion are sometimes called “burner” TNs.

Fraudulent senders target messaging services that may not require the user to supply much in the way of personally identifiable information. This allows senders to maintain relative anonymity, making investigation and law enforcement efforts difficult. If a sender is shut down by their messaging service provider, they may be able to open new accounts and continue sending.

#### Snowshoeing

Snowshoeing is a technique where an message sender uses a large number of originating sender numbers to send similar messages in order to avoid volumetric detection or per number volume limits. The content of messages sent from each number may be changed very slightly, making it more difficult for content filters to identify and group campaigns.

### Email Gateways

Email-to-SMS gateways are by far the most publicly accessible means to reach a mobile customer. Most US carriers allow customers to be reached via email using a <MSISDN>@domain address. These messages are then converted to SMS or MMS by the carrier.

Email gateways make an attractive target for bad actors, since they typically allow anyone to send messages without authentication requirements. But that very accessibility has made email gateways essential for a number of community service applications, such as emergency announcements, school closure notifications, etc.

### Application Vulnerabilities

If a messaging application or messaging service provider has inadequate authentication and authorization provisions, , bad actors may be able to exploit software vulnerabilities to send illegal messages. If such messages are eventually detected, they will be traced back to the application or service provider, but it can be difficult to trace them back to the bad actor.

### Compromised Credentials

Even if a messaging application or messaging service provider has reasonably strong authentication and authorization procedures, a legitimate user of the service may fail to protect its credentials. If those credentials are discovered by a bad actor, that actor may be able to send illegal text messages until such time the compromise is discovered. Bad actors may be able to additionally impersonate the legitimate user.

# Countermeasures

## Monitoring and Blocking

## Anti-Spoofing countermeasures

[Note: Elaborate on the intercarrier gateway and OSR anti-spoofing measures as mentioned in 6.1.1]

## 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-2)
2. https://covid19.nj.gov/pages/app [↑](#footnote-ref-3)
3. Text messages are frequently sent within businesses (messages sent by a company to its field technicians regarding schedule changes, etc) or between businesses (a vendor provides text alerts to its business customer on critical account changes, a real estate agent messages with a mortgage broker regarding an upcoming sale, etc) and do not always involve a mobile device, additionally, there are many over-the-top text messaging applications used by consumers that are used on a variety of devices. [↑](#footnote-ref-4)
4. Many texting services typically marketed to consumers (including mobile services) are used for a mixture of business and personal use or for exclusive business use, so it is often difficult or even impossible for messaging service providers to clearly differentiate between A2P and P2P messaging users today. [↑](#footnote-ref-5)
5. In the marketplace, some businesses or organizations that initiate text messages manually (often based on a legal position regarding the need to obtain prior consent) will refer to their messages as P2P. This document acknowledges and does not attempt to resolve this debate over terminology, but for purposes of discussion will define all business or organizational messages as A2P and not P2P. [↑](#footnote-ref-6)
6. Historically some messaging service providers allowed their customers to originate text messages from arbitrary sender numbers. Most US market providers have stopped this practice. [Note: Is there a reference to this effect we can use?] [↑](#footnote-ref-7)
7. SMSC do not pass their numbers through Caller ID databases as voice calls do. For example, spoofing a voice call from a number assigned to the Small Business Administration can result in that Caller Name displaying on the handset of the called party. That same TN however, if used to send an SMS text to a mobile handset, will simply display the 10-digit number, it will not display "Small Business Administration" on the mobile handset of the text recipient. A text message from a spoofed number would show a specific Caller Name if the name associated with the TN were already in the contact list of the text recipient’s handset or is otherwise known to the mobile OS. . [↑](#footnote-ref-8)
8. At the time of this writing, several providers offer branded SMS services. These may be an exception to the assumption that SMS does not display caller name information. Depending on their design, such services could be vulnerable to SMS spoofing if such spoofing were possible. [↑](#footnote-ref-9)