IQ | think teal™

SPAM PROTECTION

A Think Teal Insights Paper

The Digital Journey: Weaving a New Future for India

Today, India is in the golden era of digital leaps. India's expanding digital infrastructure is transforming individuals and businesses alike. The penetration of smartphones, improved Internet access, and telecom infrastructure are redefining how connectivity and communication processes are carried out. Businesses are evolving and adopting new technologies to enhance their efficiency and keep pace with changing customer expectations.

Banking is one such industry in India that is witnessing a digital revolution. A growing tech-savvy customer base is driving banks in India to explore new possibilities using cutting-edge technologies. Additionally, government initiatives aimed at financial inclusion are further driving banks towards digitization. However, alongside these advancements, banks also face new challenges such as increasing digital frauds. Simplifying customers' banking experience and addressing the security complexities will be a balancing act that banks in India will continue to pursue.

Factors Influencing Banking Growth in India

With a vision to become a developed country by 2047, India is committed to integrating all citizens into a formal financial ecosystem, and banks are playing a critical role in this. India has emerged as a global leader in the digital payments space. Factors like banking reforms, growing use of IT infrastructure in banks, high penetration of smartphones, and improving Internet infrastructure have all contributed to this achievement.

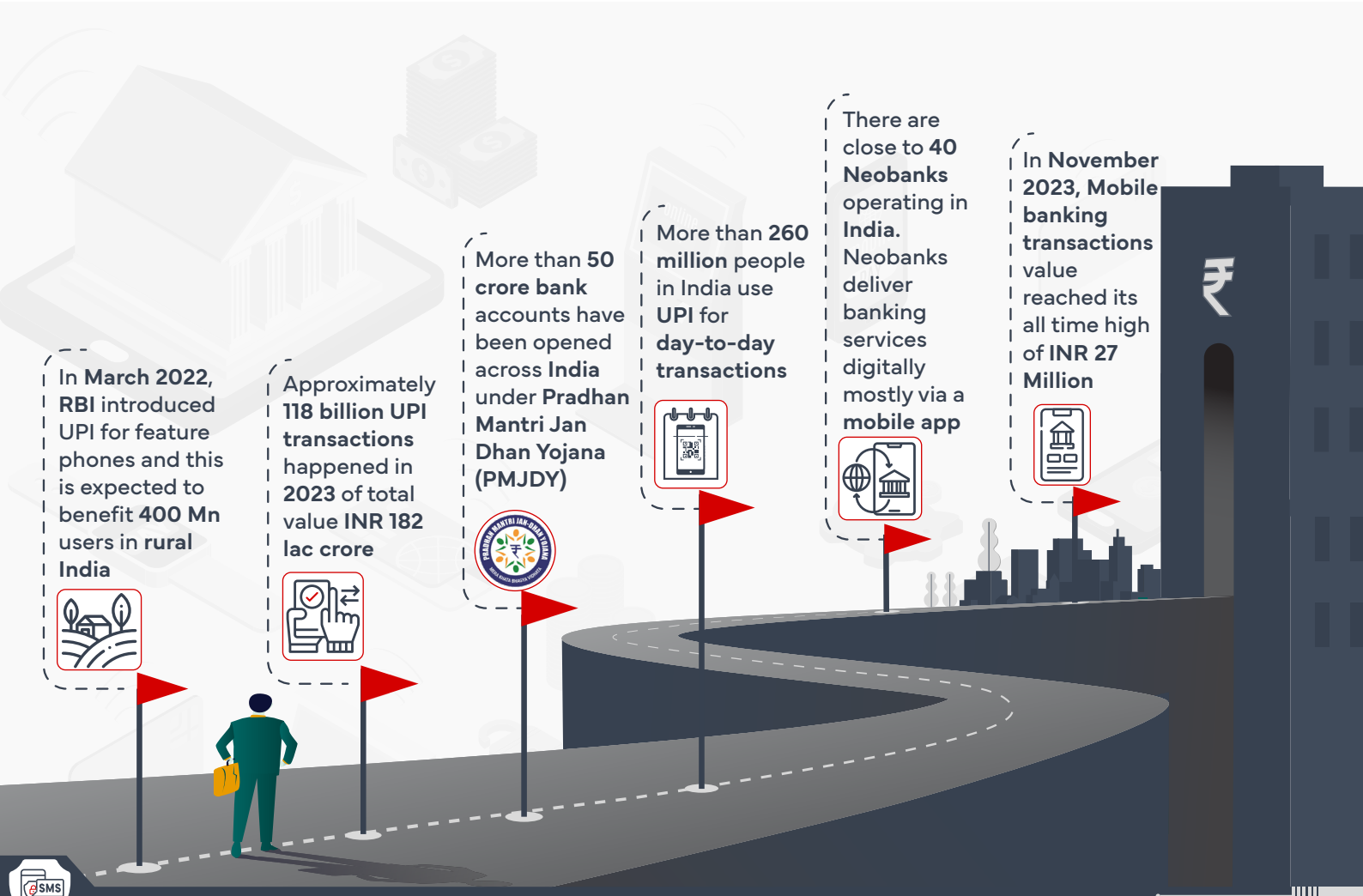
> **"Indians made more cashless payments in a month than Americans did in 3 years"**
>
> *S Jaishankar, External Affairs Minister, Government of India*

Banks are expected to continue their growth trajectory and offer new and innovative products as per changing customer demands. This will drive banks towards revisiting their IT strategy and also embrace technology-based IT solutions that can provide an agile banking experience to their customers.

India's Financial Leap: Banking Powered by Mobile Penetration

With a median age of 28.7 years, India's population is considered one of the youngest in the world, and this population is a prime driver for our digitization efforts across the spectrum. There are currently close to 700 million smartphone users in India, which is expected to reach 1 billion by 2026. Similarly, the number of smartphone users in rural India has doubled in recent years.

Mobile phones play a critical role in disseminating banking services as they are one of the most accessible modes through which banks connect and communicate with their customers. Initiatives like Pradhan Mantri Jan Dhan Yojana (PMJDY) are bringing individuals in remote areas into the financial inclusion ambit. This, along with the growing penetration of mobile phones, will further increase the number of financial transactions, and banks will use multiple communication channels to stay connected with their customers.



Zero Loss, Zero Delay: Importance of Timely and Seamless Communication in Banking

As banking processes are going digital, most financial transactions happen in real-time. In such a scenario, preventing data loss and ensuring real-time communication with customers becomes top priority. Delays in communication concerning real-time transactions might open up a window for cybercriminals to take advantage. This leads to financial losses, which can dent the bank's reputation and attract heavy penalties from the banking regulatory authorities.

With an improving digital footprint, banks in India have developed an effective communications strategy involving customers, employees, regulators and other financial authorities. India accounts for nearly 50% of the world's Real-Time Payments (RTP), with over 50 billion transactions (in 2023). As banks deal with such large volumes of monetary transactions, it becomes critical for them to ensure timely delivery of business critical communications.

2 to **5%** is the global average SMS delivery failure rate across different industries

During communication process, the message delivery failure rate for most of the businesses are in the range of 2-5% globally. For most organizations, these could very well be within acceptable limits and might not affect their business operations significantly. However, in case of banks, having a delivery failure rate even as low as 2% can still disrupt their services.

For example, banks use SMS tool for sending critical alerts. If these messages are not delivered in real-time, it can hinder customers' ability to take immediate actions which can potentially lead to financial consequences.

Banks look to achieve **100% delivery rate** as there are critical financial aspects involved

Objectives of Effective Banking Communications

Transparency in Conveying Financial Transactions
Communicate with customers for OTP delivery; notify about any account activities

Promote Customer Engagement
Communicate about new products, services, schemes or offerings

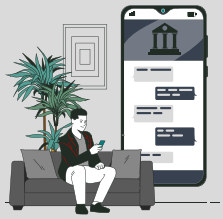
Complying to Regulatory Requirements
Notify customers through statutory messages and any potential dangers related to financial frauds

Internal Communication Purpose
Communication among employees across different branches

SMS: The Backbone for Uninterrupted Bank-Customer Communication

SMS has been one of the oldest communication methods used by businesses and consumers. Although several other forms of communication like email and live chat have emerged recently, SMS remains one of the safest and quickest methods banks use to connect with customers. SMS communications have become essential for sending transactional alerts, authentication codes, verification requests, or promotional messages. It also allows banks to have fast one-on-one or one-to-many communications. In addition to being simple, it is one of the most effective and accessible channels for banks to communicate with customers. Banks have realized the importance of SMS as an effective tool to reach customers swiftly and efficiently.

9 out of 10 times customers access transactions alert message via SMS



Nearly **80%** of the banking customers says they prefer SMS over emails/call to receive transcational communicaion

6 out of 10 people in the rural India have feature phones and use SMS extensively to access information

Banks in India are procuring **"Multi-lingual SMS"** solutions to further enhance bank-customer communications

In addition to regulatory requirements, the growing customer expectations and adoption of new technologies have pushed banks to have a proactive approach towards cyber security. The banking industry in India is the biggest adopter of cybersecurity solutions, and the spending is expected to reach nearly $1 billion by 2025. However, in recent times, the industry has also seen a continued trend of growing cyberattacks.

Growing Vulnerabilities in the Banking Industry

INR 4.69 lakh Crore is the loss banks incurred due to frauds from June 2014 to March 2023 as per RBI

Nearly **90%** of banks in India have faced Ransomware attack attempts in the past one year

12,069 cases of card and Internet banking frauds were recorded in H1FY24 as compared to 2321 cases in H1FY23

13 lakh cases of cyber-attacks were recorded in financial sector in India from Jan to Oct 2023

Secured Banks and the SMS Backdoor: Facing the Vulnerabilities

While SMS is the most straightforward method for banks to communicate with their customers, it is also one of the most vulnerable factors in banks' overall cyber security posture. As banks continue to strengthen their IT security to minimize risks that can impact banking infrastructure, SMS serves as an easy and accessible portal for cyber miscreants. While tactics like phishing have always existed for years now, the growing instances of SMS fraud have given rise to a new term called "Smishing", which is a new approach where attackers, instead of sending phishing content over email, use SMS or MMS text messages to carry out attacks.

Nearly 70% of the world's population uses text messages to communicate with other individuals or brands. In India, commercial SMS traffic has grown to almost 2 billion per day, thanks to the Internet and mobile revolution we are witnessing. Consequentially, SMS-related frauds have also seen a gradual rise in recent times. With more than 700 billion commercial messages being sent every year, SMS has become a weak link that Indian banks have to deal with despite having strong IT infrastructure security in place.

Nearly 65% of Indians fall for fake messages that they receive as SMS

On an average, Indians receive 4-5 fake messages in a day

Around 89% of Indians feel measures like DND do not stop fake messages

Common type of fake messages are job offers (60%) and bank alert messages (55%)

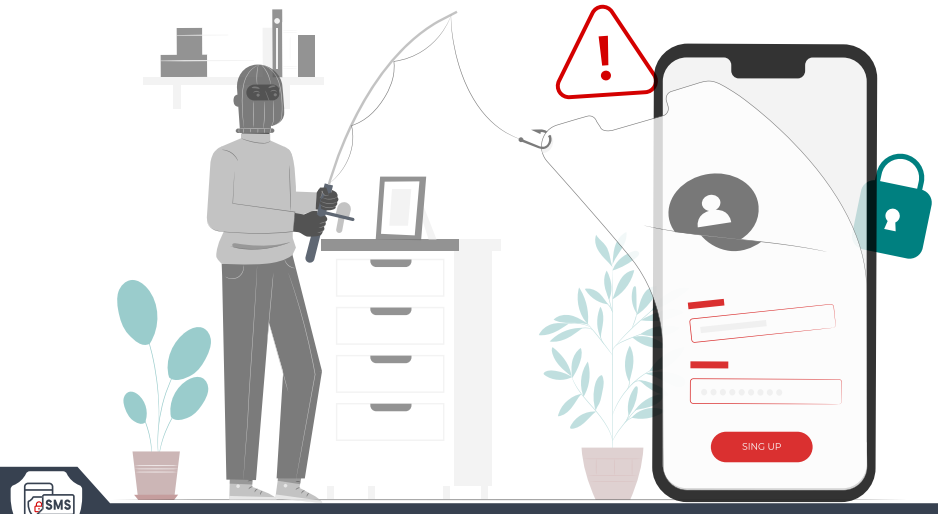
More than 54% of Indians say they are unable to identify fake SMSes

"40 and above" age group having mobile phones are most prone to SMS frauds

Role and Impact of SMS Spam and Smishing in Banking Frauds

SMS fraud or Smishing has a significant impact on both banks as well as their customers. Apart from the monetary losses for banking customers, SMS frauds can prove an entry point for cyber miscreants to carry out different types of attacks on the banking infra or overall operations. These attacks may be related to accessing the private information of banking customers and holding banks for ransom or gaining access to the bank's network infrastructure to disrupt operations or steal money. SMS fraud can also lead to a loss of trust among the customer community, thereby bringing down the brand value of banks

As the instances of fraud continue to grow via SMS, banks in India are turning towards technology to tackle SMS spam or Smishing incidents effectively. Banks and telecom service providers in India are partnering to develop solutions that can effectively mitigate risks arising from SMS. Regulatory authority TRAI had introduced blockchain based Distributed Ledger Technology (DLT) to prevent SMS spam. DLT is a digital system for keeping and managing the record of sender IDs and template. Entities need to register with the operator's DLT platform by submitting necessary business documents



AI and ML as Guardians: Proactive Strategies to Counter Threats

Globally, spam messages lead to losses of approximately $5 billion every year to telecommunication service providers. In India, TRAI has laid down stricter regulatory frameworks and levies heavy fines on telecom companies, telemarketers and brands who fail to deal with spam. To curb the menace of Unsolicited Commercial Communications (UCC), the Telecom Regulatory Authority of India (TRAI) has taken a series of measures through "The Telecom Commercial Communications Customer Preference Regulations, 2010", which protects customers from UCC and on the other hand directs the entities involved to send commercial communications only for customers who opt for receiving such communications. In 2023, TRAI introduced the Digital Consent Acquisition (DCA) program, which mandates telcos to obtain explicit user consent before sending any promotional messages. It also introduced DND 3.0, which helps users to identify and block spam calls and SMS. More importantly, TRAI has also mandated that telecom service providers use AI to check spam calls and messages. In May 2023, TRAI directed access providers to employ AI filters to protect telecom users from unwanted SMS, phone calls or emails.

But Why AI/ML for SMS Fraud Prevention?

Detection

- AI/ML, social graph techniques to automatically differentiate between actual enterprise sender and spam
- AI/ML to detect intricate patterns and anomalies within large data sets automatically
- ML to adapt and learn from new data – Useful when fraudsters try to come up with new tactics
- AI/ML for processing large volumes of SMS data automatically and in real-time

Prevention

- Establishing of secure and direct connection between the enterprise and telcos and sharing fraudulent numbers among enterprises, authorities and other telcos
- Content Analysis – AI models to identify keywords, phrases and linguistic patterns
- Behavioral Analysis – Analyzing user behavior based on historical data like frequency, timing & interactions
- Network Analysis – Analyzing network patterns using AI/ML to detect unusual activities

Response

- Automatic suspension of of simboxes, sender IDs, content templates and numbers/domains used inside smishing messages
- Notifying users when they receive potential fraudulent messages using AI/ML capabilities
- Notifying users when they receive potential fraudulent messages using AI/ML capabilities
- Combining AI/ML models with human fraud analysts to develop optimized response strategies

AI filters save businesses and telecom providers time and resources by detecting and preventing SMS fraud. With continuous machine learning (ML) techniques, the need to update the spam blocking rules manually gets eliminated, and thus, through these mechanisms, spammers can be blocked in seconds instead of hours. This also leads to improved customer experience as the number of unsolicited messages can be decreased drastically. Additionally, it also helps telcos to reduce the network load and non-value add traffic. The detection and prevention through AI and ML backed solutions will complement the regulatory frameworks that are in place to minimize SMS related fraud incidents and block SMS spam.

How AI helps in SMS Spam Detection?

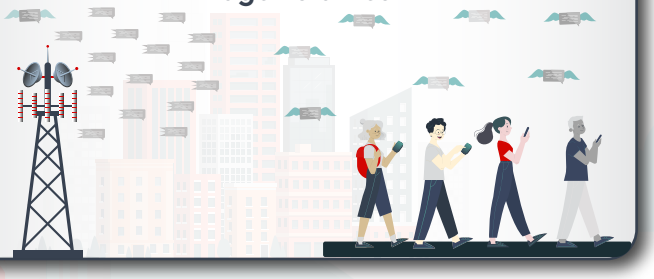
Telcos Leading On-time Delivery and Secured SMS Communicaiton

In February 2023, the Telecom Regulatory Authority of India (TRAI) directed telcos in India to block all unverified headers and message templates within the next 30 and 60 days, respectively. It also instructed telcos to reverify all registered headers & message templates on the DLT (Distributed Ledger Technology) platform in order to prevent misuse by telemarketers. It has also asked all the telcos to come up with AI/ML based SMS spam detection and prevention solutions that form an integral part of any SMS suite offered by telcos.

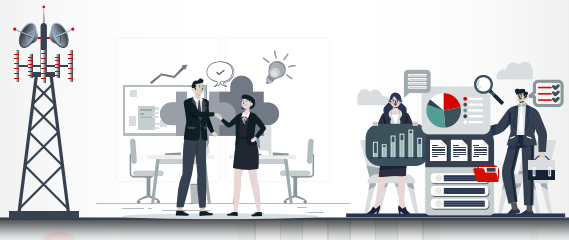
Telecom service providers are playing a significant role in SMS spam detection and prevention by introducing AI driven spam blocking solutions as a part of their SMS suite. Businesses, especially banks in India that have to deal with financial and regulatory risks, are working directly with telcos to solve SMS spam and fraud issues. Most banks, who were earlier heavily dependent on 3rd party SMS aggregators for their communication requirements, want to eliminate that extra layer between them and telcos when delivering messages to their end customers. Banks dealing directly with telcos offer a win-win situation to every stakeholder involved.

The ultimate SMS service provider, eliminating mediators in between

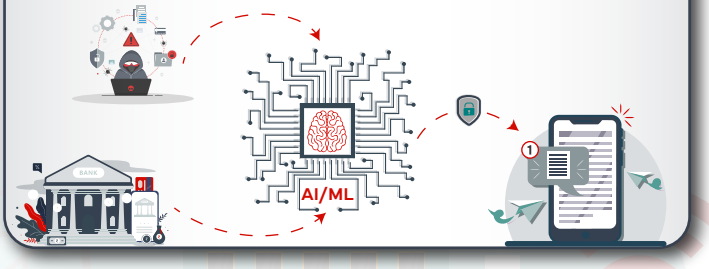
Offer robust SMS platform to handle huge volumes



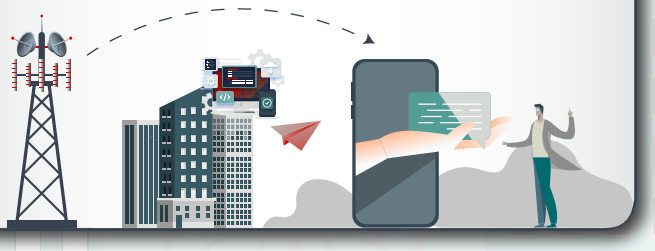
Provide business customers with transparent SMS delivery reports



Help in identifying and restricting unregistered SMS headers for banks with AI/ML capabilities

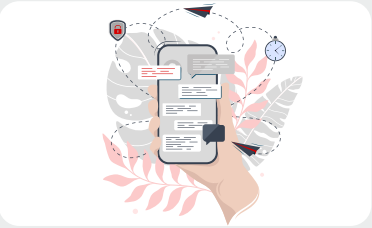


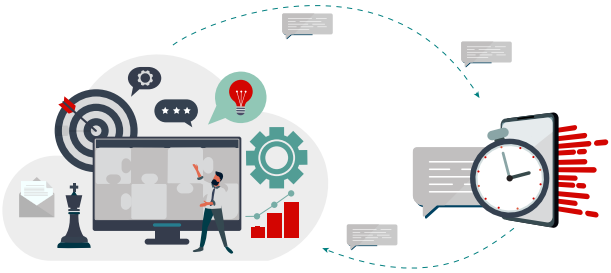
Ensure better SMS delivery timelines by eliminating mediators



Airtel IQ – Delivering Timely & Secure Customer Communications

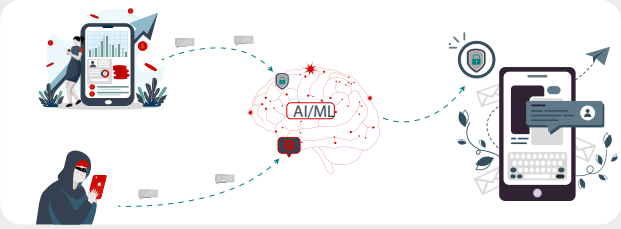
Airtel IQ is committed to ensuring optimal performance in communications by guaranteeing high delivery rates and minimal latency, alongside stringent security measures across multiple messaging channels. Not only does it ensure comprehensive reporting transparency, but it also delivers an uncompromised commitment to a seamless messaging experience.





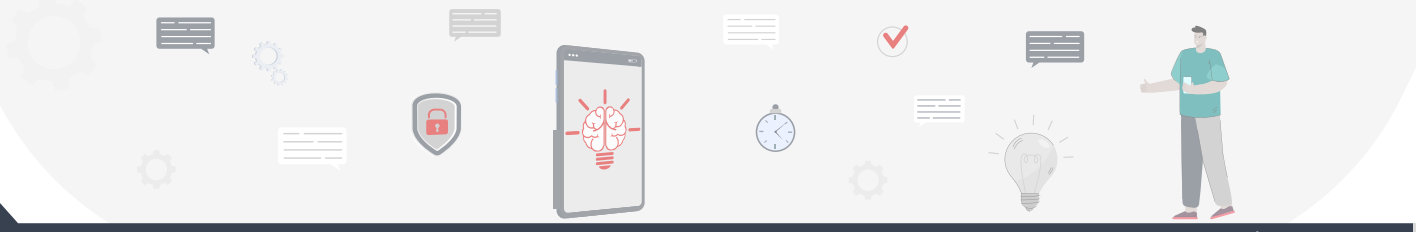
Utilizing state-of-the-art messaging technologies, Airtel IQ achieves superior delivery rates. Its intelligent communication orchestration capabilities span various channels, adapting to end-user preferences to ensure messages are received on the most relevant platforms.

Security is paramount with Airtel IQ. It establishes direct connections with financial institutions to secure the integrity of messages. Coupled with advanced AI/ML algorithms, Airtel IQ proficiently identifies spam, blocks suspicious activities, and provides sharp, actionable insights to its clientele.

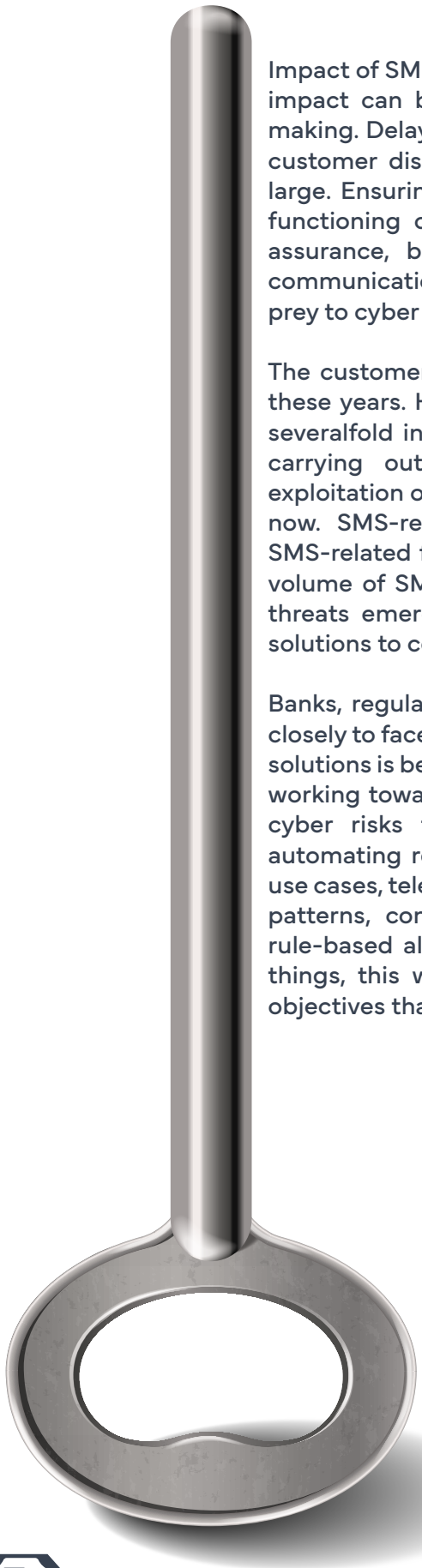


In partnership with banks, Airtel IQ contributes to fraud prevention by providing real-time alerts on critical issues like SIM swaps, device changes, and location anomalies. These proactive alerts enable banks to swiftly initiate transaction re-verification processes, bolstering defenses against fraud.

Airtel IQ's direct integration with telecom services reinforces the reliability of delivery reports. This integrity leads to unblemished transparency, offering businesses precise analytics to inform their strategic decisions.



Key Takeaway



Impact of SMS delivery failure varies from industry to industry. In case of banks, the impact can be severe affecting customer trust, security and financial decision making. Delay in communication or failure to deliver critical messages can lead to customer dissatisfaction, operational discrepancies and reputational damage at large. Ensuring zero latency in delivering messages remains crucial for seamless functioning of banks in today's modern digital landscape. Along with delivery assurance, banks have the responsibility of establishing a safe and secure communication medium with their customers. Ensuring that customers do not fall prey to cyber attackers becomes an equally important priority for banks.

The customer community has dealt with security threats from email phishing all these years. However, as the use of SMS for commercial purposes has multiplied severalfold in recent years, cyber miscreants have shifted the goalpost. They are carrying out attacks on customers using SMS-related vulnerabilities. This exploitation of SMS has given rise to new challenges that users accessing SMS face now. SMS-related scams, more popular as Smishing today, have multiplied. SMS-related fraud has become an unmanageable menace for Indian banks as the volume of SMS traffic grows. In addition to educating customers about possible threats emerging from messages, banks have felt the need to have fool-proof solutions to combat these threats.

Banks, regulatory authorities, and telecom service providers in India are working closely to face these challenges. The emergence of blockchain and AI and ML-based solutions is becoming a boon in tackling SMS fraud. They are helping businesses and working towards a more significant cause of protecting customers from potential cyber risks that can impact their financial well-being. These solutions are automating repetitive processes and minimizing human errors. Among the many use cases, telecom companies are using AI/ML capabilities to automatically identify patterns, conduct behavioural and content analysis in real-time, and build a rule-based algorithm to minimize SMS spam and fraud. In the larger scheme of things, this will help banks further their efforts in achieving financial inclusion objectives that are critical in nation-building exercises.

About Airtel Business

Airtel Business is a leading provider of integrated communications solutions in India. With a wide gamut of end-to-end solutions spanning cellular IoT, connectivity, cloud, data centre, cyber security and cloud-based communications, the company's offerings are engineered to deliver high-speed connectivity, unparalleled wide coverage and scalable bandwidth to customers across enterprises, governments, carriers and small and medium businesses (SMBs).

For more details, visit https://www.airtel.in/business/

About Think Teal

Think Teal is an Analyst firm tracking the Enterprise ICT Market in India. Think Teal helps technology firms understand the markets that they serve and support them in achieving their business objectives.

To understand more about Think Teal, reach out at connect@think-teal.com