ATIS-1000101

SMS Unwanted Message Mitigation Landscape

JOINT STANDARD

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 the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

ATIS-1000101, SMS Unwanted Message Mitigation Landscape

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000101

ATIS Technical Report on

SMS Unwanted Message Mitigation Landscape

Alliance for Telecommunications Industry Solutions

Approved September 16, 2024

Abstract

This Technical Report describes the current landscape of the text messaging ecosystem, architectures, and technologies used to deliver messages and describes countermeasures currently available to stakeholders to protect consumers from unwanted messages. The document primarily considers the Short Message/Messaging Service (SMS). A gap analysis is provided so as to identify potential areas where additional standards work to enhance existing mitigations may be needed. The document does not propose new mitigation solutions, but rather recommends the formation of a task force to evaluate methods for verified identity transmission and validation in text messaging.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) is a global standards development and technical planning organization that develops and promotes worldwide technical and operations standards for information, entertainment, and communications technologies. ATIS' diverse membership includes key stakeholders from the Information and Communications Technologies (ICT) industry – wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, VoIP providers, consumer electronics companies, public safety agencies, and internet service providers. ATIS is also a founding partner and the North American Organizational Partner of the Third Generation Partnership Project (3GPP), the global collaborative effort that has developed the Long-Term Evolution (LTE) and LTE-Advanced wireless specifications.

ATIS' Packet Technologies and Systems Committee (PTSC) develops standards related to services, architectures, signaling, network interfaces, next generation carrier interconnect, cybersecurity, lawful intercept, and government emergency telecommunications service within next generation networks. As networks transition to all-IP, PTSC will evaluate the impact of this transition and develop solutions and recommendations where necessary to facilitate and reflect this evolution.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

> NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [https://www.atis.org/policy/patent-assurances/] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

The mandatory requirements are designated by the word *shall* 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.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

ATIS Standard on –

SMS Unwanted Message Mitigation Landscape

1 Scope, Purpose, & Objectives

1.1 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). It does not look at over-the-top messaging services that do not rely on SMS. It does not discuss MMS in detail, since doing so would not materially change the conclusions.

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

1.2 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. The ATIS/SIP Forum IP-NNI Task Force (IP-NNI) has begun discussions about the text messaging ecosystem. This document summarizes 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.

2 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 Report are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] CTIA, *Messaging Principles and Best Practices*.[1]

[Ref 2] CTIA, *2023 Annual Survey Highlights*.[2]

[Ref 3] CTIA, *2022 Annual Survey Highlights*.[3]

[Ref 4] Morning Consult Survey: Nationwide poll of 1,999 registered voters, conducted December 3-5, 2021.

[1] This document is available from the CTIA at <https://api.ctia.org/wp-content/uploads/2019/07/190719-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf>.

[2] This document is available from the CTIA at <https://www.ctia.org/news/2023-annual-survey-highlights>

[3] This document is available at the CTIA at <https://www.ctia.org/news/2022-annual-survey-highlights>

[Ref 5] CTIA, *Messaging Security Best Practices.*[4]

[Ref 6] CTIA Consumer Resources: *Protect Yourself from Spam Text Messages*.[5]

[Ref 7] M[3]AAWG, *M[3]AAWG Mobile Messaging Best Practices for Service Providers*.[6]

[Ref 8] ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)*.[7]

[Ref 9] IETF RFC 9475, *Messaging Use Cases and Extensions for STIR*.[8]

[Ref 10] FCC Consumer Advisory Committee, *Report on the State of Text Messaging, August 30, 2022*.[9]

3 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/ >.

3.1 Definitions

Aggregator: Entity that facilitates the flow of Non-Consumer messaging traffic from the MSP to each WSP.

Consumer: A subscriber to the Short Message Service.

Identity: Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes.

Message Service Provider: Entity that enables Non-Consumers to send or receive text messages.

Non-Consumer: Organizational or business sender of a message to a Consumer.

Registrar: Entity that records a Non-Consumer's identity and associated information.

Sender ID: The originating or sending party number used to identify the sender of an SMS, carried in the Sender ID field of an SMS Protocol Data Unit.

Short Code: A 5- or 6-digit code used as the Sender ID for Non-Consumer messages, assigned by the Short Code Registry.

Ten-Digit Long Code: A ten-digit Telephone Number (TN) used as the Sender ID for Non-Consumer messages.

Toll-Free: A Toll-Free TN used as the Sender ID for Non-Consumer messages.

Wireless Service Provider: Entity that delivers text messages to mobile subscribers.

3.2 Acronyms & Abbreviations

A2P	Application to Person
ATIS	Alliance for Telecommunications Industry Solutions
DKIM	DomainKeys Identified Mail

[4] This document is available at the CTIA at <https://api.ctia.org/wp-content/uploads/2022/06/Messaging-Security-Best-Practices-June-2022.pdf>.

[5] This document is available at the CTIA at <https://www.ctia.org/protecting-yourself-from-spam-text-messages>.

[6] This document is available from the Messaging, Malware, and Mobile Anti-Abuse Working Group (M[3]AAWG) at <https://www.m3aawg.org/sites/default/files/m3aawg-mobile-messaging-best-practices-service-providers-2015-08_0.pdf>.

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at <https://www.atis.org/ >.

[8] This document is available from the Internet Engineering Task Force (IETF) at <https://datatracker.ietf.org>.

[9] This document is available from the FCC Consumer Advisory Committee at < https://www.fcc.gov/ecfs/document/1083135018370/1 >.

DMARC	Domain-based Message Authentication, Reporting & Conformance
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GSMA	Global System for Mobile Communications Association
IP-SM-GW	Internet Protocol Short Message Gateway
M3AAWG	Messaging and Malware Anti-Abuse Work Group
MAP	SS7 Mobile Application Part
MM1	The 3GPP interface between MMS User Agent and MMS Center
MM4	The 3GPP interface between different MMSCs
MME	Mobility Management Entity
MMS	Multimedia Message Service
MMSC	Multimedia Messaging Service Center
MSP	Messaging Service Provider
MTA	Message Transfer Agent
nnSR	netnumber Services Registry
OSP	Originating Service Provider
P2P	Person to Person
PGW	Packet Data Network Gateway
RCC	Rich Communications Client
RCS	Rich Communications Services
SMS	Short Message/Messaging Service
SMSC	SMS Service Center
SMSF	Short Message Service Function
SP	Service Provider
SPF	Sender Policy Frameworks
10DLC	Ten-Digit Long Code
TN	Telephone Number
TSP	Terminating Service Provider
UPF	User Plane Function
WSP	Wireless Service Provider

4 Overview

4.1 Automated vs Unwanted Messages

The term “robotexting” is informally used to describe 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.

This document does not attempt to address automated messages in general; rather it considers Unwanted Messages as described in Clause 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.

4.1.1 Definition of Unwanted Messages

The CTIA *Messaging Principles and Best Practices* ("Best Practices") [Ref 1] describes the term "Unwanted Messages" as follows:

- 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 [Ref 1] describes inappropriate message content in more detail.

4.1.2 Unwanted Message Statistics

Measuring Unwanted Messages 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 third-party application providers have used incoming texts to the handsets of their subscribers to extrapolate statistics for the U.S. 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 [FCC Consumer Advisory Committee, *Report on the State of Text Messaging, August 30, 2022*]. Further, complaints to the FTC about Unwanted Messages increased to 377,840 in 2021 from 107,673 in 2019 [Ref 10]. 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 [Ref 10].

4.2 Messaging Ecosystems

This section provides a high-level description of messaging ecosystems. Note some of the described ecosystems support end-to-end encryption. It is unclear how encryption support obviates, improves, or inhibits message authentication, traceback, etc.

4.2.1 Device-based messaging ecosystems

The major mobile operating systems have OS-specific messaging architectures and functions and interoperate with traditional SMS, MMS, or other OS-based messaging ecosystems using messaging gateway systems.

4.2.2 Over-the-Top messaging ecosystems

There are dozens of Internet-based mostly-closed group messaging ecosystems. Examples include weblog (aka "blog") message boards and private messaging within various social networks, as well as more well-known messaging and instant messaging applications. Some of these systems do have gateway functionality to promote interoperability with other popular messaging ecosystem applications, but not all.

4.2.3 Traditional SMS and MMS messaging ecosystems

This Technical Report provides a detailed description of the traditional SMS and MMS messaging ecosystems.

4.2.4 Rich Communications Services (RCS)

Rich Communications Services (RCS) is a set of voice and messaging services defined by the Global System for Mobile Communications Association (GSMA) in a series of Rich Communications Client (RCC) specifications

comprising the Rich Communications Suite. RCS specifications define a wide variety of possible messaging capabilities. A non-exhaustive list of the capabilities are:

- Voice and Video Calls (with enhanced imagery, reason for calling, priority, and location information)
- Standalone Messaging
- 1-to-1 Chat
- Group Chat
- File Transfer
- Geolocation Push Services
- Audio Messaging
- Content sharing
- Chatbots and chatbot functions

These services can be complex to implement and inter-working all available features between RCS-capable service providers continues to be an on-going challenge, particularly because some of the GSMA service specifications are not overly prescriptive and permit more than one way of accomplishing a given service function and potentially using non-interoperable protocol approaches.

RCS can be implemented by a single carrier and with other carriers in a peer-to-peer arrangement.

Many of the RCS services are signaled via SIP signaling protocol, therefore further study is required to determine if it is possible to leverage IETF RFC 9475, *Messaging Use Cases and Extensions for Secure Telephone Identity Revisited (STIR)*, to provide STIR/SHAKEN-like messaging authentication.

4.3 SMS and MMS Messaging Ecosystem

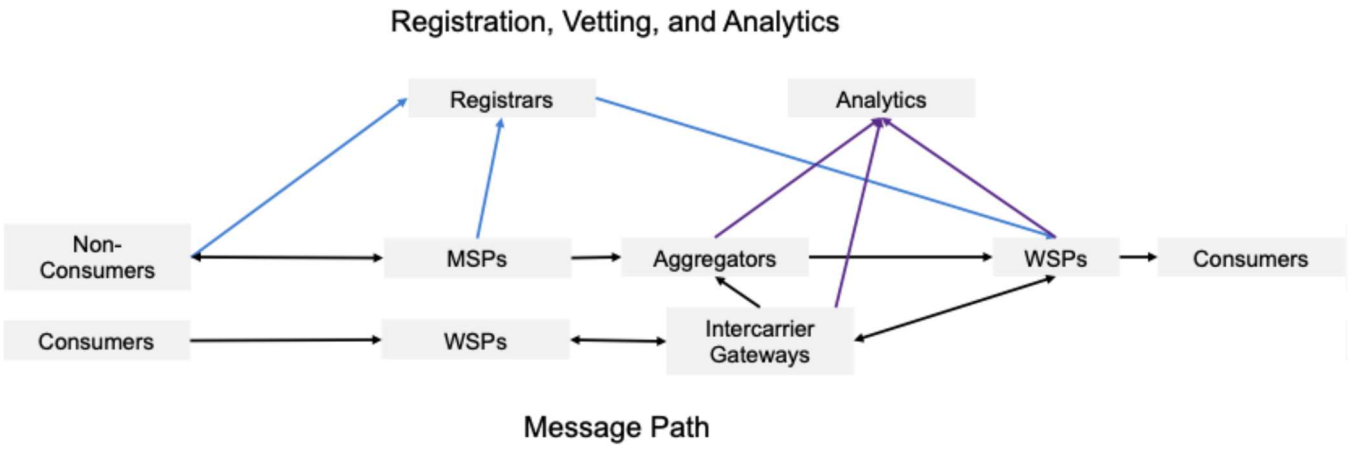

Figure 4-1: Messaging Ecosystem Stakeholders

There are several major types of entities that play different, key roles in the messaging ecosystem. Certain players may perform multiple roles. Figure 4-1 illustrates the ecosystem stakeholders and their relationships.

- **Non-Consumers** are the businesses, organizations, and other entities that originate messages to send to Consumers.
- **Consumers** are wireless subscribers that receive and send messages via their WSPs.
- **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 TNs 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 information. Registrars may perform the roles of "Campaign Registrar", "Sender ID Registrar", or a combination of both.
    - **Campaign Registrars** record a Non-Consumer's information, for example, company details and messaging use case, and evaluate the reputation of the message sender, including identity and messaging history. In some cases, Campaign Registrars also monitor Non-Consumer message senders to ensure that they adhere to industry best practices or contractual agreements.
    - **Sender ID Registrars** record a Non-Consumer's unique identifier, such as a short code, toll-free number, or 10DLC and confirm that senders have the authority to use an identifier.
- **Aggregators** facilitate the flow of Non-Consumer messaging traffic from the MSP to each WSP.
- **Analytics** providers categorize and label messages and, in some cases, enforce message delivery policies.
- **Wireless Service Providers (WSP)** validate that the Sender IDs of Non-Consumer messages are recorded by a registrar, monitor traffic to mitigate Unwanted Messages, and deliver messages to Consumer devices.
- **Intercarrier Gateways** facilitate the exchange of messages among WSPs**.**

4.4 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 2.1 trillion messages – that is over 66,000 texts per second,[10] according to the CTIA *2023 Annual Survey Highlights* [Ref 2]. 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 not only send and receive high volumes of text messages, but they also actively engage with them. SMS open rates are estimated to be as high as 98 percent and response rates as high as 45 percent, according to the CTIA *2022 Annual Survey Highlights* [Ref 3]. These engagement rates eclipse email open rates – just 21 percent [Ref 3]. 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) [Ref 4].

5 Example SMS Delivery Architectures

5.1 Messaging Categories

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 Long Code (10DLC) telephone numbers, toll-free telephone numbers, or short codes, and delivered to a Consumer's mobile device that is identified by a TN. 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.

5.1.1 Non-Consumer to Consumer ("Non-Consumer")

Non-Consumer messaging commonly refers to messages initiated by a business or organizational entity.[11] 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

[10] Per second calculation based on 86,400 seconds per day.

[11] 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.

services from an MSP, which transmits messages to a downstream MSP for termination. There are often one or more additional MSPs 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.[12] 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.

5.1.2 Consumer to Consumer ("Consumer")

Consumer to Consumer messaging commonly refers to messages that are not initiated by a business or organizational entity.[13,14] These messages may be initiated through manual or automated means (as in the example of automated text responses) but are most often sent manually.[15]

5.2 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 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.

5.3 Sender ID Types

5.3.1 Email

Most WSPs 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 services are in common use by legacy applications. Many public service and community organizations use Email-to-SMS gateways to send messages to community members.

5.3.2 Short Codes

Historically, businesses and consumers sent messages using ten-digit TNs 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 U.S. require approval and are administered under the CTIA Best Practices [Ref 1]. Delivery of short-code messages is enabled by each terminating MSP before they can be used to terminate messages to that service provider's users. Short code resources are facilitated through the CTIA Short Code Registry (www.usshortcodes.com).

---

[12] 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 on a variety of devices.

[13] 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.

[14] 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 MSPs to clearly differentiate between Non-Consumer and Consumer messaging users today.

[15] 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.

5.3.3 10-Digit Long Codes (10DLC)

More recently for ten-digit phone numbers, documents such as the CTIA Best Practices [Ref 1], as well as interconnection agreement updates pushed by individual WSPs have attempted to define, identify, and separate traffic sent from 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.

Registration of 10DLC campaigns is facilitated by The Campaign Registry (https://www.campaignregistry.com). Specific phone numbers associated with each campaign are then registered in the netnumber Services Registry (nnSR) industry database as 10DLC (https://netnumber.com/the-netnumber-services-registry-nnsr/).

5.3.4 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. The nnSR contains all the toll-free numbers which are text-enabled and therefore registered for Non-Consumer messaging.

5.4 Non-Consumer Example Architecture

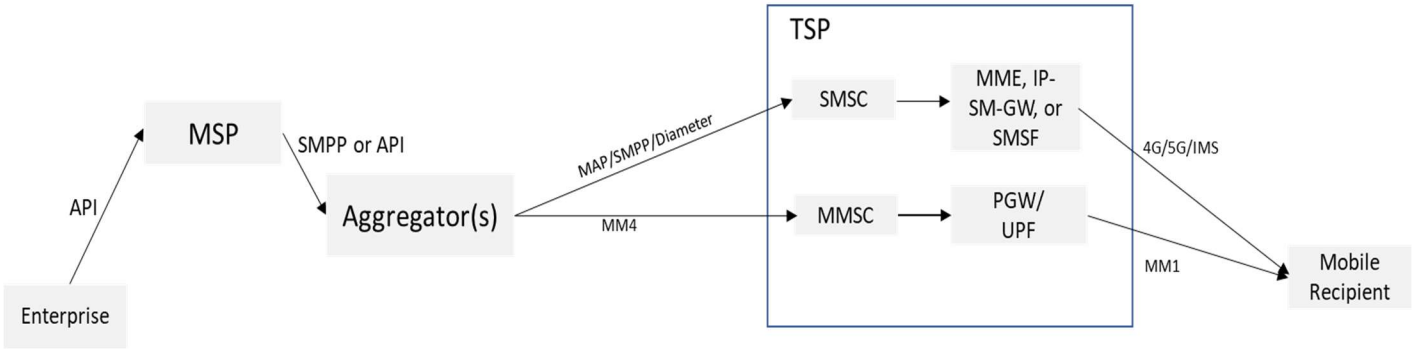

Figure 5-1: Non-Consumer Example Architecture

Figure 5-1 shows an example delivery architecture for Non-Consumer messages. It should be noted that for simplicity, roaming scenarios were not reflected in this diagram.

An enterprise sender uses an automated messaging application hosted at a Non-Consumer MSP to send messages through an Aggregator to an SMSC or an MMSC at the SP. When the mobile recipient is available, the SMSC forwards the text message to the mobile recipient via an SMSF, MME, or IP-SM-GW, or the MMSC forwards the multimedia message via UPF or PGW depending on the network type.

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 as illustrated below in Figure 5-2).

5.5 Consumer Example Architecture

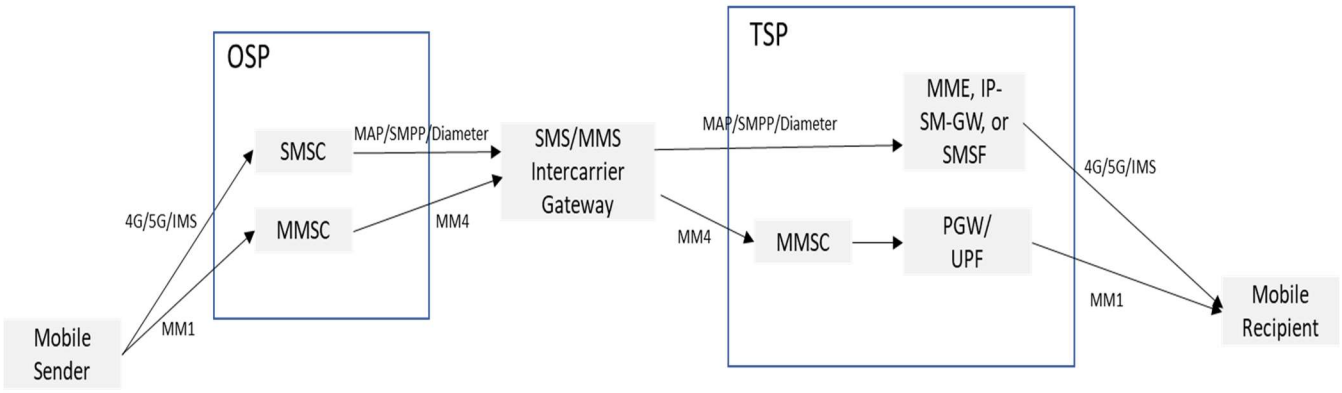

Figure 5-2: Consumer Example Architecture

Figure 5-2 shows an example delivery architecture for Consumer messages. It should be noted that for simplicity, roaming scenarios were not reflected in this diagram.

In this example, a mobile user sends an SMS or MMS to another mobile user. The SMS message is submitted to the SMSC and the MMS is submitted to the MMSC at the OSP. When the recipient is available, the SMSC/MMSC sends the message towards the recipient, typically via an SMS/MMS Intercarrier Gateway, which forwards the message to the mobile recipient via an SMSF, MME, or IP-SM-GW for SMS messages, or UPF or PGW for MMS messages depending on the network type.

6 Unwanted Text Messages

6.1 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.

6.1.1 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 user. In the text messaging context, spoofing a Sender ID is far less common than for voice calls. This Report uses the term “spoofing” to refer to falsified Sender IDs and distinguishes spoofing from other types of impersonation attacks that do not use fake Sender IDs.

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

- In SMS 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.[16] 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 Clause 7.3 for more detail on such countermeasures.

[16] Historically some messaging service providers allowed their customers to originate text messages from arbitrary sender numbers. Most U.S. market providers have stopped this practice.

- 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.[17,18]

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.

6.1.2 Non-Spoofed Impersonation

As discussed in Clause 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.

6.1.3 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.

6.1.3.1 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.

6.1.3.2 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.

---

[17] 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.

[18] At the time of this writing, several providers offer branded SMS services. These may be an exception to the assumption that SMS do not display caller name information. Depending on their design, such services could be vulnerable to SMS spoofing if such spoofing were possible.

6.1.3.3 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.

6.2 Message Insertion Techniques

6.2.1 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-compliant 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.

6.2.1.1 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.

6.2.1.2 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 many SIMs. SIM boxes may enable Non-Consumer traffic on Consumer channels. SIM boxes may also be used to enable TN cycling techniques.

6.2.2 Disposable TNs and Snowshoeing

Bad actors exploit “disposable” TNs, which are free or very inexpensive TNs generally obtained through web-based services or pre-paid SIM card purchases. Disposable TNs are typically used for a 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 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 MSP, they may be able to open new accounts and continue sending Unwanted Messages.

Snowshoeing is a technique where a message sender spreads similar messages across many different TNs in order to avoid volumetric detection or per TN volume limits. Snowshoe messaging is closely tied to the use of disposable or temporary TNs. 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.

6.2.3 Email Gateways

Email-to-SMS gateways are highly accessible and public means to reach a mobile customer. Most U.S. carriers allow customers to be reached via email using a <MSISDN>@domain address. These messages are then converted to SMS 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 to text 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.

There have been recent reports of the use of email-to-SMS gateways to disguise the sender of Unwanted Messages, where a specially constructed email "From" header field resulted in the display of a confusable Sender ID on the recipient's device. For example, messages were displayed apparently from a five- or six-digit number that a recipient might assume to be a valid short code.

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. They also help protect participating domains against certain impersonation attacks. Accordingly, The CTIA *Best Practices* [Ref 5] section 4.1 states that message senders should ensure that all messages utilize common or standardized email authentication technology (e.g., DomainKeys Identified Mail [DKIM], Sender Policy Framework [SPF]).

6.2.4 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 [Ref 5, Section 6].

Even if a messaging application or MSP 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.

7 Countermeasures

7.1 Registration and Vetting

Registration and vetting frameworks make it easier to identify legitimate messages and to label or 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. Campaign Registrars evaluate the reputation of the message sender, including a message sender's identity and messaging history. Sender ID Registrars confirm that a sender has 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, The Campaign Registry, and the nnSR.

7.2 Monitoring and Blocking

Messaging stakeholders use several tools and approaches to actively manage their networks.

SMSCs can integrate "SMS Firewall" services to provide monitoring, analytics, and filtering 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.

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 – Message 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.

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. 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 [Ref 5]. 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 systems that are distributing Unwanted Messages.

Beyond registries, providers may have information about potential sources of Unwanted Messages 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.

7.3 Anti-Spoofing Techniques

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

- MSPs only allow message senders to choose TNs that they are authorized to use.
- Access to the Intercarrier Gateway for Consumer messaging is limited to trusted partners. There are protections in place at the Intercarrier Gateway to ensure that an MSP (for example) can't submit a message from a number belonging to another MSP.[19]
- For Consumer messages, SMS Firewall services can query the sending number's HLR/HSS to determine that the subscriber is registered.

7.4 Sender authentication

Text messages, especially Non-Consumer messages, may cross several entities between senders and recipients. Only the first entity (typically an MSP) directly authenticates the identity of the SMS sender and verifies that the sender has the authority to use the TN. SMS uses a hop-by-hop model to communicate the Sender ID to the TSP and the end-user. This requires a transitive-trust approach among MSPs, Aggregators, Intercarrier Gateways, and WSPs.

The message recipients must trust that their WSPs only accept messages from trusted sources. TSPs must trust that aggregators and intercarrier gateways only accept messages from trusted MSPs or OSPs. MSPs and OSPs authenticate message 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 rather than through technical means.

7.5 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

[19] While messaging ownership of a text-enabled number can be recorded in the nnSR, access to changes is tightly controlled and must be performed or authorized by the carrier owner.

customers through 7726 to further calibrate spam filters and other sophisticated tools to protect Consumers from spam messages. Use of 7726 is described in CTIA Consumer Resources, *Protecting Yourself From Spam Text Messages* [Ref 6].

Certain end-user device platforms, such as iOS and Android, offer additional subscriber 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.

7.6 Forensic Analysis Cooperation

Messaging stakeholders often need to cooperate in forensic analysis to determine the source of Unwanted Messages. There are several documented best practices for forensic analysis cooperation [Ref 5, Section 3.2]:

- 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 Your 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.

7.7 Message Branding – Rich Sender Data

Several service providers have promoted “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 ensure message branding is not improperly applied.

7.8 Email Gateways

As mentioned in Clause 5.3.1, email-to-text gateways remain a 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:[20]

- Use standardized email authentication techniques, including Sender Policy Frameworks (SPF); DomainKeys Identified Mail (DKIM); and Domain-based Message Authentication, Reporting & Conformance (DMARC). These mechanisms help protect against attempts to impersonate protected domains in email that come from other sources. They may also help improve 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 Message Transfer Agents (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 MTAs that commit to certain best practices, for example, “Know Your Customer” practices. (See Clause 7.9)
- Only accept email from domains with which the SP has a contractual relationship or directly controls.
- Decommission email gateways entirely. This would be the simplest and most complete solution. But it is not typically feasible in the 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 can encourage such entities to move to using MSPs in the long run, with a goal of eventually decommissioning email gateways.

7.9 Best Practices

The Messaging and Malware Anti-Abuse Work Group (M^{3}AAWG) and CTIA have published relevant best practices documents: *M^{3}AAWG Mobile Messaging Best Practices for Service Providers* [Ref 7] and *Messaging Principles and Best Practices* [Ref 1], respectively.

CTIA’s Best Practices [Ref 1] 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;
- Any Service Provider 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 Message 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 CTIA Best Practices [Ref 1] 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* [Ref 5] identify several 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

[20] WSPs are understood to be taking action to mitigate Unwanted Messages via email gateways in parallel with the development of this Report, using some of the techniques mentioned in this section as well as others. This may have already reduced the impact of such gateways as a source of Unwanted Messages.

- 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
- MSPs and compromised API credentials or systems

8 Gap Analysis

This clause analyzes the currently available countermeasures for opportunities to further reduce Unwanted Messages.

8.1 Email Gateways

Implementation of best practices intended for email MTAs in general have significantly reduced Unwanted Messages sent via email gateways.

Some WSPs have enabled DMARC in their email gateways. DMARC also incorporates SPF and DKIM. This is helpful in reducing impersonation attempts against domains that publish DKIM and DMARC.

There may be opportunities to further reduce Unwanted Messages via email gateways by implementing other techniques described in Clause 7.8. If WSPs move gateway users to friendly MSPs instead of email or require gateway users to have direct, authenticated relationships with WSPs, it might be possible to further reduce email origination of Unwanted Messages. These opportunities are based on existing standards and best practices and are not likely to require new standards work.

8.2 Transitive Trust

Clause 7.4 describes the hop-by-hop trust model currently in effect for SMS messaging. This is effectively a transitive-trust model. A transitive model depends on each intermediary in the message path to do its job correctly. This creates a larger attack surface than would be the case with an end-to-end approach. If an intermediary becomes compromised or otherwise fails to implement proper controls, the chain of trust relationships is broken.

Transitive trust for text messaging has worked reasonably well in practice, as evidenced by the lack of a significant problem with spoofed Sender IDs. The ecosystem is more tightly controlled than that of email or even voice. Stake holders that do not follow required practices risk having their traffic blocked and interconnections terminated by downstream intermediaries or WSPs.

Existing end-to-end attestation frameworks such as ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)* [Ref 8], are designed to work with SIP-based services that can imbed signed PASSporTs in the SIP request headers. The IETF STIR working group published RFC 9475, *Messaging Use Cases and Extensions for STIR* [Ref 9], a document that applies STIR to SIP-based messaging; however, the existing SMS infrastructure is not end-to-end SIP so RFC 9475 cannot be applied to SMS without further standards development. RFC 9475 [Ref 9] does mention the potential application of STIR to non-SIP messaging using out-of-band techniques, but adapting it to do so would require additional standards work.

8.2.1 Impact on Forensic Analysis Cooperation

The transitive-trust model means that forensic cooperation requires the involvement of each entity in the message path. If any such entity fails to cooperate or fails to keep sufficient logs, Unwanted Messages cannot be traced back to the original sender. By contrast, end-to-end attestation frameworks only require the cooperation of the entity that attested to the Sender ID.

Note that, even with SHAKEN [Ref 8] in place, voice calls are sometimes delivered with incorrect attestation. This can be for any number of reasons, many of which do not involve bad actors or intentions. Even so, STIR/SHAKEN still has the advantage of enabling downstream parties to directly identify the call signer.

8.2.2 Impact on Monitoring and Blocking

Sender ID can be an important input into message filtering algorithms and end-user display decisions, but only to the degree that the information can be trusted by the terminating TSP. While WSPs do not generally deliver messages from untrusted sources, transitive-trust relationships are by nature indirect. If any entity in the message path fails to adhere to correct procedures and best practices, the chain of trust may be broken.

9 Conclusions

Text messaging continues to be a trusted source of communications, but bad actors are increasingly finding ways to deliver spam or scam messages to U.S. consumers. In considering technical solutions to mitigate spam or scam text messages, SMS-based text messaging has the distinct advantages of being asynchronous, carrying content that can often be analyzed prior to delivery to the message recipient, and at least for messages sent from U.S. phone numbers, Sender ID spoofing is uncommon. The wireless industry also uses filtering technologies and registration systems that have successfully mitigated an enormous amount of fraudulent messaging traffic. These advantages and solutions make it challenging to identify additional technical solutions to mitigate Unwanted Messages, but there is value in evaluating potential technical solutions that can streamline or bring consistency to these efforts, particularly for verifying Sender ID information at scale.

Accordingly, while the joint ATIS and SIP Forum IP-NNI Task Force has focused primarily on voice, this Technical Report has been created to establish a baseline of member understanding of U.S.-based text messaging. For example, systems such as STIR/SHAKEN [Ref 8] were not initially designed to apply to SMS messaging and currently do not directly apply to that channel. Based on this Report, the IP-NNI TF would like to convene experts in text messaging to discuss technical solutions to drive efficiency and improve intelligence in mitigating Unwanted Messages. Sourcing broad expertise from email, internet security, financial institutions, and others may further improve perspectives and ensure that the communications industry can capitalize on systems and learnings gleaned from other industries. Discussions should start with establishing shared goals and a common understanding of currently captured data and intelligence, any processes or standards for vetting or verifying that data and when those means are applied, and how traffic is reviewed and treated to mitigate fraud.

10 Recommendations

The ATIS/SIP IP-NNI TF proposes the creation of an ATIS/SIP Forum joint task force under or in parallel with the IP-NNI TF to evaluate and, if necessary, develop new standards for verified identity transmission and validation in text messaging (i.e., authentication). The TF should first focus in educating participants in available mitigation tools, resources, and techniques prior to any consideration of new standards, as well as provide a venue for ongoing discussion. Participation should include experts in establishing trust frameworks or policies, vetting identity credentials, the secure transmission of identity information, and mitigating fraudulent traffic.