GSMA

Case Study: Airtel

Combatting SIM swap and one-time password (OTP) fraud through network APIs

Case Study: Airtel

Combatting SIM swap and one-time password (OTP) fraud through network APIs

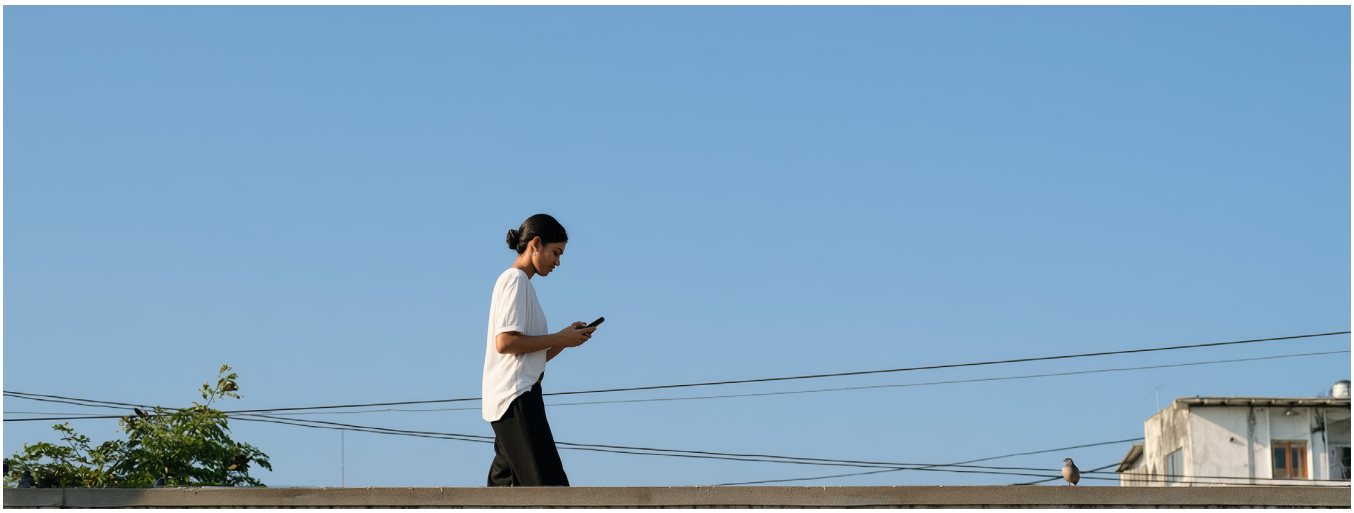
Fraudsters increasingly exploited unauthorised SIM swaps and device changes to hijack customer accounts, intercept one-time passwords (OTPs) and take over banking, fintech and messaging accounts. Banks, fintechs and over-the-top (OTT) platforms typically lacked real-time visibility of telecom-side signals, such as a recent SIM or device change, that would have allowed them to identify these account takeover attempts before a transaction was authorised. This gap left customers vulnerable to fraud rings that used unauthorised SIM replacements, social engineering, account compromise and device changes to intercept authentication codes and bypass existing security checks.



Solution

Airtel developed and implemented a suite of real-time fraud prevention application programming interfaces (APIs), compliant with GSMA Open Gateway / CAMARA standards, that banks, fintechs, OTTs and government agencies could integrate to tackle financial fraud at scale. Several of these APIs addressed account takeover fraud directly.

- The SIM Swap API detected whether a SIM change had occurred within a defined time window, helping partners identify high-risk transactions potentially linked to unauthorised SIM replacements (SIM swaps) or account takeover attempts.
- The Device Swap API flagged recent changes in SIM-device pairing, allowing OTT and messaging platforms to prompt additional verification and identify potentially fraudulent activity where a subscriber's SIM is suddenly associated with a new device shortly before a high-risk transaction.
- The Call Forwarding Signal detected whether call forwarding was enabled on a device, helping identify potential account takeover attempts and other fraud scenarios.



Airtel complemented these with five additional APIs that strengthened identity and location-based verification as outlined below:

- The Location Verification API, subject to explicit user consent and applicable privacy requirements, verified whether a device was present at a specified latitude and longitude, supporting customer onboarding and underwriting workflows in banking and fintech.
- The Location Retrieval API enabled authorised applications, subject to explicit user consent and applicable privacy requirements, to obtain network-derived location information to help validate a user's whereabouts during a financial transaction.
- The Device Roaming Status Check determined whether a device was currently roaming, helping identify potentially suspicious or high-risk transactions.
- The Number Verification API confirmed that a phone number belonged to the connected device over the mobile network, enabling secure SIM binding and a seamless, passwordless login experience.
- The One-Time Password (OTP) SMS API allowed developers to send and validate short-lived verification codes directly through a network operator.
- All eight APIs were lightweight, responded in real time and returned a simple Yes/No signal, enabling partner businesses to take instant decisions such as delaying a transaction or enforcing re-authentication.

Impact

The APIs provide banks, fintechs, and OTT platforms with telecom-level insights that were previously unavailable, enabling them to identify high-risk transactions linked to SIM replacements, swapped devices or intercepted OTPs before they are completed, and to trigger additional verification or delay authorisation where appropriate. Designed as a modular solution requiring minimal changes to existing systems, the APIs can be integrated quickly, enabling rapid deployment and faster time-to-value. The OTP Validation API has already received GSMA certification, is live in India, and is being scaled to additional international markets.

Additional information	
Cost:	Not specified.
Participating organisations:	airtel
Location:	Asia Pacific.

