**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**].

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 |
| 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. |
| May 2. 2023 |  | Changed scope to cover “Unwanted Messages”, not just illegal. Changed A2P to “Non-Consumer” and P2P to “Consumer”. Added new text in the countermeasures section and empty section 6 subsections. Edited some terminology to align with CTIA Best Practices document. Other editorial changes. | Ben Campbell |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Objectives

## Scope

This Technical Report (“Report”) describes example message delivery architectures, methods used by senders of Unwanted Messages, countermeasures available to messaging stakeholders, and provides 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 that do not rely on SMS or MMS.

The document does not attempt to address laws or regulations and should not be interpreted or construed as providing legal advice.

## Purpose

As the implementation of various mitigation techniques have been successful in helping protect consumers from illegal and unwanted “robocalls”, fraudulent actors are increasingly using other modes of communication, such as text messaging. IP-NNI has begun discussions about the text messaging ecosystem. This document documents the current landscape of the messaging ecosystem, architectures and technologies used to deliver messages, including Unwanted Messages, and countermeasures available to stakeholders to protect consumers from Unwanted Messages.

The Report is intended to educate the IP-NNI task force, messaging industry participants, and policymakers and serve as a basis for future discussion. While it describes perceived gaps, it does not propose new mitigation solutions. It is not intended to be used as direct comments to regulators on the above topics.

[Note: This version of the report is not complete. We contribute it to enable early discussion of the problem statement, the SMS delivery architecture, various techniques used by bad actors, and available countermeasures.]

# 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

## Automated vs Unwanted Messages

The term “Robotexting” is informally used to describe to the automated sending of messages. Like automated calls, 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). Automated messages are commonly used for a variety of legitimate purposes, including sending delivery notifications, two factor authentication codes, and appointment reminders. For example, 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)

This document does not attempt to address automated messages in general; rather it considers Unwanted Messages as described in section 4.1.1 The discussion is not limited to automated messages; text messages sent via manual means may also be Unwanted Messages and are encompassed by this report.

This report makes no attempt to distinguish illegal messages from other Unwanted Messages, since the legality of messages may vary by jurisdiction.

### Definition of Unwanted Messages

The CTIA Messaging Principles and Best Practices[[3]](#footnote-4) (“Best Practices” ) describes the term “Unwanted Messages” to refer to the following:

* Unsolicited bulk messaging (i.e. spam)
* “Phishing” messages intended to access private or confidential information through deception
* Messages that require opt-in without consent from the recipient
* Other forms of abusive, harmful, malicious, unlawful, or otherwise inappropriate messages

Section 5.3 of the Best Practices describes inappropriate message content in more detail.

### Unwanted Message Statistics

Measuring SMS and MMS spam is a complex undertaking given the variety of data points, sources, and evolving tactics used by bad actors. There is a paucity of network-level statistics on Unwanted 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. 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.

Consumer complaints to the Commission and FTC can be informative of the volume of Unwanted Messages. Complaints made in 2021 to the FCC about Unwanted Messages increased to 15,300 in 2021 from 5,700 in 2019.16 Further, complaints to the FTC about Unwanted Messages increased to 377,840 in 2021 from 107,673 in 2019.17 Given the volume of text messages (trillions per year), this data suggests that consumers submitted one complaint for every nearly 80 million text messages. The volume of complaints about text messages is still far lower than the volume of complaints about other platforms like robocalls. Indeed, the FCC has reported that the number of complaints about Unwanted Messages is only about one-third of the number of complaints about autodialed calls, and about one-quarter of complaints about spoofing violations in the voice context.18

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

## The Messaging Ecosystem

## Messaging Ecosystem Stakeholders

There are several major types of entities that play different, key roles in the messaging ecosystem. Certain players may play multiple roles.

* **Non-Consumers** are the businesses, organizations, and other entities that originate messages to send to consumers.
* **Message Service Providers (MSP)** are entities that enable Non-Consumers to send or receive text messages. The MSP 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. (The term MSP should not be confused with SP, which is commonly used more narrowly to refer to network operators.)
* **Registrars** record a non-consumer’s unique identifier, such as a 10-digit telephone number, verify associated information, evaluate the reputation of the message sender, including identity and messaging history, and confirm that senders have authority to use an identifier. In some cases, registrars also monitor non-consumer message senders to ensure that they adhere to industry best practices or contractual agreements.
* **Cloud-Based Providers** are MSPs thatenable Non-Consumers to send messages, among other communications services, through internet-based portals and applications over various channels to be delivered to consumers.
* **Aggregators** facilitate the flow of Non-Consumer messaging traffic from the cloud-based provider systems to each mobile wireless network.
* **Wireless Service Providers** validate that Non-Consumer messaging traffic is recorded by a registrar, monitor traffic to mitigate Unwanted Messages, and deliver messages to consumer mobile devices.

##  Growth of Text Messaging

Since its launch in 1992, text messaging has evolved into one of the most popular forms of communication for Americans, with trillions of wireless text messages sent each year in the U.S. In 2021, American consumers exchanged 2 trillion messages—that’s over 63,600 texts per second.[[4]](#footnote-5) Much of this increase was driven by the exchange of media, such as GIFs and videos over MMS.

American consumers, businesses, and many other entities are not only sending and receiving high volumes of text messages, but they are also actively engaging with them. SMS open rates are estimated to be as high as 98 percent and response rates as high as 45 percent.[[5]](#footnote-6) These engagement rates eclipse email open rates – just 21 percent.[[6]](#footnote-7) Further, consumers prefer texting over voice calling, nearly 2 to 1, and nearly half of all consumers text every single day (more than the use of any other communications medium, including voice or email).[[7]](#footnote-8)

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

# Example SMS and MMS Delivery Architectures

## Types of Message delivery

There are multiple ways that text messages can be exchanged through the messaging ecosystem.

Text messages can be exchanged among consumers’ mobile devices that are identified by 10-digit telephone numbers and routed through servers on mobile wireless networks using storage and retrieval functionality (“store and forward”). Non-Consumer messages can be originated by non-consumer message senders identified by a number of sources including 10-digit telephone numbers (“10DLC”), toll-free telephone numbers, or short codes, and delivered to a consumer’s mobile device that is identified by a 10DLC. Depending upon the identifier of the message senders (e.g., 10DLC, toll-free), each of these means of exchanging text messages is considered a distinct platform with differing purposes, use-cases, and applicable policies. Further detail is provided below.

### Non-Consumer to Consumer (“Non-Consumer”)

Non-Consumer messaging commonly refers to messages initiated by a business or organizational entity[[8]](#footnote-9). These message senders may also use agents, representatives, or other individuals acting on behalf of the business, organization, or other entity. Non-Consumer 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 Non-Consumer messages are mobile terminated, although there is a significant amount of Non-Consumer traffic that does not involve mobile users.[[9]](#footnote-10) Both Consumer and Non-Consumer text messages may be sent through automated or manual means and typically use a texting application. Non-Consumer message senders are typically subject to Service Provider registration requirements that do not apply to Consumer message senders.

### Consumer to Consumer (“Consumer”)

Consumer to Consumer messaging commonly refers to messages that are not initiated by a business or organizational entity.[[10]](#footnote-11)[[11]](#footnote-12). These messages may be initiated through manual or automated means (as in the example of automated text responses) but are most often sent manually.[[12]](#footnote-13)

### Segmentation of Non-Consumer and Consumer traffic

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

This segmentation effectively creates Non-Consumer and Consumer “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.

#### 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 Non-Consumer and Consumer traffic. Registered short codes were the first channel created for the exclusive use of Non-Consumer messaging traffic. Short codes in the US require approval and are administered under the Messaging Principles and Best Practices. Delivery of short-code messages is enabled 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 (www.usshortcodes.com).

### 10 Digit Long Codes (10DLC)

Historically, businesses and consumers sent messages using ten-digit phone numbers without a distinction between Non-Consumer and Consumer traffic. More recently, documents such as the CTIA Messaging Principles & Best Practices as well as interconnection agreement updates pushed by individual mobile SPs have attempted to define, identify, and separate traffic sent from 10-digit “long codes” (10DLC . Traffic that originates from any MSP other than a major mobile SP and includes a local 10DLC in the sender ID field is automatically treated as Non-Consumer traffic and subject to registration requirements and additional per-message fees. In some cases, a sender may be able to get an exemption approved by the local mobile SP, but such exemptions are rare.

### 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 Non-Consumer messaging.

## Non-Consumer Example Architecture



Figure 1 Non-Consumer Example Architecture

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

An enterprise sender uses an automated messaging application hosted at a Non-Consumer Messaging Service Provider to send 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 Non-Consumer 10DLC message traffic. This leads to an alternate path where the Aggregator sends messages via the SMS/MMS Intercarrier gateway (Similar to Consumer message traffic).

[Note: Do we need a diagram to illustrate scenarios where persons act as agents, representatives or act on behalf of a business, organization or entity to send non-consumer messages?]

## Consumer Example Architecture



Figure 2 Consumer Example Architecture

Figure 2 shows an example delivery architecture for Consumer 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.

Editor’s note: Think about interactive conversations between Consumers and Non-Consumers.

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

[Question: Do we need additional diagrams to describe MMS delivery?]

#  Unwanted Text Messages

## Unwanted Message Types

The following are examples of common types of Unwanted Messages. This is not an exhaustive list. Several of the Unwanted Message type descriptions overlap. Any specific message may have aspects of multiple types.

### Spoofed Sender ID

The term “spoofing” is commonly used to describe electronic communication sent with a false identity, or more generally, impersonation attacks. For example, spoofing in the messaging context occurs when a sender uses a false Sender ID (phone number) with the intent to deceive the recipient, often with the purpose of impersonating another caller. In the text messaging context, spoofing a Sender ID is far less common that for voice calls. This Report uses the term “spoofing” to refer to falsified Sender IDs and distinguishes spoofing from other types of impersonation attack that do not use a fake Sender IDs.

Sender ID spoofing is uncommon in text messaging for several reasons:

* One reason for this is that 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.[[13]](#footnote-14) 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. See Section 7.2 for more detail on such countermeasures.
* 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.[[14]](#footnote-15)[[15]](#footnote-16)

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

There are also legitimate cases where a third party is given the authority to send messages on behalf of another, using their Sender ID. For example, a TN owner may authorize third parties to send texts on their behalf. It is important that anti-spoofing countermeasures do not also prevent authorized use.

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

### Non-Spoofed impersonation

As discussed in 6.1.1, Sender ID spoofing in texting 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 ID does not match the identifying information in the message content.

### 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 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 unsolicited advertising.

#### Phishing Attacks

A Phishing attack is an impersonation attack that uses links or other means to attempt to trick the recipient into revealing authentication credentials or other 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. Phishing attacks via SMS are sometimes called “Smishing” attacks.

## Message Insertion Techniques

### Gray Routes

Messaging Gray Routes are routes that bypass operator policies. The “gray” comes from the routes that may be legal at the origination side but illegal or otherwise non-complaint with destination side policies. Gray routes are often used to bypass tolls but may also be used to circumvent message delivery policies, for example by allowing messages to be originated by an MSP with lax authentication or “Know Your Customer” practices. Gray routes can take several forms.

#### Consumer channel abuse

Non-Consumer senders may disguise messages as consumer messages to avoid fees and to circumvent registration and vetting processes established for Non-Consumer message delivery. This is typically done by sending messages via a method normally intended for Consumer messages. They sometimes send messages via international paths.

Toll-bypass fraudsters may send messages via aggregators local to the destination to bypass international message tolls.

#### SIM boxes

SIM boxes are IP gateway devices that can be used to impersonate a potentially large number of mobile handsets, often by physically housing a large number of SIMs. SIM boxes may enable Non-Consumer traffic on Consumer channels. SIM boxes may also be used to enable TN cycling techniques.

###  Disposable TNs and Snowshoeing

Bad actors exploit “disposable” TNs, which are free or very inexpensive telephone numbers generally obtained through web-based services or pre-paid SIM card purchases. Disposable TNs are typically temporary purpose When the Unwanted Messages are eventually traced to a disposable TN, the attacker moves on to use a new TN. TNs used in this fashion are sometimes called “burner” TNs.

Fraudulent senders target MSPs that may not require the user to supply much personally identifiable information in order to obtain a disposable TN. 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 is a technique where a message sender spreads similar messages across many different TNs in order to avoid volumetric detection or per number volume limits. Snowshoe messaging is closely tied to the use of disposable or temporary telephone numbers. 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. The accessibility of email to text gateways have led to this messaging pathway being used for several legitimate use cases, including community service applications, such as emergency announcements, school closure notifications, etc. However, email gateways that do not authenticate in-bound email may become targets for bad actors, who may be able to bypass the message authentication requirements of other messaging pathways.

Email authentication technologies protect Consumers by allowing Service Providers and other stakeholders to perform forensic analysis and, thus, more easily identify the actual sending domain, identify the bad actor, and take appropriate action. Accordingly, Message Senders should ensure that all messages utilize common or standardized email authentication technology (e.g., DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF)).[[16]](#footnote-17)

###  Compromised API Credentials or Systems

Third-Party Messaging Applications with inadequate authentication and authorization provisions for Message Senders may be susceptible to software vulnerabilities that could be exploited to send Unwanted Messages. Inadequate authentication provisions may also make it difficult to identify the message sender for forensic purposes. [[17]](#footnote-18)

Even if a messaging application or messaging service provider has reasonably strong authentication and authorization procedures, a legitimate user (e.g., CPaaS providers, Message Senders, and other users 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 Unwanted Messages until such time the compromise is discovered. Bad actors may be able to additionally impersonate the legitimate user.

### Other

[Note: Do we need to consider things like SMSC/GT scanning?]

# Countermeasures

## Registration and Vetting

Registration and vetting frameworks make it easier to identify legitimate messages and to label of block Unwanted Messages by collecting and maintaining accurate information about message senders. With accurate information, stakeholders can prevent Unwanted Messages from being delivered to consumers and can share information with each other and with law enforcement agencies to stop bad actors from further sending such messages. Registrars record a non-consumer’s unique identifier, such as a 10-digit telephone number, verify associated information, evaluate the reputation of the message sender, including a message sender’s identity and messaging history, and confirm that senders have authority to use an identifier. In some cases, registrars also monitor non-consumer message senders’ adherence to industry best practices or contractual agreements.

Example registry frameworks include the CTIA Short Code registry ([www.usshortcodes.com](http://www.usshortcodes.com)) and The Campaign Registry (https://www.campaignregistry.com)

## Monitoring and Blocking

Messaging stakeholders use a number of tools and approaches to actively manage their networks.

SMSCs can integrate “SMS Firewall” services to provide monitoring, analytics, and filtering services on inbound message traffic. Inter-carrier gateways can provide similar services on traffic between SPs. Both can operate based on route, content, and volumetric patterns:

Message **Filters** –Wireless providers and their partners throughout the messaging ecosystem actively monitor daily text messaging traffic for factors like high throughput and volume, using techniques like artificial intelligence and machine learning to detect and mitigate suspected spam or other Unwanted Messages in real-time.

* Route filtering – Messages are blocked if they arrive via an unexpected route for the TN. This can help differentiate Non-Consumer and Consumer traffic as well as mitigate certain gray route issues.
* Content filtering – Messages are blocked if they contain inappropriate content (e.g. SHAFT content). Content filtering may help mitigate link attacks by blocking messages from unknown sources that contain URLs.
* Volumetric filtering -- Messages are blocked if they show a pattern of usage that is not appropriate for the message type. For example, Consumer sources sending high volumes of traffic may be engaged in Non-Consumer messaging. Volumetric techniques may also detect changes in behavior, such as might occur if a legitimate sender or MSP becomes compromised.

**Targeted Blocking** – Providers employ targeted blocking of messages in a balanced approach aimed at protecting consumers from Unwanted Messages while also protecting legitimate messages. Providers may block texts if high-volume messages come from a sender that has not registered or is not using appropriate Non-Consumer messaging channels, or if providers have evidence that a message is Unwanted. CTIA’s *Messaging Security Best Practices* note that a risk assessment of Unwanted Messages may include, but is not limited to, network monitoring and evidence of fraud or other malfeasance, including fraud or malfeasance associated with compromised API credentials, utilization of gray routes, lack of authentication, or a pattern of abuse of industry best practices. Additionally, wireless providers use “account fingerprinting” techniques to identify accounts that are sending high volumes of messaging traffic with little or no voice or data usage. High volumes of messaging traffic often indicate the use of computer programs, such as “bots” or other automated system that are distributing Unwanted Messages.

**Account Suspension -** Beyond registries, providers may have information about potential sources of Unwanted Messaging that can prevent them from being delivered to consumers. For example, providers may be able to identify the unique identifiers (e.g., telephone numbers), SIM cards, websites, and other information associated with spam campaigns and take action to suspend or shut down accounts and prevent bad actors from sending spam.

## Anti-Spoofing Techniques

There are a number of available countermeasures to mitigate or reduce Sender ID Spoofing:

* Messaging Service Providers only allow message senders to choose TNs that they are authorized to use.
* Access to the intercarrier SMS/MMS Gateway for Consumer Messaging is limited to trusted partners. There are protections in place at the intercarrier gateway to ensure that a message service provider (for example) can’t submit a message from a number belonging to another messaging service provider[[18]](#footnote-19).
* For Consumer messages, Messaging Firewalls can query the sending number’s HLR/HSS to determine that the subscriber is actually registered.

## Sender authentication and TN verification

SMS and MMS use a hop-by-hop model to authenticate sender identity and to verify that senders have the requisite authority to use TNs. This approach requires transitive trust among MSPs, aggregators/gateways, and SPs.

Text messages, especially Non-Consumer messages, may cross several entitles between senders and recipients. The final message recipients trust that their TSPs only accept messages from trusted sources. TSPs trust that aggregators and intercarrier gateways only accept messages from authenticated MSPs or OSPs. MSPs and OSPs authenticate senders and require them to comply with applicable laws and regulations. Individual MSPs and OSPs may also contractually require message senders to comply with industry Best Practices, as well as individual SP policies. These trust relationships are established and enforced through interconnection agreements and policies.

Currently available end-to-end attestation frameworks such as STIR/SHAKEN[ref] are designed to work primarily with SIP-based voice services that can imbed signed PASSporTs in the request headers. The IETF STIR working group is working on a draft to apply STIR to SIP-based messaging. While this may apply to SIP-based messaging modes such as RCS [ref], it does not directly address SMS or MMS because the underlying technologies cannot imbed signed PASSporTs. It does allow for the application of STIR to non-SIP messaging using out-of-band techniques, but there is no current IETF or ATIS effort to standardize this.

## Consumer Reporting Tools

"“7726” reporting gives subscribers an easy way to report Unwanted Messages. Customers can forward Unwanted Messages to 7726 or “SPAM” to report them to their wireless provider. Providers use information reported by customers through 7726 to further calibrate spam filters and other sophisticated tools to protect consumers from spam messages.[[19]](#footnote-20)

Certain end-user device platforms, such as iOS and Android, offer additional end-user reporting options with more metadata. Closed-loop monitoring services can monitor sender compliance with laws and best practices. These techniques often involve “honeypot” recipients to capture traffic samples and perform analytics. The effectiveness of closed-loop monitoring is dependent on forensic analysis capabilities to identify bad actors.

## Forensic Analysis Cooperation

Messaging stakeholders often need to cooperate in forensic analysis to determine the source of Unwanted Messages. The CTIA Messaging Security Best Practices describe several best practices for forensic analysis cooperation[[20]](#footnote-21):

* Stakeholders should only request information that is reasonably necessary to identify senders of Unwanted Messages.
* Stakeholders should respond to legitimate requests in a timely manner. Responses should be sufficiently substantive to enable the requestor to continue an investigation to eliminate the sending of Unwanted Messages.
* Stakeholders should notify cooperating parties of steps taken to mitigate the sending of Unwanted Messages and steps to mitigate future threats.
* Stakeholders should take reasonable steps to “know their customer” by obtaining sufficient information to authenticate a Message Sender’s identity prior to sending a message.

MSPs can help stakeholders prevent and mitigate Unwanted Messages by including information such as the following:

* The message origination point (e.g., IP address, telephone number, or other information associated with the message sender)
* Message destination (e.g., IP address, telephone number, or other information associated with the recipient)
* The date and time of the message
* Session Initiation Protocol (SIP) header anomalies;
* Evidence that the message was an Unwanted Message (e.g., evidence that the message was abusive, harmful, malicious, unlawful, or otherwise inappropriate)
* The volume of messages

By maintaining accurate information about message senders and sharing actionable information about bad actors, messaging ecosystem stakeholders can apply a variety of anti-spam solutions to minimize Unwanted Messages.

## Message Branding – Rich Sender Data

Several service providers offer “Branded Messaging” services, where senders can register to have additional branding displayed with their messages. For example, message recipients may see the sender’s logo as part of a message. Branded messaging can be helpful in countering non-spoofed impersonation attacks because they give recipients ways to distinguish trustworthy messages from non-trustworthy messages. Branded messaging is not a complete solution to impersonation attacks, but it can be part of a broader solution. Any Branded Messaging service needs to take measures to insure message branding is not improperly applied incorrectly.

## Email gateway

As mentioned in 5.1.6.2, email-to-text gateways are currently a significant source of Unwanted Messages. There are several approaches that SPs can take to reduce Unwanted Messages sent through email gateways. The following is a list of several techniques in order of increasing intrusiveness:

* Use standardized email authentication techniques, including Sendor Policy Frameworks (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DKIM), and Authenticated Received Chain (ARC). This approach better enables message filtering and forensic analysis to determine the sources of Unwanted Messages.
* Block email domains that show a pattern of improper message origination.
* Only accept email from domains that meet certain minimum standards. For example, reject email from MTAs that do not publish SPF records or that do not publish a DMARC policy of at least “quarantine” or “reject”.
* Only accept email from domains and intermediate Message Transfer Agents (MTAs) that commit to certain best practices, for example, “Know Your Customer” practices. (See section 7.7)
* Only accept email from domains with which the SP has a contractual relationship or directly controls.
* Decomission email gateways entirely. This would be the simplest and most complete solution. But it is not typically feasible in short run. Email gateways are commonly used for legitimate purposes by senders that cannot easily adapt to other methods, for example, community or safety announcements from local governments, schools, and public safety organizations. However, SPs could encourage such entities to plan to move to using Messaging Service Providers in the long run, with a goal of eventually decommissioning email gateways.

## Best Practices

The Messaging and Malware Anti-Abuse Work Group (MAAWG) [Ref] and CTIA-The Wireless Association (“CTIA”) have published relevant best practices documents.

CTIA’s *Messaging Principles and Best Practices* identify the following core principles to protect consumers from Unwanted Messages:

* “All Service Providers should use reasonable efforts to prevent Unwanted Messages from being sent by or to Consumers;
* All Service Providers may filter or block Unwanted Messages before they reach Consumers;
* To the extent practical and consistent with Service Providers’ Unwanted Message prevention and mitigation methods, Service Providers may notify the Message Sender sending Unwanted Messages when Service Providers block Unwanted Messages;
* Service Providers should adopt Unwanted Messaging traffic practices that protect Consumers in a manner that facilitates the exchange of wanted wireless messaging traffic; and
* Where appropriate, wireless ecosystem members should collaborate to maintain Consumer trust and confidence in wireless messaging services.”

A Message Sender’s failure to abide by such principles may increase the risk that a Message Sender’s messages are blocked. The *Messaging Principles and Best Practices* have helped the wireless industry consistently mitigate spam over text messaging and bolster trust. However, they are voluntary, and bad actors have sometimes been successful in evading industry best practices*.*

CTIA’s *Messaging Security Best Practices* identify a number of activities that could threaten messaging security, as well as the steps that stakeholders should take to protect against and address those threats. They include general messaging security best practices:

* Monitoring and blocking
* Forensic analysis cooperation
* Consumer education

In addition, they include best practices to address certain messaging security threats:

* Email origination, as noted above
* Disposable telephone numbers and text-enabled telephone numbers
* CPaaS providers and compromised API credentials or systems

[Note: Verify that the MAAWG best practices are relevant to SMS/MMS]

## Others?

# Gap Analysis

# Conclusions

1. This document is available from ORGANIZATION at <website>. [↑](#footnote-ref-2)
2. [↑](#footnote-ref-3)
3. https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-interoperability-sms-mms [↑](#footnote-ref-4)
4. https://www.ctia.org/news/2022-annual-survey-highlights [↑](#footnote-ref-5)
5. https://www.ctia.org/news/2022-annual-survey-highlights [↑](#footnote-ref-6)
6. https://www.ctia.org/news/2022-annual-survey-highlights [↑](#footnote-ref-7)
7. Morning Consult Survey: Nationwide poll of 1,999 registered voters, conducted December 3-5, 2021. [↑](#footnote-ref-8)
8. Non-Consumer messaging has been historically referred to as Application to Person (A2P) messaging. The industry is moving away from that term because it did not fully describe organizational messaging. [↑](#footnote-ref-9)
9. 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-10)
10. Consumer messaging has been historically referred to as Person to Person (P2P) messaging. The industry is moving away from that term because it caused confusion about messages sent by a person on behalf of an organization. [↑](#footnote-ref-11)
11. 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 Non-Consumer and Consumer messaging users today. [↑](#footnote-ref-12)
12. 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 Consumer. 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 Non-Consumer and not Consumer. [↑](#footnote-ref-13)
13. 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-14)
14. 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-15)
15. 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-16)
16. <https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf> (section 4.1) [↑](#footnote-ref-17)
17. <https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf> (section 6). [↑](#footnote-ref-18)
18. 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. [↑](#footnote-ref-19)
19. https://www.ctia.org/protecting-yourself-from-spam-text-messages [↑](#footnote-ref-20)
20. <https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf> (section 3.2) [↑](#footnote-ref-21)