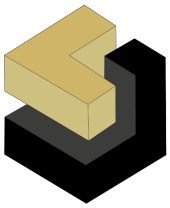

One Consortium

ONE CONSORTIUM

White Paper – Messaging

Release 1.0 – January 2026

Working Group 5

Executive Summary

Messaging has become a foundational communications channel for consumers, businesses, and governments worldwide. Short Message Service (SMS), Multimedia Messaging Service (MMS), Rich Communications Services (RCS), and Over-the-Top (OTT) messaging applications are now used interchangeably by consumers, despite using different technologies and being governed by markedly different regulatory frameworks. This divergence has created significant challenges in protecting consumers from spam, scams, and fraud, while simultaneously complicating enforcement, accountability, and industry coordination.

This white paper examines the global messaging ecosystem and highlights how inconsistent regulatory treatment across message types and jurisdictions has enabled fraud to migrate from more regulated channels, such as SMS, into less regulated or unregulated environments, including RCS and OTT platforms. Encryption, while critical for privacy and security, further limits visibility and hampers traditional network-based mitigation tools, exacerbating risks as messaging traffic increasingly shifts away from carrier-operated services.

The paper outlines key messaging technologies and use cases, including person-to-person (P2P) and application-to-person (A2P) messaging, and describes the complex ecosystem of stakeholders involved in message origination, routing, delivery, and enforcement. It reviews regulatory approaches across multiple regions, demonstrating that similar consumer-facing messaging services are often subject to vastly different legal obligations, even within the same country. These disparities undermine consumer trust, weaken fraud prevention efforts, and increase compliance burdens for legitimate businesses operating across borders.

The analysis also details the evolving threat landscape, including spam, phishing and smishing scams, SIM box abuse, artificial inflation of traffic (AIT), spoofing, and message reselling. It assesses existing mitigation tools, such as registries, KYC and brand vetting frameworks, traceback initiatives, industry codes of conduct, and consumer reporting mechanisms, while acknowledging their limitations—particularly in encrypted and non-carrier-operated environments.

To address these challenges, the paper offers a set of strategic, forward-looking recommendations aimed at strengthening consumer protection and restoring trust in messaging services globally. These include greater policy harmonization across messaging channels, alignment and interoperability of national brand and campaign registries, enhanced industry and cross-industry collaboration, unified global KYC standards, improved traceback and intelligence-sharing frameworks, and expanded education and awareness initiatives for regulators, industry participants, and consumers. The paper also emphasizes the need for rigorous security practices and privacy-respecting approaches to addressing abuse in encrypted messaging environments.

By aligning regulatory principles, technical standards, and industry best practices across SMS, RCS, and OTT messaging, and by leveraging international coordination through industry and regulatory forums, stakeholders can create a more consistent, resilient, and trusted global messaging ecosystem. This white paper provides a roadmap for achieving that goal while balancing innovation, privacy, and consumer protection in an increasingly complex messaging landscape.

One Consortium

CONTENTS

Introduction

As consumers increasingly rely on messaging to communicate, protecting consumers from scams and spam is critical to maintain consumer trust. Different message types and technologies, encryption methods, and varying regulatory treatment make it difficult to fight spam and scam messages, creating challenges in combatting fraud and maintaining trust. This paper explores the messaging landscape, outlines regulatory disparities, highlights threats to consumers and tools to mitigate harm, and recommends key strategies and initiatives to combat messaging fraud and enhance consumer protection in global messaging services.

I. Voice and Messaging Platforms are Different

Traditional voice calls use circuit-switched technology in the Public Switched Telephone Network (PSTN) while carrier-operated Short Message Service (SMS) messaging platforms use packet-switched technology. Messages flow from the sender to the recipient over SMS platforms from various sources, including, but not limited to other devices, Over-the-Top (OTT) applications, and email-to-text gateways.[1] Although text messages may use 10-digit numbers for routing purposes, they do not touch the PSTN.

The delivery of voice calls often involves a long chain of providers. In contrast, the routing of SMS messages differs based on the type of traffic. For Peer-to-Peer (P2P) messages, providers usually require an indication of the originating provider when a message enters the network.[2] This allows other providers to identify the source using an industry-wide routing database. The path for P2P messages is generally deterministic, meaning there's a single, direct path from sender to receiver.

However, Application-to-Person (A2P) or Business SMS routing can be more complex and resemble voice call routing, with the potential for multiple hops through Campaign Service Providers (CPs), Connectivity Partners (CNPs) and Direct Connect Aggregators (DCAs). [See Table 2] Additionally, while checks on the legitimacy (registration) of message Campaigns and associated sending numbers or caller identification (CIDs) are contained in registries, such as The Campaign Registry (TCR) and CTIA's Short Code Registry in the U.S., their application across the messaging chain has been adopted and can be identified through API calls to NetNumber and Somos.[3] Brands often have multiple Campaigns, utilize multiple Suppliers (CSPs, CNPs, DCAs) and may split network delivery. The same Campaign can have one (1) or 1000's of Numbers delivering messaging content.

II. Messaging Types

"Text message" is a term that has become synonymous with any message sent to or received by a consumer via wireless device, regardless of the service provider (mobile network operator vs. technology company) or the technology. For wireless consumers,

[1] All U.S. Tier 1 Mobile Network Operators (MNOs) shut down their respective email-to-text gateways in 2025 due to problems with spam.

[2] Messages can operate over SMS in carrier-operated networks or IP-based services like over-the-top messaging apps (e.g., WhatsApp, WeChat, and iMessage.)

[3] Routing databases include the NetNumber Services Registry (nnSR®) or for toll-free, the Texting and Smart Services (TSS) Registry.

it might be difficult to distinguish from among the following message types and underlying technologies:

SMS & MMS (Short Message Service & Multimedia Messaging Service)
SMS and MMS are carrier-operated messaging services that are routed through messaging service provider networks. SMS supports text only, while MMS supports multimedia, including images, and video. SMS is used throughout this paper to refer to both SMS and MMS.

RCS (Rich Communications Services) / RBM (RCS Business Messaging)
RCS operates over cellular data (4G/5G) or WiFi. RCS, and RCS Business Messaging (RBM) offer real-time texting notifications, read receipts, file sharing, high-resolution photo and video sharing, and encryption. RBM is the communication protocol for non-consumer/business rich messaging.

OTT (Over -the-Top)
OTT or Internet protocol (IP) based messaging applications can be downloaded from smartphone app stores or are native to a wireless device. Some applications are used exclusively over the Internet and use IP addresses for routing, and other applications exchange messaging traffic over the Internet.

Table 1: Comparison of Message Types

Type	Operator Controlled	End-to-End Encryption	Interoperability	Regulatory Oversight
SMS	Yes	No	High	Yes
RCS	Partial	Yes[4]	Moderate	Limited
OTT	No	Yes	Low	Rarely Regulated

Wireless consumers can utilize the messaging client native on their respective device (e.g., Apple's iMessage, Google Messages, or Samsung Messages). If a messaged party is an iPhone user and does not have an Internet connection or the customer chooses to disable RCS or iMessage on the device, messages can still be sent and received via SMS or MMS. Wireless consumers can also download an OTT messaging app (e.g., WhatsApp or WeChat) to their device to exchange messages. In the United Kingdom, most messages sent today are OTT, which do not traverse the cellular network.[5]

[4] Google Messages and iMessage are end-to-end encrypted. GSMA has released specifications for interoperable end-to-end encryption, but as of the date of this paper, it has not yet been implemented.
[5] According to Statista, the number of outgoing SMS and MMS messages sent in the United Kingdom (UK) has fallen significantly over the past decade, from a peak of over 150 billion in 2012 to around 32 billion in 2023. The decline in SMS use in the UK has been driven by the broad adoption of alternative messaging services such as WhatsApp. https://www.statista.com/statistics/271561/number-of-sent-sms-messages-in-the-united-kingdom-uk/

III. Messaging Use Cases

Person-to-Person/Peer-to-Peer (P2P) Consumer

P2P messages are typically sent by one individual to another individual and are used to communicate with friends, family, and other known contacts. Consumers do not include agents, representatives, or any other individuals acting on behalf of non-consumers, including businesses, organizations, political campaigns, or entities that send messages to consumers.

Application-to-Peer/Person (A2P)/Business SMS

A2P / Business SMS are sent to a consumer by a business or entity using a software application or web-based system to send mass messages to a larger customer base.

Messaging Ecosystem

The A2P / Business SMS ecosystem involves several stakeholders who collectively generate, process, and deliver messages via sanctioned and supported channels. Mobile Network Operators (MNOs) and other messaging stakeholders have developed best practices and codes of conduct that message senders are encouraged or required to abide by to help protect wireless consumers from unwanted or fraudulent messages.

Table 2: A2P / Business SMS Messaging Ecosystem Stakeholders

Role	Description
Brand /Content Provider (message generator)	Entity initiating the message (e.g., a business)
Campaign	Type of message (e.g., marketing, alerts)
Campaign Service Provider (CSP)	Launches campaigns; has direct contact with the Brand/Business sending the message.
Connectivity Partner (CNP)	CNPs provide the connection between the CSPs and the MNOs[6]
Connectivity Partner	Facilitates message routing to MNOs
Aggregator	Bridges CSP/CNP with MNOs
Direct Connect Aggregator (DCA)	Provides direct connection to MNO gateways
Registry	Collects brand and campaign data for validation

[6] In the U.S. every CSP that registers with The Campaign Registry is automatically added to the list of electable CNPs.

Rollout of RBM

On the A2P / Business SMS side, the global rollout of RBM is launching in phases. Germany quickly emerged as a gold standard for RCS adoption and implementation due to several key reasons:

- Carrier collaboration: MNOs work closely to deliver unified RCS experience, investing in infrastructure and ensuring cross-network interoperability.
- Privacy and Security: Strong data protection laws like GDPR have driven secure RCS deployments, aligning with features like end-to-end encryption and verified senders.
- Business Innovation: Industries such as retail, finance, and logistics use RCS for interactive support, personalized offers, and transactional messaging.
- Robust Infrastructure: Germany's advanced telecom infrastructure supports seamless RCS rollout.
- Early Adoption: As an early RCS adopter, Germany has developed mature practices and a stable ecosystem.
- Partner Enablement: Operators proactively support aggregators and brands, accelerating enterprise RCS deployment.

While Germany has been recognized as a benchmark for successful RCS deployment, several other countries have also demonstrated strong carrier collaboration in RCS implementation, though perhaps not always to the same extent or with the same public visibility. For example, Google is still working to launch its RBM product in the U.S, while India, South Africa, Mexico, Spain and France are already using RBM and reportedly experienced the biggest increase in 2024. An average of 15% of smartphone users across the five markets received messages via RBM.[7]

[7] MEF's 10th Annual Consumer Trust Study available via https://mobileecosystemforum.com/10th-annual-trust-study/

IV. Regulatory Treatment by Country and Message Type

Despite being used interchangeably by consumers, text messages are subject to different legal and regulatory regimes, even within the same country.

Table 3: Regulatory Overview by Country

Examples are shown below.

Country/ Region[8]	SMS	RCS	OTT	Lead/Primary Regulator
U.S.	Yes	No	No	Federal Communication Commission (FCC)
EU	Yes	Limited (via GDPR)	Limited	European Commission
Canada	Yes	No	No	Canada Radio-television and Telecommunications Commission (CRTC)
Australia	Yes	Yes	Limited	Australian Communications and Media Authority (ACMA)
Singapore	Yes	Limited	Limited	Infocomm Media Development Authority (IMDA)
India	Yes	Limited	Limited	Telecom Regulatory Authority of India (TRAI)
Ghana	Yes	No	No	National Communications Authority
Germany	Yes	Yes	Yes	Bundesnetzagentur

U.S.

In the U.S., SMS messaging is subject to federal laws, including the Telephone Consumer Protection Act, the Truth in Caller ID Act, Do Not Call rules, and the TRACED Act, as well as federal regulations promulgated by the Federal Communications Commission (FCC). However, IP-based messaging services, including OTT and RCS, are not subject to regulation by the FCC.

In 2023, the FCC adopted a Report and Order and Further Notice of Proposed Rulemaking[9] that requires wireless providers to block texts based on a reasonable Do Not Originate (DNO) list and to maintain or ensure that entities that block texts on their networks maintain a single point of contact for message senders to report erroneously

[8] For a comprehensive survey of message regulation by country, please refer to One Consortium's International Survey.
[9] See *In the Matter of Targeting and Eliminating Unlawful Text Messages, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-21, CG Docket Nos. 21-402 and 02-278, rel. Mar. 17, 2023.

blocked texts. Also in 2023, the FCC adopted a Second Text Blocking Order and Second Further Notice of Proposed Rulemaking[10] to require wireless providers to block texts from a particular number or numbers following Commission notification of illegal texts and encourage providers to make email-to-text service available on an opt-in basis.

Europe

In May of 2018, the European Union (EU)'s General Data Protection Regulation (GDPR) went into effect, imposing data privacy and security standards governing the collection, access, usage, and processing of personal data, including messaging services. GDPR rules require business message senders to obtain explicit, informed consent and enable customers to opt-in or opt-out of receiving messages. Message senders are also subject to requirements to securely store customer conversations, implement measures to protect data against unauthorized access, and maintain and make public a privacy policy that outlines the collection, processing, and storage of data in compliance with GDPR regulations.

UK

Recent SMS consultations and guidance include:

Initiative	Status	Focus
A2P SMS termination market review	Completed / Outcome issued (Oct 2025)	Termination pricing, market power, and voluntary commitments
Combatting mobile messaging scams	Active consultation (closes Jan 2026)	Rules & guidance to prevent scam messages (P2P & A2P), identity verification
Draft guidance on protections from scam mobile messages	Published 29 Oct 2025	Helps providers interpret proposed protections

Singapore

To address the increasing threat of fraudulent and misleading SMS messages, the Infocomm Media Development Authority (IMDA) established the comprehensive Singapore SMS Sender ID Registry (SSIR) regime on an optional basis in March 2022.[11] On January 31, 2023, Sender ID Registration became mandatory for all organizations utilizing SMS with alphanumeric Sender IDs for A2P / Business SMS traffic in Singapore. Under this new whitelist-based approach, businesses must register their secured SMS

[10] See *In the Matter of Eliminating Unlawful Text Messages, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Advanced Methods to Target and Eliminate Unlawful Robocalls,* Second Report and Order, Second Further Notice of Proposed Rulemaking, FCC 23-107, CG Docket Nos. 02-278 and 21-402, and Waiver in CG Docket No. 17-59, rel. Dec. 18, 2023.

[11] Singapore's SMS Sender ID Registry, https://www.sgnic.sg/smsregistry/overview

Sender IDs against their Unique Entity Number (UEN) to send SMS messages to customers. Any Sender IDs that are not registered are automatically flagged as "Likely-SCAM." Registered Sender IDs must be processed through authorized and participating aggregators.

India

The Telecom Regulatory Authority of India issued a directive to help mitigate spam by requiring telecom companies to stop transmitting messages with URLs, OTT links, Android application packages (APKs), or call-back numbers that are not whitelisted to prevent phishing. Under the directive, banks, financial institutions, and online platforms were required to register message content by August 31, 2024, or risk their messages being blocked.[12]

Ghana

Ghana's National Communications Authority (NCA) sought comments on draft guidelines for the management of network promotional messages. The guidelines seek to provide opt-in and opt-out mechanisms for consumers and help with message sender identification.[13]

V. Customer Consent

As noted above, many countries treat messaging services differently, whether by regulation or industry self-governance. However, most countries do require some form of opt-in consent prior to sending non-consumer texts, and a mechanism for customers to opt-out and unsubscribe from future messages from the sender. There is also an expectation that consent records be stored. However, how and where a customer opts-in to receive A2P / Business SMS / RBM messages and where that consent is managed and owned might differ by country and across message types.[14] Further, in many countries consent travels across messaging services without additional consumer consent (e.g., SMS to RCS).

---

[12] *TRAI Mandates Whitelisted URLs, APKs, or OTT links for SMS Traffic*, Telecom Regulatory Authority of India, September 26, 2024, Press Release. https://www.trai.gov.in/sites/default/files/2024-10/PR_No.67of2024.pdf

[13] *Public Consultation on Draft Guidelines for the Management of Network Promotional Messages*, National Communications Authority, 2024, https://nca.org.gh/wp-content/uploads/2024/08/GUIDELINES-ON-NETWORK-PROMOTIONAL-MESSAGES-2.pdf

[14] In the U.S., message senders are encouraged to document and retain opt-in consent, including a timestamp and the medium of consent acquisition, the campaign that the consumer opted in to and method of consent, along with the consumer phone number, name or identifier of individual who consented. *See* CTIA Messaging Principles and Best Practices, May 2023. https://api.ctia.org/wp-content/uploads/2023/05/230523-CTIA-Messaging-Principles-and-Best-Practices-FINAL.pdf

Table 4: Customer Consent by Country

Examples are shown below.

Country/Region	Required Consent	Best Practice/Industry Guidelines
EU	Yes	No
United Kingdom	Yes	No
United States	Yes	Yes
Canada	Yes	Yes
Australia	Yes (some exemptions for transactional)	Limited
India	Yes	No
Singapore	Yes	No
New Zealand	No	Yes

VI. Know your Customer (KYC) /Brand Onboarding and Verification

The onboarding and vetting of brands for business-to-consumer (non-consumer) messaging across the United States, Canada, and Europe involves a multi-layered process designed to ensure compliance, authenticity, and consumer protection. Messaging channels such as SMS, MMS, 10DLC, Toll-Free messaging, and RBM each have distinct market, regulatory, and/or MNO requirements, but share a common emphasis on verifying brand identity, securing consumer consent, and preventing fraud. We are beginning to see this activity, especially for SMS and Sender ID, across these and other regions, including India and Ireland. Onboarding typically includes submission of brand information, validation of legal entities, verification of brand identity, and vetting provided by MNO approved entities. Messaging aggregators, CNPs, and CSPs must analyze the right-to-use assets and/or a behavioral history analysis to prevent bad actors from entering the channel. Standards are geared to align with local laws and telecom standards.

A critical component of the vetting process is the ability to trace messaging activity back to the responsible entity, ensuring accountability and transparency across the ecosystem. This traceability not only supports regulatory enforcement but also helps prevent bad actors from re-entering messaging channels after being shut down for violations. Vetting platforms support automated workflows and customizable KYC configurations to meet the varying needs of each channel and jurisdiction. Additionally, work is being done to enable unified vetting for brands operating on multiple channels that are entering networks via multiple Direct Carrier Aggregators (DCAs). This improves efficiency and reduces costs for the ecosystem while creating a secure, scalable, and compliant messaging environment across all markets that enables brands to engage consumers responsibly and effectively.

VII. Messaging Threats and Abuse

Fraudulent messages generally fall into one of the following categories: identity theft/spoofing, data theft, commercial exploitation, network/system manipulation, and disallowed content.[15] The financial impact of messaging fraud on both consumers and MNOs is significant.[16] According to Mobilesquared, MNOs lost an estimated USD $3.64B in 2021 due to A2P events via the SMS channel resulting from unsanctioned use of MNO networks to send non-consumer messages, commonly known as ”grey routes.“ This figure represents 16% of MNOs' potential A2P / Business SMS revenue. SMS attacks increased by an average of 30% in 2021, with 55% of MNO respondents confirming this trend in ROCCO Research's SMS Firewall Vendor Benchmarking Report 2022.[17]

Spam

“Spam” is a broad term for any unwanted or unsolicited message regardless of whether the sender has malicious intent.

Scam

“Scam” messages refer to deceptive, fraudulent messages intended to promise something (e.g., money, prizes, employment, etc.) by enticing the recipient to provide personal information, including bank account information, credit card information, or other personal information (e.g., a Social Security number) to claim a gift or reward.

SIM Box Abuse

SIM boxes are devices that enable SMS/MMS spam (and voice spam) to be sent from multiple Subscriber Identity Module (SIM) cards, often obtained for prepaid service. The use of SIM boxes allows criminals to make calls or send messages from a SIM card in one part of the world through wireless networks in another part of the world, bypassing higher international tariffs and evading applicable regulations. In some cases, scammers may deploy SIM boxes vertically allowing scammers to control and use their own SIM boxes to make money from messaging-based schemes like phishing/SMishing. In other cases, SPam-as-a-Service (SPaaS) providers use large SIM box networks to provide bulk messaging services to criminal clients.

SIM boxes can be located through customer detail records (CDR) and IMEI analysis, historical cell site analysis, radio frequency triangulation, data mining 7726 (SPAM)

---

[15] In the U.S. and Canada, there are clear guidelines on message types that are not permitted to run over any carrier-operated messaging platform based on MNO Messaging Codes of Conduct. Disallowed content includes, but is not limited to high-risk financial services, third-party debt forgiveness, and sex, hate, alcohol, firearm, or tobacco (”SHAFT”) message content. *See* https://community.sinch.com/t5/SMS/A2P-Messaging-in-the-United-States-amp-Canada-Disallowed-Content/ta-p/7091 and https://help.twilio.com/articles/360045004974-Forbidden-Message-Categories-in-the-US-and-Canada-Short-Code-Toll-Free-and-Long-Code_

[16] According to the Federal Trade Commission, Americans lost a total of nearly $440M through text message scams in 2022. “How much does text message fraud cost Americans?” USAFacts, December 11, 2023, https://www.usafacts.org/articles/how-much-does-text-message-fraud-cost-americans

[17] *SMS Firewall Vendor Benchmarking Report*, 2022, ROCCO Research, www.roccoresearch.com/tag/sms-firewall/

customer complaints, and examination of payment, activation, and SIM shipment records. SMS spam can also be sent to wireless consumers from large numbers of bulk-activated free email accounts, such as Gmail and Outlook via Simple Mail Transfer Protocol (SMTP).

Artificial Inflation of Traffic (AIT) / SMS Pumping / Revenue Share Fraud

Artificial inflation of traffic (AIT) or SMS pumping is a type of fraud in which bad actors exploit a system or website that sends legitimate alerts or notifications via SMS, including one-time PINs sent from businesses. The attackers use bots to generate large volumes of fake SMS to exploit and profit from the way MNOs charge for SMS delivery. According to a joint report by Enea and Mobilesquared[1], more than 20B fraudulent AIT messages were sent in 2023, costing the industry an estimated $1.16B.

Message Reselling

The wireless industry has also observed cases of companies offering mobile subscribers the option to resell their messaging quota for a gift voucher or a cash credit. This has allowed criminals to take advantage of the unlimited messaging plans offered by mobile operators. MNO or MNO customers sell SIM cards/MSISDN or their numbers to generate SMS terminations and originations. The subscriber must download an app that triggers messages from the mobile subscriber number to global numbers.

Spoofing

In the U.S., originator number spoofing – sending bulk text messages from a number that is not registered to the originating service provider – is rare. Identity spoofing/imposter fraud – a scam involving impersonation of a brand or government agency designed to extract sensitive personal information or to defraud consumers – is a more common issue. However, originator number spoofing is more common in the UK and other countries where A2P/CPaaS providers use alphanumeric numbers that can be manipulated.

VIII. Mitigation Tools

Network Tools
MNOs have spam filters and other network-level defenses in place to identify threats, analyze complaints, and to block illegal and unwanted traffic. The messaging ecosystem has developed and employed additional tools to protect consumers, which include, but are not limited to the following:

SMS Firewall
SMS firewalls can safeguard against fraudulent activities, including grey routes exploited by aggregators, to maximize profits by abusing mobile network vulnerabilities. By monitoring all entry points (e.g., on-net & off-net traffic, SIM boxes, international SCCP carrier SS7) of mobile networks, SMS firewalls can protect against spam and threats and avoid revenue leakage from grey routes.

Regular Network Efficiency Testing / Network Penetration Testing
Network efficiency or penetration testing can be used to identify vulnerabilities in messaging infrastructure, strengthening security to ensure effective monetization. For those MNOs with SMS firewalls in place, Network Penetration Testing aids in optimizing the SMS Firewall performance (e.g., firewall algorithm optimization recommendations). It can also help identify illegally leased Global Titles and spot bad actors who are manipulating message content or sender IDs. Network penetration testing can be used by MNOs to detect SMS grey routes and bypass, increasing SMS firewall performance, and optimizing SMS monetization.

STIR/SHAKEN
STIR/SHAKEN refers to a set of Internet Engineering Task Force (IETF) and Alliance for Telecommunications Industry Solutions (ATIS) technical standards and protocols for IP networks to authenticate caller identity to combat spoofing by allowing authenticated metadata associated with a phone call to travel with the call. This verifies to the terminating provider that the originating number was not changed in transit (i.e., spoofed) and enables call signatures to be used as forensics information for traceback and enforcement purposes.

The IETF has been exploring how STIR/SHAKEN could be used to authenticate text messages, assuming those messages are sent using the SIP protocol. However, text messages sent from mobile phones on 4G/5G networks often get converted into other formats—like Apple's iMessage or the SMPP protocol—before reaching their destination. This makes it difficult to add STIR/SHAKEN signatures to these messages, because protocols like Short Message Peer-to-Peer (SMPP) would need to be changed to support digital signatures. Updating these standards would require agreement across the industry and the development of a new digital identity system.

Currently, there are no widely accepted standards for using STIR to authenticate text messages. Even if such standards were proposed, they would likely face major challenges due to complexity, cost, and the rapid decline in the use of SMS.

Messaging Platform Security

In an era of increasing cyber threats, there are enhanced "best practice" security measures that organizations can implement to protect their communications. For example, at the core of preventing unexpected access and account takeover (ATO) fraud are:

- *Strong Authentication*: Enforce multi-factor authentication (MFA) and strict password policies.
- *Access Controls:* Restrict dormant accounts, limit login attempts, and apply least privilege access.
- *Session Management*: Automatically log out inactive users to reduce exposure.
- *Secure Integrations*: Protect APIs with OAuth 2.0 and rotate keys regularly.
- *Monitoring & Alerts*: Continuously audit account activity, apply anomaly detection, and act quickly on suspicious behavior.
- *Incident Response*: Maintain a clear incident response plan with communication protocols upstream and downstream.

IX. Industry Tools

Registries

Several countries, including the U.S., UK, India, Ireland, Australia and Singapore, have implemented, or plan to implement, more trusted Business Messaging through the mechanism of a National Brand or National Campaign Registry. These registries enable MNOs to identify and mitigate potential abuse by A2P / Business SMS message senders by verifying the sender's identity and risk profile to facilitate adherence to best practices, while mitigating spam and abuse and aiding in message delivery for wanted messages. Based on experiences thus far, this solution will likely help significantly reduce spam, fraud, spoofing, and scams. Many national regulatory agencies are now actively exploring this solution.

For example, in 2018, MEF announced the creation of a collaborative effort between the National Cyber Security Centre (NCSC) and the mobile, banking, and finance industries in the UK to enable information sharing to help identify and block fraudulent SMS spoofing and phishing attempts.[18] The Registry enables businesses and organizations to register their message headers to prevent fraudsters from impersonating brands by checking whether the sender ID is a legitimate, registered sender.

In 2024, the TRAI issued a directive to senders of SMS messages in India using the Distributed Ledger Technology (DLT) platform to require call to action (CTA) campaign whitelisting.[19] Under the directive, senders using URL shortening in their respective CTA

[18] MEF SMS Sender ID Protection Registry, https://mobileecosystemforum.com/sms-Sender ID-protection-registry
[19] TRAI Directive, September 26, 2024, https://www.trai.gov.in/sites/default/files/2024-10/PR_No.67of2024.pdf

campaigns must include a registered sender ID to be whitelisted and avoid blocking. CTAs in RCS and WhatsApp messages are not impacted.

Recognizing the challenges of a nation-by-nation approach to global messaging (especially from global brands and global business messaging providers) if each country takes a completely different approach in terms of principles, functions, technology and governance, the One Consortium Messaging Working Group identified and proposes some level of global best practice, harmonisation, and international standards while recognising the sovereignty of each country's policies, practices, and obligations. This may well involve collaborating with other industry and regulatory associations who are actively developing these solutions.

An example of this collaboration is a current plan to work with MEF on reviewing and potentially adopting their Trusted Messaging Working Group document titled, "High Level Principles / Best Practices to Enable Trusted Business Messaging." This document defines principles and best practices for establishing a trusted business messaging ecosystem, designed to ensure a secure environment for sensitive business communications for native mobile messaging on a national and global scale. It covers Sender ID, national registries and global engagement and harmonization across national registries.

Industry Best Practices / Self-Regulation

Best Practices for A2P / Business SMS include policies and practices that messaging ecosystem stakeholders develop and follow to facilitate the delivery of messages to the consumers who want to receive them. Existing best practices, as well as those still under consideration, recommend a message sender obtain prior consent to send messages and provide a mechanism for the consumer to revoke consent and stop receipt of future messages.

Joint i3Forum and Global Leaders Forum (GLF) Messaging Code of Conduct

The joint Code seeks to combat fraud in the international market by encouraging organizations to follow five key principles to combat SMS fraud, such as monitoring and blocking suspicious traffic and sharing information about fraudulent activity. The Code also stresses the need for organizations to comply with all relevant regulations and contractual agreements.

MEF Code of Conduct

Examples of industry best practices include MEF's Business SMS Code of Conduct (the "Code"), which sets out best practices for all actors operating within the Business SMS

sector.[20] The Code offers 10 principles on commercial, procedural, and technical requirements for A2P and P2P messages, with a focus on consumer protection. Signatories to the Code commit to adhere to the Code or face sanctions.

CTIA Messaging Best Practices

In the U.S., CTIA's Messaging Best Practices are voluntary best practices developed to protect and ensure consumer trust in messaging. The best practices apply to messaging services that use 10-digit numbers assigned from the NANP as the unique identifier for the sender and/or recipient of individual or group messages, which includes SMS, MMS, and RCS messages. Under CTIA's Messaging Best Practices, message senders are expected to obtain consent from message recipients for the recipients to receive messages and provide message recipients with the ability to revoke consent. Ecosystem stakeholders apply these guidelines through commercial agreements and policies in conjunction with registration and vetting frameworks to protect consumers from unwanted messages and maintain consumer trust in the messaging platform.[21] Many U.S. based carriers also have their own respective Messaging Codes of Conduct that incorporate by reference CTIA's Messaging Best Practices.

CTIA Messaging Security Best Practices

CTIA also has best practices on the wireless industry's efforts to protect consumers from unwanted messages and preserve trust in the messaging platform. In late 2025 and again in early 2026, CTIA revised its Messaging Security Best Practices[22] to address SIM Card enabled messaging abuse and included Threat Mitigation Best Practices that encourage wireless providers, MVNOs, and other messaging service providers to actively monitor messaging activity, employ detection technologies, and use analytics to identify and prevent wireless messaging abuse by message senders. Proactive

---

[20] Mobile Ecosystem Forum Business SMS Code of Conduct v2.0, December 14, 2020, https://www.mobileecosystemforum.com/wp-content/uploads/2020/12/mef-codeofconduct-business-sms_v2.0_RELEASED-1.pdf

[21] *See e.g.*, AT&T, *AT&T Code of Conduct for Short Code and 10-digit A2P SMS Messages* (Aug. 14, 2020), https://sinch.github.io/docs/sms/sms-other/downloads/ATT_Code_of_Conduct_062020.pdf; T-Mobile, *Code of Conduct* (Nov. 2020), https://www.t-mobile.com/support/public-files/attachments/T-Mobile%20Code-%20of%20Conduct.pdf; Twilio, *Twilio Messaging Policy* (Mar. 14, 2022), https://www.twilio.com/legal/messaging-policy; Aparna Khurjekar, *Let's keep text messaging services free of spam* (July 25, 2019) https://www.verizon.com/about/news/lets-keep-text-messaging-services-free-spam; *see also* 10DLC.org, Carrier Code of Conduct, https://www.10dlc.org/en/verizon-tmobile-att-sprint-carrier-code-of-conduct ("Verizon adopted a code of conduct based on the CTIA guidelines") (last visited Aug. 17, 2022).

[22] CTIA Messaging Security Best Practices, October 2025, https://api.ctia.org/wp-content/uploads/2025/10/Messaging-Security-Best-Practices-_October-2025.pdf

measures include setting limits on SIM card and number activations, monitoring for suspicious sender behavior, and restricting or reporting abusers to prevent further access to the messaging ecosystem.

CTIA Short Code Messaging
CTIA's Short Code Monitoring Handbook describes best practices for using short codes to enable messaging services. All short code programs are encouraged to comply with this basic code of conduct, including: providing consumers the best possible user experience; honoring consumer choices and preventing abuse of messaging platforms; delivering flexible guidelines that communicate compliance values clearly; enabling the short code industry to self-regulate; and facilitating enforcement measures, if necessary, to protect consumers quickly and consistently.

As mentioned above, the CTIA Secure Messaging Initiative provides a resource in the U.S. for traceback of SMS text messages. Some international wireless service providers and all three of the U.S. major wireless providers (AT&T, T-Mobile, and Verizon) have agreed to use the Google Jibe hub. It is unknown whether RCS messages which transit the Google Jibe Hub are included in the traceback support of the CTIA's SMI program or any similar program that may exist internationally.

X. Consumer Tools

MNO SPAM Reporting
Many countries allow wireless customers to report unwanted text messages to their carrier through carrier-supported short codes (e.g., 7726 or "SPAM") or online. More recently, operating system providers have released their own complaint reporting features.

Operating System (OS) Reporting ("Report Junk")
To report complaints on Apple devices, consumers can select "Delete and Report Junk" while Android device users can use the "Report Junk" feature in their messaging app. Messaging campaigns that generate significant numbers of complaints can be at risk for treatment, including blocking. In its latest release, iOS18, Apple added Call and Message Screening options that are user configurable. Both incorporate AI to selectively screen and identify content.[23]

[23]Apple, June 9, 2025, "Apple elevates the iPhone experience with iOS26." Retrieved from https://www.apple.com/newsroom/2025/06/apple-elevates-the-iphone-experience-with-ios-26/

XI. Law Enforcement Tools

Law Enforcement Collaboration

In the U.S., CTIA launched the Secure Messaging Initiative (SMI),[24] an industry-led effort that provides a construct for U.S. MNOs to legally share selected scam / spam messaging information with government agencies. The SMI also includes a cross-carrier and broader industry technical working group which works to identify and mitigate spam sources. Through this partnership, the U.S. wireless industry delivers referral packages to federal and state law enforcement as well as federal enforcement partners at the FCC, Federal Trade Commission, Department of Justice, and the State Anti-Robocall Task Force; enforcement entities can then further investigate to potentially bring charges against bad actors.

A new, industry-led message trace process is also under development in the U.S. to aid law enforcement partners identify the scam / spam message origination path, including the originating messaging provider or platform responsible for transmitting one or more specific messages.

Lawful Interception

The capability for lawful interception of SMS messages is required in many jurisdictions, including the U.S., EU, Russia, China, India, Australia. Depending on the network capabilities and regulatory requirements, interception can occur in SS7 and/or SIP-based signaling environments. However, end-to-end encryption of RCS and OTT messaging can hinder the interception process. For example, OTT messaging by applications such as WhatsApp and Telegram are encrypted end-to-end and lawful surveillance of OTT messaging lack access to encryption keys. Research is ongoing to develop a 3GPP-compliant key escrow mechanism to allow for scoped message decryption.[25] It is not yet known whether the anticipated mechanism will also work to decrypt messages sent with RCS end-to-end encryption.

XII. Challenges to spam and scam mitigation

Unlike OTT and RCS, SMS is a carrier-operated messaging service. SMS messages are routed over the cellular network, and MNOs have implemented network-based filters and processes to help detect and treat spam and unwanted text messages before they reach wireless consumers. However, spam mitigation tools designed for one type of message will not naturally work for all message types, which pose challenges in ongoing efforts to combat messaging spam as consumers messaging shifts from SMS to RCS.

---

[24] CTIA Secure Messaging Initiative, https://www.ctia.org/ctia-secure-messaging-initiatve

[25] SS8 Securing Societies Always, January 6, 2025, "Global Lawful and Local Intelligence Outlook: 2025." Retrieved from https://www.ss8.com/global-lawful-and-location-intelligence-outlook-2025/

Encryption

MNOs have visibility into the message traffic that transit their respective networks. Spam filters or network defenses designed to combat SMS/MMS spam or scam messages may not work on OTT where messaging apps are encrypted between clients. Similar challenges exist for RCS messaging.

Android devices using Google Messages can use end-to-end encryption for RCS messages. Apple iPhones can also support end-to-end encryption (E2EE) when using iMessage. For years, messages exchanged between iPhone and Android users defaulted to SMS/MMS. However, following the rollout of iOS18, GSMA announced that work is underway to enable E2EE on RCS messages between Apple and Android users. As customers upgrade their devices and the Apple iMessage client enables E2EE, most RCS messaging volumes will be encrypted which will present challenges for MNO's capability to filter or block messages. And as more messaging traffic moves from SMS/MMS to RCS, spammers and scammers can be expected to follow suit.

XIII. Recommendations

The messaging ecosystem now spans SMS, MMS, RCS, and an expanding range of OTT options. Consumers use these services interchangeably, but the rules governing them vary significantly. This inconsistent treatment of similar messaging channels - combined with the added complexities of encryption and the limited visibility into services not operated by carriers - has created challenges across the global ecosystem. As a result, stakeholders are finding it increasingly difficult to prevent fraud, maintain accountability, and protect consumers from unwanted or malicious content.

The following recommendations are offered by One Consortium's Messaging Working Group to help protect consumers globally and restore trust in messaging services.

Policy Harmonization

Regulators and policymakers should adopt harmonized policies that apply consistently across SMS, MMS, RCS, and OTT messaging. Messaging abuse routinely shifts from highly regulated channels into less regulated channels when policy diverges. Without a unified approach, consumers are left vulnerable, and enforcement becomes fragmented.

Harmonization should include:

- Uniform consent requirements (opt-in/opt-out/unsubscribe) across channels.
- Equitable enforcement standards for spoofing, impersonation, and malicious link distribution regardless of channel.
- Consistent definitions of spam, fraudulent content, illegal content, and harmful campaigns.

- Clear baseline consumer rights that are not contingent upon how the message is delivered.

Collaboration with GIRAF to develop harmonized recommendations and best practices that national authorities can reference would help provide industry stakeholders (MNOs, OTT platforms, aggregators) with insight into upcoming harmonization trends, enabling proactive adaptation. By leveraging the global memberships of One Consortium and GIRAF, the industry can ensure harmonization efforts are truly international in scope and avoid regional fragmentation.

Global Registry Alignment

To aid in enhancing trust in the messaging space, MNOs globally should work to facilitate greater coordination and alignment of registration standards for brands, campaigns, and sender identities to reduce impersonation, increase trust, and streamline global compliance. This includes, in alignment with GIRAF, harmonization of national registries to protect all consumers from disallowed content and fraudulent messaging.

Harmonization should include:

- Develop a global registry blueprint, in collaboration with GIRAF, that can be used as a reference by national regulators and industry stakeholders. This blueprint will outline common data elements such as brand identity, sender ID, campaign type, and risk indicators.
- Utilize the planned work of One Consortium Working Group 6 (Identity) to provide the foundation of a cryptographically signed portable token which can be used to capture the Brand/Enterprise Identity including elements like brand name, logo, Sender IDs (telephone numbers, short code or alphanumeric), right-to-use, vetting verification, etc.
- Define common risk scoring models and authentication processes for senders, with mechanisms for cross-border verification.
- Implement interoperable APIs, or interfaces, so that registries across jurisdictions can exchange sender identity data and fraud signals in near real time.
- Create shared best practices for registry governance, audit mechanisms, enforcement escalation, and escalation paths for identified bad actors.

Increased Industry Collaboration

Establish structured, ongoing collaboration between messaging ecosystem participants – carriers, OTT providers, registries, KYC teams and providers, and aggregate platforms. GIRAF is a necessary conduit between regulators, industry, and cross-industry collaboration to ensure regulation and policy allows for data and intelligence sharing.

Collaboration Pillars:

- Cross-platform, industry, and cross-industry threat intelligence sharing for SMS, MMS, RCS, OTT, email-to-text, etc.
- Joint abuse mitigation protocols – rapid blocking, suspension, and coordinated takedown.
- Shared detection models and behavior analytics to identify anomalous messaging patterns.
- Unified consumer complaint channels and reporting frameworks regardless of service type.
- Regular collaboration with GIRAF and industry to ensure alignment and harmonization.

Education and Awareness

Implement multi-tiered education and awareness initiatives connecting regulators, industry, and consumers using One Consortium and GIRAF to coordinate global messaging ecosystem literacy.

- Launch a global messaging fraud awareness portal with customized modules for consumers, regulators, and operators.
  - Regulators: Differences between SMS, MMS, RCS and OTT; the impact of encryption on detection; need for harmonized policy and global coordination; etc.
  - Industry: Best practices for compliance, registration, KYC, fraud detection, global coordination, etc.
  - Consumers: How to recognize scams across channels; complaint and reporting mechanisms; etc.
- Host webinars and virtual roundtables that include industry, regulatory, and law enforcement to share evolving threats and mitigation strategies.
- Develop consumer-facing information to raise awareness of brand verification, secure messaging habits, and how to report suspicious content across channels.

Emphasis on Security

Encourage all messaging ecosystem participants to adopt rigorous security frameworks. This will include industry-led regulatory collaboration through One Consortium and GIRAF.

Core Security Areas

- Account Protection & Authentication: MFA, automated inactive account suspension/deactivation, and other measures that secure the accounts and prevent account takeover.
- API & Platform Security: Secure token and Authorization flows, key rotation, comprehensive logging, anomaly detection.
- Infrastructure Hardening: Regular pen testing, secure configuration, monitoring of message routing systems.

- Incident Response & Coordination: Shared reporting channels, escalation frameworks, cross-industry deconfliction for larger threat campaigns.

Encryption Considerations:

- With end-to-end encryption (E2EE) expanding across RCS and OTT, GIRAF and industry must collaborate on privacy-respecting mechanisms to detect patterns of abuse without undermining encryption.
- Develop global alignment on how encrypted platforms interface with registries, tracebacks, and enforcement protocols.

Know Your Customer

Apply unified, harmonized, and global minimum Know Your Customer (KYC) standards. For messaging it should include SMS, RCS, OTT, A2P/Business SMS, P2P, etc. Know Your Customer takes many different viewpoints to also include Know Your Traffic (KYT), Know Your Upstream Provider (KYUP), Know Your Business (KYB), Right-to-Use verification of identity attributes, including Sender IDs, phone numbers, brand names and logos, etc. All should be looked at accordingly to establish minimum standards and best practices.

Weak or inconsistent KYC allows bad actors to impersonate brands, route fraud through under-regulated channels, or migrate from one service type to another. A global baseline closes that doorway.

Harmonized KYC Standard:

- Entity validation via trusted government business registries or identity databases.
- Behavioral risk scoring: history of abuse, migration between channels, flagged behavior.
- Unified brand identity onboarding and maintenance across all platforms.
- Shared violation/disqualification list accessible to carriers, OTT platforms, registries, and regulators.
- Real-time verification checks tied to campaign launches or high-risk messaging types.

GIRAF can define minimum KYC standards and identity validation protocols that regulators worldwide can reference. National registries can integrate KYC data flows into the global registry framework. Aggregators, CSPs, and OTT platforms share onboarding data (within privacy regulation) to reduce duplicate vetting efforts and prevent threat actors from shifting platforms stealthily.

There should also be consideration to expand this for cross-industry collaboration as financial, retail, and others may be looking at the same data and information or have vital insights to share. This, too, will require GIRAF and regulatory involvement to ensure privacy regulations allow this sharing both nationally and globally.

Enhanced Traceback, Threat Intelligence and Data Sharing
Build global, multi-channel traceback standards, intelligence sharing frameworks, and cooperation best practices, with GIRAF providing regulatory coordination and One Consortium providing industry coordination. These are strongly recommended approaches for both voice and messaging services. For more detailed information, please refer to the documentation provided by One Consortium Working Group 3.

- Extend traceback models to cover SMS, MMS, RCS and, where feasible, OTT channels.
- Develop global traceback standards, with GIRAF's guidance, so that scams and illegal calling can be effectively traced and actioned at a global scale.
- Agree on standardized metadata retention policies and support for regulators and law enforcement.
- Create privacy compliant framework to exchange sender ID failures, fraudulent link signatures, behavioral anomalies, and law enforcement data.
- Establish global threat intelligence hubs, industry led and regulator supported, to aggregate and disseminate messaging fraud indicators - cross-platform, cross-border, and cross-industry.

By aligning policy, registries, KYC, security, traceback, collaboration and education under a globally recognized framework – leveraging the GIRAF multilateral forum and One Consortium industry coordination – stakeholders can build a unified, resilient, trusted messaging ecosystem. These recommendations chart a clear path toward preventing abuse, maintaining accountability, and protecting consumers across all messaging channels worldwide.