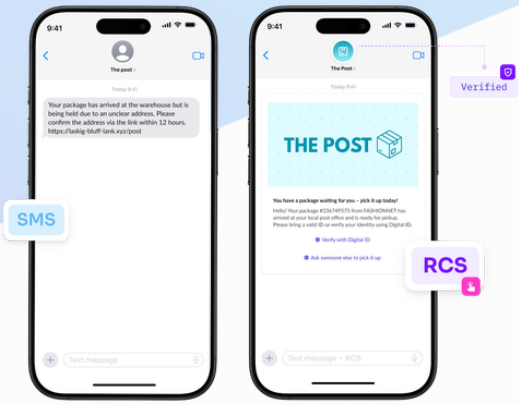
RULE

Read more about RCS | Book demo

RCS – A Safer Way to Communicate with Your Customers

Why high-integrity industries are moving beyond SMS



The challenge: Your customers can't tell what's real

SMS has long been a critical channel for customer engagement, yet it was never built to handle modern security threats. Today, smishing (SMS phishing) is one of the fastest-growing fraud methods globally, with financial, insurance, and logistics brands most at risk.

The Structural Vulnerability:
SMS lacks a native mechanism to guarantee sender identity. Because "Sender IDs" can be spoofed or injected into existing message threads, trust has become a matter of appearance rather than fact. For organizations in banking, insurance, or public services, this means your brand can be replicated with zero access to your internal systems, leaving the burden of verification entirely on the unsuspecting customer.

Why the Risk is Escalating

Fraudsters target industries where messages are expected and urgent. Banking, logistics, and public services share a common trait: customers are accustomed to receiving time-sensitive updates. This familiarity is exactly what makes impersonation effective. Even well-informed users can make incorrect decisions at urgent situations.

At the same time, customer skepticism is rising. As users become more cautious of SMS links, a "trust gap" emerges. The result is a paradox: organizations are sending more communication, but achieving less trust.

The Solution: RCS as the New Security Standard

Rich Communication Services (RCS) is not just "SMS with pictures." It is a fundamental shift in mobile identity management. By moving to an IP-based framework, RCS introduces three layers of security that SMS cannot match:

The Verified Sender Framework

RCS requires a "Verified Sender" status. Before sending a single message, your brand undergoes a rigorous vetting process by platform providers (e.g., Google or Carriers). Once approved, your messages are delivered with a Verified Badge that is cryptographically tied to your specific agent. This cannot be spoofed or replicated by scammers.

On-Device Authentication

When an RCS message arrives, the device OS validates the sender's certificate. If successful, your official logo, brand name, and colors are displayed. If validation fails, these branded elements are withheld. This removes the "burden of proof" from the customer. If they see the checkmark, they know with full certainty it is you.

Enhanced Transit Security

RCS utilizes **Transport Layer Security (TLS)**. From the moment a message leaves your server until it reaches the device, it is encrypted. This ensures that sensitive data, such as policy updates or transaction alerts, remains private and tamper-proof.

RULE

Read more about RCS | Book demo

RCS – A Safer Way to Communicate with Your Customers

Why high-integrity industries are moving beyond SMS

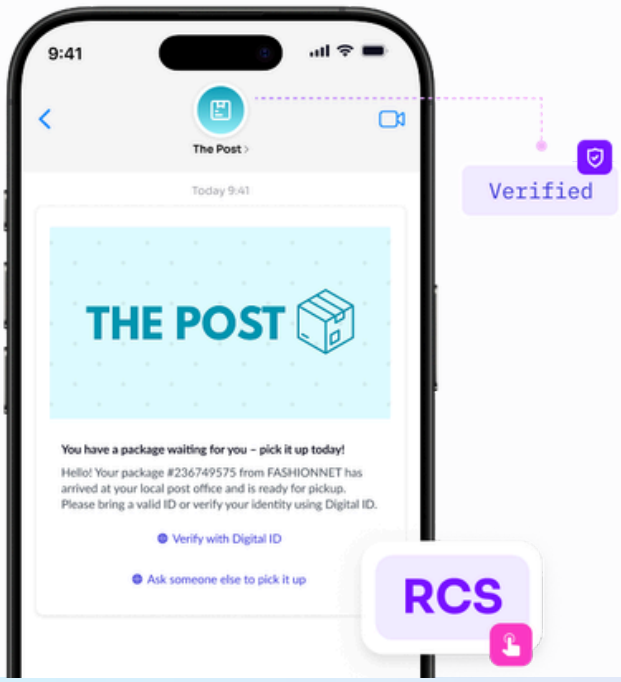
Higher Trust Equals Higher Engagement

Security is often viewed as a cost, but with RCS, it is a performance driver. By removing the "fear factor" of clicking a link, engagement rates rise:

Increased Engagement: RCS branded messages see up to a 74% higher engagement rate than plain-text SMS.

Higher Conversions: Campaigns have shown 20–35% improvements in conversion rates due to the trusted, interactive nature of the channel.

Reduced Support Costs: Providing a verified channel reduces the volume of "Is this message real?" inquiries to customer support.



Implementing Secure RCS Messaging with Rule

Rule's RCS editor allows organizations to adopt this new standard without technical complexity. Rule provides the interface to manage your verified sender profile and communication flows from a single platform. With Rule, you can:

- **Design secure, branded messages** aligned with compliance requirements
- **Communicate** through carrier-verified channels
- **Track performance and engagement** in real-time
- **Ensure 100% Reach:** Rule utilizes SMS Fallback. If a recipient's device does not yet support RCS, the system automatically defaults to a standard SMS, ensuring no customer is left out

Conclusion: A Strategic Necessity

The transition from SMS to RCS represents **a shift from exposure to control**. With SMS, your brand identity is at the mercy of external risks; with RCS, your identity is enforced by the network.

For high-trust industries, the question is no longer if you should move to RCS, **but when**. By adopting RCS with Rule, you are reclaiming your brand from scammers, protecting your customers, and upgrading your marketing.

RULE

Read more about RCS | Book demo

RCS – A Safer Way to Communicate with Your Customers

Why high-integrity industries are moving beyond SMS

Example of Industry-Specific Impact

Industry	Critical Use Case	RCS Security Advantage
Banking & Finance	One-Time Passwords (OTPs) & Fraud Alerts	Verified sender status **prevents** "smishing" attempts where scammers trick users into revealing credentials.
Insurance	Policy Updates & Claim Handling	**Securely** share rich media over encrypted channels without requiring a third-party app download.
Postal & Logistics	Delivery Tracking & Proof of Delivery	Interactive buttons allow customers to reschedule or confirm deliveries securely within the thread.

At a Glance: SMS vs. RCS

Feature	Regular SMS	RCS Business Messaging
Identity	Unverified	Verified (Cryptographically Secure)
Branding	None	Full Logo & Brand Colors
Security	No Native Encryption	TLS Encryption in Transit
Interaction	Text & Links only	Interactive Buttons & Carousels
Trust Level	Declining	High (Verified Badge)