



MOBILE MESSAGING FRAUD PREVENTION MARKET 2025-2030

Competitor Leaderboard

Prepared for Tata Communications



Why Read This Report

This section provides an overview of the product offerings of leading mobile messaging fraud prevention vendors. This does not consist of an exhaustive list of messaging fraud prevention vendors operating in this market, rather a selection of 21 fraud prevention vendors that Juniper Research judges to be leading the market, due to a range of factors discussed below.

Mobile messaging fraud prevention is a fast-paced market, with messaging fraud evolving significantly over the past couple of years. Messaging fraud prevention vendors therefore need to keep up with trends in messaging fraud; ensuring that they are blocking unusual activity through monitoring and classifying application-to-person (A2P) SMS traffic. Leading vendors will be those who offer the fundamentals of fraud prevention, alongside value-added solutions to maximise enterprises' defence against messaging fraud.

Juniper Research is a Europe-based provider of business intelligence. We specialise in providing high-quality data and fully researched analysis to manufacturers, financiers, developers, and service/content providers across the communications sector. Juniper Research is fully independent, and able to provide unbiased and reliable assessments of markets, technologies, and industry players. Our team is drawn from experienced senior managers with proven track records in each of their specialist fields.

Key Mobile Messaging Fraud Prevention Market Takeaways

Fraud Over SMS Will Continue to Decline

The fundamental takeaway from this report is that mobile messaging fraud over SMS will continue declining in 2025 through 2030, with enterprises losses to artificially inflated traffic (AIT) having peaked in 2023. This is driven by greater awareness and education surrounding messaging fraud on both the MNO and enterprise levels, due to the high levels of AIT seen in the last few years. Furthermore, A2P SMS is also in decline; owing to alternative authentication methods, such as passkeys and biometrics, and because of a rise in over-the-top (OTT) and RCS Business Messaging (RBM).

The increasing use of OTT and RBM does mean that fraudulent players will migrate their efforts to these channels. This will not necessarily be in the form of AIT, rather techniques such as phishing and account takeover (ATO) will be prominent due to AI making attacks significantly more personalised.

So that AIT does not simply migrate to RBM and OTT messaging, the price of both these channels will be critical. The incentive for bad actors to partake in fraudulent activity is the potential financial return, so if the price of RBM and OTT messaging remains low, there will be little incentive for fraudulent players to migrate AIT to these channels.

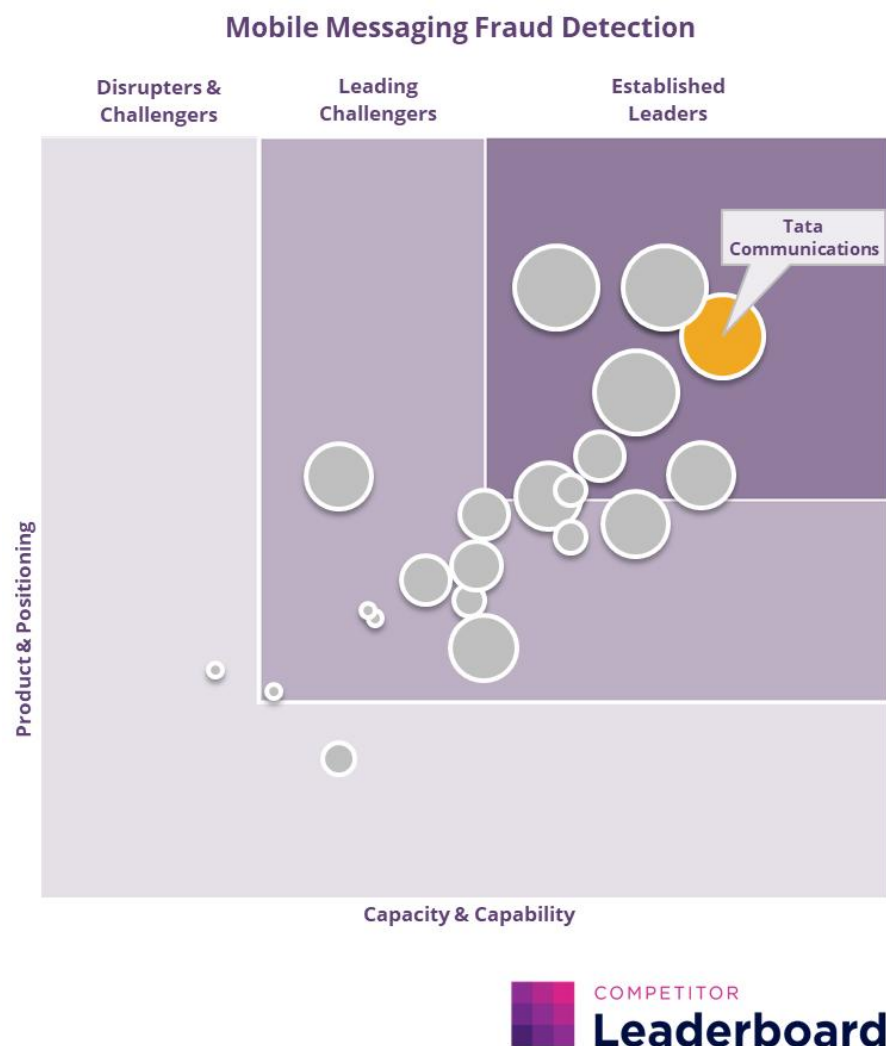
North America and Far East & China Best Equipped to Combat SMS Fraud

Juniper Research predicts that North America and Far East & China will be best equipped to combat mobile messaging fraud, with the greatest decline in the cost of AIT to enterprises occurring in these regions. These regions both had particularly high levels of AIT traffic and enterprise losses resulting from AIT, which put increased pressure on mobile network operators (MNOs) and enterprises to implement solutions to combat the fraud. MNOs in these regions tend to be at the forefront of technological innovation due to the size and scale of the operations that they run. The combination of innovative MNOs and high pressure from enterprises has led to a significant decline in AIT, as well as other types of SMS fraud in these regions.

Furthermore, these regions are set to experience high rates of declining A2P SMS traffic. With lower A2P SMS traffic, SMS fraud will be easier to detect as there will be less traffic to monitor – making it easier to filter messages and detect anomalies such as unusual spikes in traffic.



Figure 1: Juniper Research Competitor Leaderboard: Mobile Messaging Fraud Prevention



Source: Juniper Research

TATA COMMUNICATIONS

Juniper Research has ranked Tata Communications as an Established Leader in Mobile Messaging Fraud Prevention, as scored in the Juniper Research Competitor Leaderboard.

Tata Communications scored highly on the strength and coverage of its messaging fraud prevention platform and solutions; its extent of innovation, and the extensive experience it has in the fraud prevention market.

Tata Communications scored well across all the categories; attaining the highest score possible in seven out of 11 categories. The company's use of application programming interfaces (APIs) in fraud prevention continues to be a standout feature in its approach to Artificially Inflated Traffic (AIT) mitigation. Tata Communications will integrate Intellectual Property (IP) address-based APIs to further enhance the depth of insights available to enterprises and operators. This will allow for more granular detection of suspicious traffic patterns and geographic anomalies; strengthening fraud detection capabilities

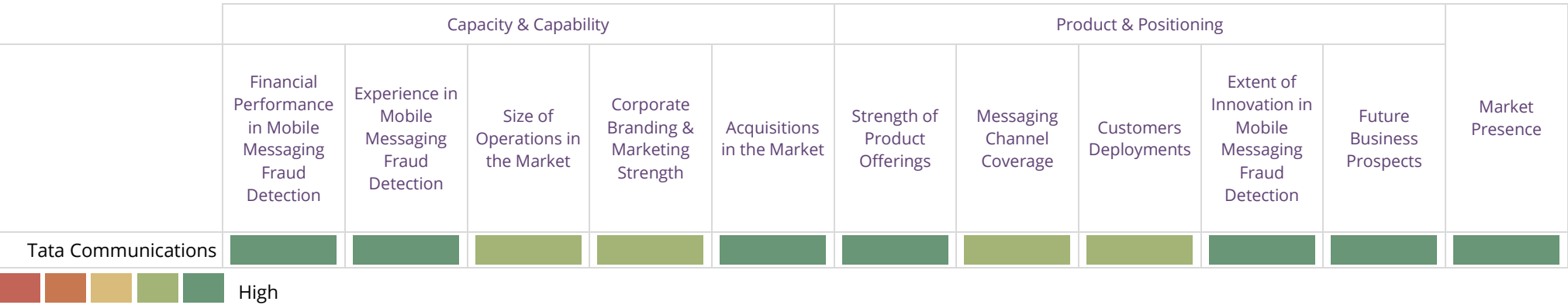
Juniper Research believes that Tata Communications' automation of dashboards and monitoring tools play a vital role in identifying and responding to AIT threats. As the speed and complexity of AIT attacks increases, we expect enterprises to be attracted to the strength of Tata Communications' solutions, as well as its extensive experience in the fraud prevention market.



1.1.1 Tata Communications



Table 2: Juniper Research Competitor Leaderboard Heatmap: Mobile Messaging Fraud Prevention



Source: Juniper Research

i. Corporate Information

Founded in 1972, Tata Communications is part of the Tata Group; a leading CommTech player that powers its customers’ hyperconnected ecosystems through its digital fabric. It brings together tools, platforms, skills, and expertise to help its customers build agile infrastructure, enable compelling employee and customer experiences, deploy connected solutions, and build cyber resilience.

Tata Communications carries around 30% of the world’s Internet routes and connects businesses to 80% of the world’s cloud giants, and four out of five mobile subscribers. The enterprise owns and operates the Tata Global Network; a submarine cable network that provides connectivity to countries around the world, with 300 PoPs across the globe. Moreover, Tata Communications is part of the Asia Direct Cable (ADC) Consortium; an organisation which is building a high-performance submarine cable connecting China, Japan, the Philippines, Singapore, Thailand, and Vietnam.

Tata Communications’ leadership team consists of Amur Swaminathan Lakshminarayanan (Managing Director and CEO), Bhaskar Gorti (EVP, Cloud and Cybersecurity Services), Genius Wong (EVP, Core and Next-Gen Connectivity Services, and CTO), Kabir Ahmed Shakir (CFO), Natarajan Sivasamban (EVP and Head of Operations), Sumeet Walia (EVP, and Chief Sales and Marketing Officer), Tri Pham (EVP, Corporate Strategy Head), and Troy Reynolds (Chief Legal and Compliance Officer).



Table 3: Tata Communications' FY 2024-25 & FY 2023-24 Revenue and Profit, Adjusted to USD

	FY 2024-25	FY 2023-24
Gross Revenue	\$2.70 billion	\$2.51 billion
Net Profit (PAT)	\$189.78 million	\$116.08 million

Source: Tata Communications

In October 2023, Tata Communications completed the acquisition of Kaleyra for \$100 million. Through this acquisition, Tata Communications has leveraged Kaleyra's expertise in technology, engineering, and research and development, including its CPaaS solutions. Tata Communications also added new points of presence in the US, in Latin America, in the UK, Italy, the Middle East, and Asia Pacific.

Tata Communications' Customer Interaction Suite is part of their Interaction Fabric, which enables contextual, seamless, and personalised customer interactions for enterprises.

ii. Geographical Spread

Within North America, Tata Communications has four offices in the US and one in Montreal, Canada.

In Europe, the company has offices in Germany, the UK, Spain, Russia, France, Netherlands, Norway, and Poland. It also has five offices in India, including the company's Mumbai headquarters.

In Asia Pacific, Tata Communications operates out of Hong Kong, Malaysia, Singapore, and Australia. It also has offices in Dubai and Abu Dhabi in the UAE, and Sri Lanka.

Tata Communications also has a vast system of networks which provide coverage across the Americas, Europe, the Middle East and Africa, Asia Pacific, as well as India and neighbouring countries; enabling it to provide services around the world.

iii. Key Clients & Strategic Partnerships

Tata Communications' customer portfolio spans a variety of industries including automotive, financial services, construction, consulting, eCommerce, education, energy, finance, government, healthcare, holdings, utilities, IT/ITES, legal, manufacturing, media and entertainment, pharmaceutical, real estate, retail, services, sports, and telecommunications.

An example of one of Tata Communications' customers is Isansys; a digital healthcare provider. Isansys leverages WhatsApp's API with Tata Communications' Kaleyra to help notify healthcare professionals of patients' early warning signs in real-time.

Tata Communications has also previously formed strategic partnerships with AWS, Cisco, Google Cloud, Microsoft, MotoGP™, SailGP, and Singapore Airlines.

- In February 2024, Tata Communications announced a partnership with Microsoft to provide flexibility in collaboration and connectivity on Microsoft Teams for enterprises in India. Its GlobalRapid platform will enable Indian enterprise users and multinationals with local presence to make and receive PSTN voice calls on any Teams device, anywhere across the globe, using the Operator Connect platform.
- Tata Communications has also launched its AI cloud infrastructure powered by NVIDIA's graphics processing units (GPUs). The first phase, launched at the end of 2024, resulted in one of India's largest cloud-based supercomputers utilising NVIDIA Hopper GPUs. Through this collaboration, Tata Communications strengthened its position as a key enabler of AI-driven solutions across sectors such as manufacturing, healthcare, retail, and banking and financial services.

iv. High-level View of Offerings

Tata Communications offers a suite of fraud prevention solutions that enable enterprises and MNOs to secure their messaging services. The company takes a proactive approach to detecting, mitigating, and blocking fraudulent traffic – such as spam, grey routes, and smishing – before it reaches the end user or results in revenue loss. Its modular and cloud-based solutions integrate easily into existing telecom environments; helping operators and enterprises to monetise traffic and protect customer trust.



As part of its broader fraud protection portfolio, Tata Communications offers Fraud Prevention-as-a-Service (FPaaS), SMS and messaging firewalls, and real-time analytics solutions. These services are tailored for both CPaaS and MNO players and are designed to scale with growing messaging traffic volumes.

SMS Firewall

- Hosted SMS Firewall – filters and blocks illegitimate A2P traffic, smishing, and spam messages at the network level. It also prevents grey route abuse and supports revenue recovery by enforcing message routing policies.
- Signalling Security – protects SS7, diameter, SIP signalling protocols to prevent network intrusion, message tampering, and SIM-based attacks. Enables real-time anomaly detection and automated blocking.
- iFMS (Intelligent Fraud Management System) – monitors both inbound and outbound messaging traffic to detect unusual or suspicious patterns. For outbound traffic, it triggers alerts that are reviewed and validated by a 24/7 Fraud Prevention Team. For inbound traffic, it analyses historical usage trends to detect surges or anomalies that may indicate fraud.
- STMS (Subscriber Traffic Management System) – tracks subscriber-level traffic in near real-time to identify potential abuse. The system establishes thresholds and triggers alerts or blocks traffic when anomalies or fraud indicators are detected.
- Real-time Fraud Analytics & APIs – provides dashboards and custom alerts for fraud incidents. Telcos and enterprises can integrate these tools into their OSS/BSS environments using APIs for automated rule enforcement.
- Traffic Pattern Monitoring – uses AI and ML to detect irregular behaviour and message abuse – flagging potential ATO, artificial inflation, or OTP abuse.

a) Messaging Protection (via Kaleyra CPaaS)

Alongside FPaaS, Tata Communications integrates fraud protection directly into its CPaaS platform, Kaleyra. Fraud-related services include:

- Secure OTP Delivery – ensures OTPs are sent via trusted channels and blocked when delivery attempts are made via grey routes or fraudulent SIMs.
- Sender ID Verification & Routing Control – prevents SMS spoofing and unauthorised brand impersonation.
- Carrier-Grade Messaging Integrity – monitors inbound and outbound message flows for irregularities, including click-through spam or phishing attempts.



1.1.2 Juniper Research Leaderboard Methodology

Juniper Research provides details about 21 mobile messaging fraud prevention solution providers. To qualify for the leaderboard, companies must be involved in the direct provision of mobile messaging fraud prevention solutions. The companies included here have developed specific expertise in the space, although some embarked on the route earlier than others and, therefore, have wider customer bases or geographical reach. Additionally, it must be noted that many service providers here have developed mobile messaging fraud prevention solutions alongside other services that comprise a higher proportion of a company's revenue.

This research covers a significant number of vendors; however, we cannot guarantee that this list is exhaustive. Juniper Research's approach is to use a standard template to summarise the capability of players offering mobile messaging fraud prevention services. This template concludes with our view of the key strengths and strategic development opportunities for each vendor.

We also provide our view of vendor positioning in the mobile messaging fraud prevention market using our Juniper Research Leaderboard technique. This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor's capability and capacity, in addition to its product and position in the market. The resulting leaderboard exhibits our view of relative vendor positioning.

1.1.3 Limitations & Interpretations

Our assessment is based on a combination of quantitative measures, where they are available, (such as revenue and numbers of employees), that indicate relative strength, and also on qualitative judgement, based on available market and vendor information as published. In addition, we have added our in-house knowledge from meetings and interviews with a range of industry players. We have also used publicly available information to arrive at a board, indicative positioning of vendors in this market, on a 'best effort' basis.

However, we would also caution that our analysis is almost by nature based on incomplete information and, therefore, with some elements of this analysis we have

had to be more judgemental than others. For example, with some vendors, less-detailed financial information is typically available if they are not publicly listed companies. This is particularly the case when assessing early-stage companies, where a degree of secrecy may be advantageous to avoid other companies replicating elements of the business model or strategy.

We also remind readers that the list of vendors considered is not exhaustive across the entire market but, rather, selective. Juniper Research endeavours to provide accurate information. While information or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy, the analysis is presented on a 'best effort' basis.

The Leaderboard compares the positioning of platform providers based on Juniper Research's scoring of each company against the above criteria that Juniper Research has defined. The Leaderboard is designed to compare how the vendors position themselves in the market based on these criteria. Relative placement in one particular unit of the Leaderboard does not imply that any one vendor is necessarily better placed than others. For example, one vendor's objectives will be different from the next and the vendor may be very successfully fulfilling them without being placed in the top right box of the Leaderboard, which is the traditional location for the leading players.

Therefore, for avoidance of doubt in interpreting the Leaderboard, we are not suggesting that any single cell in the Leaderboard implies in any way that a group of vendors is more advantageously positioned than another group, just differently positioned. We additionally would draw the reader's attention to the fact that vendors are listed alphabetically in a unit of the Leaderboard and not ranked in any way in the cell of the Leaderboard.

The Leaderboard is also valid at a specific point in time, September 2025. It does not indicate how we expect positioning to change in future, or indeed in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis; it is merely intended as an analytical summary by Juniper Research as an independent third party.



Table 4: Juniper Research Competitor Leaderboard Scoring Criteria: Mobile Messaging Fraud Prevention Vendors

Category	Scoring Criteria	Relevant Information
Capability & Capacity	Financial Performance in Mobile Messaging Fraud Detection	This criterion relates to the financial revenue from mobile messaging fraud detection and mitigation solutions only, relating only to the previous 12 months.
	Experience in Mobile Messaging Fraud Detection	Here, Juniper Research assesses the experience each company has in the provision of messaging fraud detection and mitigation solutions. It takes into consideration both the length of time in the market, as well as the accomplishments during that time.
	Size of Operations in the Market	This score includes the amount of traffic that each messaging fraud detection and mitigation solution assesses. It takes into consideration the traffic over the last 12 months, over messaging channels including SMS, RCS, and OTT business messaging apps.
	Corporate Branding & Marketing Strength	For this criterion, Juniper Research evaluates the marketing and branding strength of each company within the messaging fraud detection and mitigation market.
	Levels of Investment in the Market	Here, we assess both the levels of investment into the company from external sources, as well as the investment from the company into other sources, including acquisitions that can improve the provision of messaging fraud detection and mitigation solutions.
Product & Positioning	Strength of Product Offerings	Juniper Research evaluates the strength of each product offered by the company; considering the fraud tactics that it can measure and the sources of information that are ingested by the platform.
	Messaging Channel Coverage	We assess the number of messaging channels that can be monitored by the messaging fraud detection and mitigation solutions.
	Customers' Deployments	Here, we look at the number of customer deployments for messaging fraud detection and mitigation solutions. These deployments must be commercial, and we do not count trials.
	Extent of Innovation in Mobile Messaging Fraud Detection	Analysts' opinions on the extent of innovation of products over the last 12 months. High scores here indicate that the company is investing and developing in products that Juniper Research believe will disrupt the market.
	Future Business Prospects	Analysts' opinions on each company's degree of future success over the next five years. High scores here indicate that Juniper Research believes that the company will improve its standing over the next two years.
Market Presence	Market Presence	Here we look at various factors, including the number of countries that the company operates in, the global market share in the mobile messaging fraud detection space, and the number of clients in the space.

Source: Juniper Research



About Tata Communications



Tata Communications is a leading digital ecosystem provider that powers today's fast-growing digital economy. The company enables the digital transformation of enterprises globally, including 300 of the Fortune 500; unlocking opportunities for businesses by enabling borderless growth, boosting product innovation and customer experience, improving productivity and efficiency, building agility, and managing risk.

With its solutions-orientated approach, proven managed service capabilities and cutting-edge infrastructure, Tata Communications drives the next level of intelligence with its cloud, mobility, Internet of Things, collaboration, security, and network services.

Tata Communications is part of the rich heritage of the Internet in India. Over the last 25 years, its enterprise-enabled services have been essential to the adoption of digital services in the country. From utility to transformation, connectivity is an essential fabric of sustenance for the economy.

For more information about Tata Communications, please visit:

<https://www.tatacommunications.com/>

About Juniper Research



Juniper Research was founded in 2001 by the industry consultant Tony Crabtree, in the midst of the telecoms and dot-com crash. The business was fully incorporated in February 2002 and has since grown to become one of the leading analyst firms in the mobile and digital tech sector.

Juniper Research specialises in identifying and appraising new high growth market sectors within the digital ecosystem. Market sizing and forecasting are the cornerstones of our offering, together with competitive analysis, strategic assessment and business modelling.

We endeavour to provide independent and impartial analysis of both current and emerging opportunities via a team of dedicated specialists - all knowledgeable, experienced and experts in their field.

Our clients range from mobile operators through to content providers, vendors and financial institutions. Juniper Research's client base spans the globe, with the majority of our clients based in North America, Western Europe and the Far East.

For more information about Juniper Research, please visit:

<https://www.juniperresearch.com/home>