

Inmarsat, Inc.

Robocall Mitigation Plan

Implemented: February 14, 2023
Last Revised: February 24, 2026

Table of Contents

A.	Robocall Mitigation Plan Introduction.....	1
1.	Company Summary	1
2.	Identification of STIR/SHAKEN Extension Category	2
B.	Robocall Mitigation Plan	4
1.	Economic Components.....	4
2.	Contractual Terms.	5
3.	Know Your Customer Protocols.....	6
4.	Monitoring of Network Traffic.....	7
5.	Handsets.	7
6.	Caller-ID Spoofing.....	7
7.	Traceback Requests.	8
	Exhibit A – Company Information	10
	Exhibit B – Principals.....	11

A. Robocall Mitigation Plan Introduction

Consistent with the rules and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Plan details the policies and practices that Inmarsat, Inc., on behalf of itself and its affiliates ISAT US Inc., Inmarsat Solutions (US) Inc., and Inmarsat Group Holdings Ltd., (collectively, “Inmarsat”)¹ has established to prevent unlawful robocalls from originating on its voice network. In general, this Robocall Mitigation Plan provides information regarding Inmarsat’s:

1. Voice network being a highly improbable platform for illegal robocalls;
2. Contractual terms that mitigate the origination of illegal robocalls;
3. Know your customer protocols;
4. Equipment architecture that mitigates origination of illegal robocalls;
5. Monitoring and investigation of suspicious calling patterns; and
6. Commitment to cooperate in traceback requests.

1. Company Summary

Inmarsat is a leading provider of mobile satellite services, providing data and voice connectivity to end-users worldwide, with 40 years of experience in designing, launching and operating satellite-based networks. Inmarsat’s primary address is 1441 L St NW, Suite 610, Washington D.C. 20005 and is not a foreign voice service provider.

Inmarsat has an in-orbit fleet of owned and operated satellites in geostationary orbit and it provides a comprehensive portfolio of global mobile satellite communications services for customers on the move or in remote areas for use on land, at sea and in the air.

The company was formed in 1979 as an international governmental organization under treaty, with an initial objective to provide communications and safety services to ships at sea. Inmarsat was established with a mandate to operate profitably and to generate returns on the invested capital. In 1999, Inmarsat was privatized and became a private limited company under the laws of England and Wales. In June 2005, Inmarsat completed an initial public offering and listed its ordinary shares on the London Stock Exchange. Inmarsat delisted from the London Stock Exchange when it was

¹ Inmarsat also has a previous business name: Inmarsat PLC. Further, Viasat Inc. acquired Inmarsat in 2023, but each company is filing a separate Robocall Mitigation Plan.

acquired by private equity firms in 2019, and the Inmarsat group was subsequently sold to Viasat, Inc. in 2023.

Inmarsat provides broadband data and voice services, which support safety communications; standard office applications such as email, internet, secure VPN access and video conferencing; and, increasingly with respect to broadband services, more advanced commercial applications. Inmarsat's strategy is to deliver on its purpose of "enabling the connected world" by meeting the remote and mobile connectivity needs of its customers, giving them what they need to connect, reliably, securely, and globally.

Inmarsat's global sales and marketing activities are operated through four customer-facing business units:

- Maritime, focusing on worldwide commercial maritime services;
- Government, focusing on civil and military government services, including those specific to US government customers;
- Aviation, focusing on commercial, business and general aviation services; and
- Enterprise, focusing on worldwide energy, industry, media, carriers and M2M services.

2. Identification of STIR/SHAKEN Extension Category

The FCC's regulations define a provider of "voice service" as an entity that is interconnected with the public switched telephone network ("PSTN") and that furnishes voice communications to an end user using resources from the North American Numbering Plan ("NANP") or any successor to the North American Numbering Plan.² Further, a "small voice service provider" is defined as a "provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates)."³ The FCC has granted an indefinite STIR/SHAKEN implementation extension on the basis of undue hardship to small voice service providers that originate calls via satellite using NANP numbers in the caller-ID.⁴

² 47 C.F.R. §64.6300(g).

³ *Id.* § 64.6304(a)(2).

⁴ See *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18, ¶¶ 79-82 (2023) ("Call Authentication Sixth Report and Order"); The Commission has also concluded that satellite providers originating calls using non-NAP numbers are not "voice service providers" within the meaning of the TRACED Act. The FCC also concluded that where satellite providers "utilize NANP resources for call forwarding to non-NANP numbers," such calls also fall outside the scope of the TRACED Act. *Id.* ¶ 78. Finally, the FCC

Inmarsat furnishes such voice services to end users using resources from the NANP for fewer than 100,000 voice subscriber lines. Inmarsat therefore qualifies for an indefinite STIR/SHAKEN implementation extension.⁵

concluded that satellite providers subject to the extension must still submit a certification to the Robocall Mitigation Database. *Id.* ¶ 82.

⁵ Inmarsat understands that the Commission must reevaluate the extension annually and will update its Robocall Mitigation Plan as needed in response to any changes to FCC regulations. See 47 C.F.R. § 64.6304(f). On September 28, 2023, the Commission released a Public Notice referencing its previous findings that “because satellite service costs make the high-volume calling necessary for robocallers uneconomical,” there was “little evidence that satellite providers or their users are responsible for illegal robocalls,” and the number of satellite subscribers using NANP resources was “miniscule.” See *Wireline Competition Bureau Seeks Comment on Previously Granted STIR/SHAKEN Implementation Extensions Pursuant to Section 64.6304(f) of the Commission’s Rules*, WC Docket No. 17-97, Public Notice, DA 23-910 (rel. Sept. 28, 2023) (internal quotes removed). The Commission has not taken further action since the Public Notice to change the status of the indefinite STIR/SHAKEN implementation extension for small satellite providers originating calls using NANP numbers.

B. Robocall Mitigation Plan

1. Economic Components.

Illegal robocallers' use of any satellite service – including Inmarsat's – to engage in high-volume calling campaigns is economically inhospitable. Congress, the FCC and the Federal Trade Commission have all emphasized that illegal robocallers rely on voice service platforms that make it cheap and easy to originate millions of illegal robocalls on a daily basis.⁶ The FCC recently observed in its report to Congress under the TRACED Act that “[d]eclining call costs over the past few decades have eliminated financial barriers to entry for would-be robocallers.”⁷ It further noted that domestic call rates were 25 to 50 cents per minute fifty years ago, whereas wholesale rates today to U.S. mobile phones cost less than a penny per minute.⁸ The FCC concluded that this has created a “cottage industry” for certain voice providers to specialize in so-called “dialer traffic.” Such dialer traffic is uniformly characterized by low cost, high-volume, and short duration calls.⁹ Such characteristics are absent from satellite platforms providing voice service to end users.

This dynamic creates an environment whereby Inmarsat's voice service offering is economically inhospitable to the illegal robocallers that generate such dialer traffic. Publicly available information demonstrates that satellite voice services generally charge per minute rates that exceed the thresholds necessary to originate illegal robocall traffic.¹⁰ One industry expert on illegal robocalls noted that low-cost pricing plans – such as those that are less than a penny per minute – create an environment whereby a VoIP provider originating one hundred million robocalls in a single month could expect to net approximately \$50,000 to \$100,000 in profit.¹¹

⁶ See, e.g., FCC, *The FCC's Push to Combat Robocalls & Spoofing*, <https://www.fcc.gov/spoofed-robocalls> (last visited Feb. 13, 2024) (noting that “advancements in technology make it cheap and easy to make massive numbers of robocalls”); see also Hearing, U.S. Senate Committee on Commerce, Science, & Transportation, Statement of U.S. Sen. John Thune (R-SD) (April 18, 2018), <https://www.commerce.senate.gov/2018/4/abusive-robocalls-and-how-we-can-stop-them#> (visited June 17, 2021) (stating that “as more phone systems move from copper wires to the internet, it has become easier and cheaper for bad actors to make illegal robocalls from anywhere in the world.”).

⁷ See FCC Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information (December 27, 2023), at 15 (“FCC Report”).

⁸ *Id.*

⁹ *Id.*

¹⁰ See Satellite Phone Store, *Inmarsat IsatPhone 2*, <https://www.satellitephonestore.com/isatphone-pro-service> (last visited Feb. 13, 2024).

¹¹ See Hearing, *Combating Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors*, United States Senate, Special

In stark contrast, any illegal robocaller utilizing a satellite voice platform such as Inmarsat's to originate dialer traffic would incur prohibitive expenses. Even assuming that the satellite provider charges in 20 second increments, the illegal robocaller would incur expenses alone of approximately \$22 to \$33 million for the same volume of calls. Consistent with the FCC's requirements for robocall mitigation plans, these cost dynamics alone can reasonably be expected to significantly mitigate any risk that illegal robocalls will originate from the Inmarsat network.

2. Contractual Terms.

Inmarsat has also implemented contractual terms and policies that will mitigate the origination of illegal robocall traffic from its network. These terms and policies are enshrined in Inmarsat's publicly available terms and conditions governing use of its satellite voice service ("Inmarsat Terms and Conditions").¹² In particular, end users obtaining services from Inmarsat are subject to contractual terms that can reasonably be expected to significantly reduce the origination of illegal robocalls.¹³ The Inmarsat Terms and Conditions include the following contractual provisions:

- ***Contractual Obligations to Comply with All Federal and State Laws.*** The Inmarsat Terms and Conditions also affirmatively obligate end users to comply with all applicable laws and regulations and requirements of any governmental body.¹⁴ In addition to this affirmative obligation, end users are expressly prohibited from using the services, or knowingly permitting them to be used: (i) for any unlawful, illegal, immoral, indecent, abusive, defamatory or fraudulent purpose; or (ii) in a way that interferes with Inmarsat's ability to provide services to its other customers.¹⁵
- ***Suspension or Deactivation of Voice Services Under Certain Circumstances.*** The Inmarsat Terms and Conditions permit it to bar or suspend any satellite terminals or subscriber identity module ("SIM") cards in any country or countries, if Inmarsat: 1) has reason to believe that the end user is abusing the service or using it fraudulently or unlawfully or is failing to

Committee on Aging, July 17, 2019, Testimony of David Frankel, Telecommunications Consultant, p. 3.

¹² See Inmarsat, *Terms and Conditions*, <https://www.inmarsat.com/legal/inmarsat-customer-terms-conditions/> (last updated April, 2025) ("*Inmarsat Terms and Conditions*"). The Inmarsat Terms and Conditions apply to its direct end customers; however, Inmarsat imposes these same contractual obligations on its wholesale partners through Inmarsat's Master Services Agreement.

¹³ *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, ¶ 78 (October 1, 2020).

¹⁴ *Inmarsat Terms and Conditions*, Section 3.4.

¹⁵ *Id.*

provide complete and accurate information;¹⁶ and/or 2) has reason to believe that the satellite terminal or its use or operation may adversely affect the Inmarsat network or Inmarsat's ability to provide its service.¹⁷ In addition, although such termination can occur with prior notice to the end user, Inmarsat may bar or suspend such service without such prior notice under certain circumstances.¹⁸

3. Know Your Customer Protocols.

Consistent with Principle #5 of the Attorneys General anti-robocall principles, Inmarsat also follows appropriate Know Your Customer ("KYC") protocols when onboarding new commercial customers.¹⁹ As part of its KYC protocols, Inmarsat requires any commercial customer to provide sufficient information to ensure its legitimacy. Among other things, Inmarsat requires its commercial customers to provide the full legal name of the company (and its parent company if applicable), the physical address of its operations, its value added tax identification number,²⁰ and the number of years the company has been in business. Companies must also provide contact information (to include valid email and telephone numbers) for their Chief Financial Officer, and billing and operational contacts. As part of its KYC protocols, Inmarsat also requires applicants to provide two separate industry credit references and the identities of any current or previous satellite communications providers. Applicants must also provide a copy of its current audited financials, along with the name and contact information for its external auditor.

All applicants must certify to the accuracy of the information provided to Inmarsat. As part of the KYC protocols, applicants must also expressly authorize Inmarsat to: 1) obtain from the identified references listed in the form any information requested by Inmarsat, and 2) obtain credit reports and other documentation from third parties. All customer must agree that Inmarsat's acceptance of any application is contingent upon Inmarsat's satisfaction with the credit review, and that Inmarsat may suspend or terminate the supply of services and/or equipment if it is not satisfied with the customer's credit.

¹⁶ *Id.*, Section 8.1.1.

¹⁷ *Id.*, Section 8.1.4.

¹⁸ *Id.*, Section 8.2.

¹⁹ See, Inmarsat, *Customer Application Form*, https://www.inmarsat.com/content/dam/us-site/legal/documents/inmarsat/Inmarsat_Customer_Account_Request_Form_Effective_November_2024.zip (last updated November, 2024).

²⁰ A value added tax identification number ("VAT") identification number is an identifier used in many countries, including the countries of the European Union ("EU"), for value added tax purposes. In the EU, a VAT identification number can be verified online at the EU's official VIES website. See, European Commission, *VIES VAT Number Validation*, https://ec.europa.eu/taxation_customs/vies/ (last visited Feb. 13, 2024).

Finally, Inmarsat operates with two Tier 1 upstream providers to facilitate all voice traffic originating or terminating to the Inmarsat network. The relationships between Inmarsat and its upstream providers involve strong contractual terms.

4. Monitoring of Network Traffic.

Consistent with Principle #3 of the Attorneys General anti-robocall principles,²¹ Inmarsat's Robocall Mitigation Plan also sets out policies and procedures to govern the analysis and monitoring of its outbound network traffic. Inmarsat maintains and operates a Network Operations Center in London, England ("London NOC"), and a Network Control Center located in Burum in the Netherlands ("Burum NCC"). Collectively, the London NOC and the Burum NCC monitor the continued and reliable operation of the Inmarsat networks on a 24/7 basis. To ensure continuous monitoring of Inmarsat's network, there is always at least one staff member on duty at each of these control centers. Inmarsat continuously directs and manages traffic routing through its network, continuously monitoring for and reporting any anomalous voice traffic. NOC/NCC engineers supervise network operations, coordinate network activities, and take corrective actions as necessary to meet the network availability and service quality objectives, including daily traffic analysis, incident classification and reporting, and investigations into suspicious network activity.

5. Handsets.

In addition to the economic considerations to originate a call on the Inmarsat network discussed in Section (A)(1), the handsets themselves present an additional limitation on the practicality of utilizing the Inmarsat network to conduct high volume calling campaigns. Inmarsat handsets are designed to provide robust, reliable, always-on call connectivity. These devices are not designed to support the origination of high-volume dialer traffic regularly employed by illegal robocallers. Additionally, only Inmarsat authorized and subscribed devices can access the Inmarsat network to originate voice traffic on its network. The Inmarsat network is not configured to enable end users to operate unauthorized equipment over the Inmarsat network, such as an autodialer.

6. Caller-ID Spoofing.

The risk of illegal caller ID spoofing is substantially mitigated as Inmarsat customers generally cannot change or spoof their assigned caller ID information when calling from an Inmarsat device.²² Inmarsat furnishes voice services to end users using

²¹ State Attorneys General, *Anti-Robocall Principles*, at 2, <https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf> (last visited Feb. 13, 2024).

²² *Call Authentication Trust Anchor*, WC Docket No. 17-97, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, ¶ 4 (Mar. 31, 2020)

resources from the NANP for fewer than 100,000 voice subscriber lines. In certain instances, these NANP numbers are only used to *forward* incoming calls to the telephone number actually assigned to the Inmarsat device—a twelve-digit international phone number, starting with country code 870. Outgoing calls in these calling scenarios will display the unique non-NANP telephone number assigned to the end user. A very limited number of Inmarsat end users are allocated NANP resources to both originate and receive voice traffic, and in those instances the NANP number will be presented as the outbound caller-ID. However, the anti-spoofing capabilities inherent to most services furnished by Inmarsat to end users, limits their utility for use by illegal robocallers.

Inmarsat also complies with FCC requirements to maintain and enforce a Do Not Originate (DNO) list designed to block calls from numbers that should not place outbound calls.

7. Traceback Requests.

To the best of its knowledge, Inmarsat has never received a traceback request and the FCC’s recent report to Congress under the TRACED Act reflects that Inmarsat did not receive a traceback request in 2023.²³ Additionally, Inmarsat has not been the subject of a formal Commission law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description within the past 2 years. However, Inmarsat takes the issue of unwanted and illegal robocalls seriously and is committed to ensuring that its network is not utilized for the origination of such calls. Inmarsat will therefore respond promptly to all traceback requests from the Commission, the Traceback Consortium, and law enforcement agencies, consistent with the FCC’s rules and regulations within 24 hours.

In furtherance of this policy, Inmarsat provides the following information for its designated individual responsible for responding to traceback inquiries from the FCC, the Traceback Consortium, and law enforcement agencies. This information, which includes the name and contact information, is as follows:

Contact Name: Donna Bethea Murphy
Contact Title: Senior Vice President Global Regulatory
Contact Address: 901 K Street NW, Suite 400
Contact City: Washington, DC

(recognizing that “the ability to use spoofing to mask the true identity of an incoming call...ha[s] turned to this technology [into] a quick and cheap way to defraud targets and avoid being discovered.”).

²³ See, *FCC Report*, Appendix A (listing participating and non-participating voice providers in tracebacks conducted by the Traceback Consortium in 2020. Inmarsat is not identified as ever receiving such a request.).

Contact State and Zip Code: 20001
Contact Telephone Number: (202) 383-5050
Contact Email: traceback@inmarsat.com

Exhibit A – Company Information

<u>DBA/Affiliate Name</u>	<u>FRN</u>	<u>OCN</u>
Inmarsat Inc. ²⁴	0008262784	N/A

²⁴ See Viasat, Inc., Annual Report (Form 10-K) available at <https://investors.viasat.com/financial-information/sec-filings>

Exhibit B – Principals

The principals of Inmarsat, which has been acquired by Viasat Inc., are included within the Viasat 10K, which may be found at the following address:

<https://investors.viasat.com/financial-information/sec-filings>