comviva
A TECH MAHINDRA COMPANY

MONETIZING A2P FOR A **LEADING TELECOM OPERATOR** WITH SMS FIREWALL AND MANAGED SERVICES

THIS MAJOR COMVIVA CUSTOMER IS ONE OF THE LARGEST OPERATORS IN AFRICA

WITH A 15% SHARE OF THE SUBSCRIBER BASE IN THE COUNTRY IT OPERATES

comviva
A TECH MAHINDRA COMPANY

WITH ITS VOICE AND MESSAGING REVENUES FROM P2P GOING INTO A STEEP DECLINE, THE OPERATOR WISHED TO **LEVERAGE THE A2P OPPORTUNITY TO DRIVE BRAND VALUE AS WELL AS REVENUES.**

For the leading operator in Africa, monetizing A2P messages was a significant challenge. **Grey routes were accounting for more than 50% of A2P messaging traffic** for the operator leading to significant revenue leakage.

This was attributed to leading global brands contributing to grey route partnering with external aggregators. Also, UCC messages being sent to subscribers were leading to customer dissatisfaction and churn.

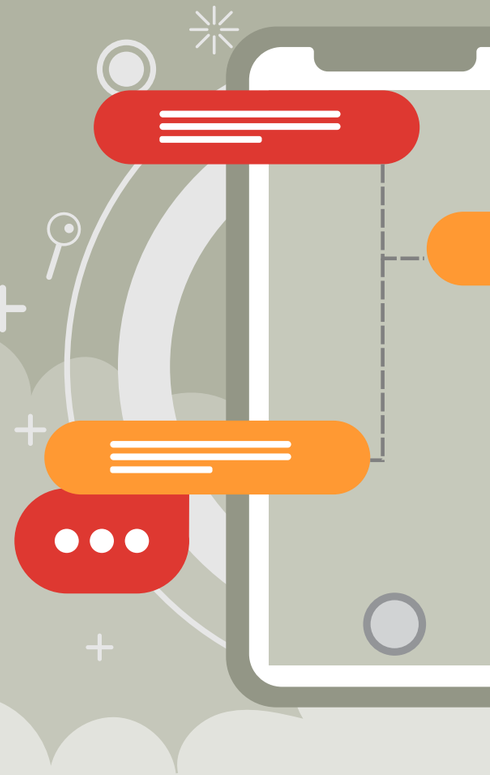
A2P OPPORTUNITY

IN A RELATIVELY SHORT SPAN OF TIME, A2P HAS BECOME THE GO TO CHANNEL FOR ENTERPRISE ENGAGEMENT ALL OVER THE WORLD.

No other customer channel matches its reach or immediacy. Open rates of SMS are higher than any other channel of communications, including email.

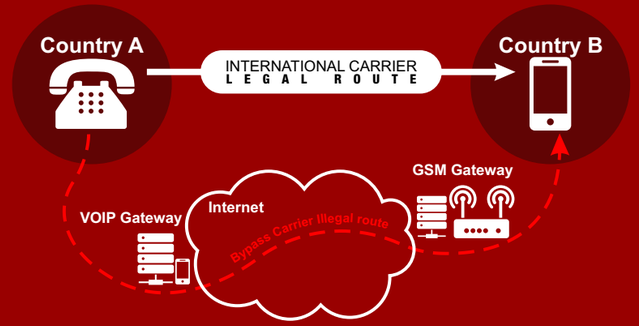
SMSs are read within seconds, creating an effective vehicle for customer targeting.

SMS is device and platform agnostic, unlike OTT apps, making it even easier for enterprises to communicate with their customers, anytime, anywhere with a certain degree of certainty.

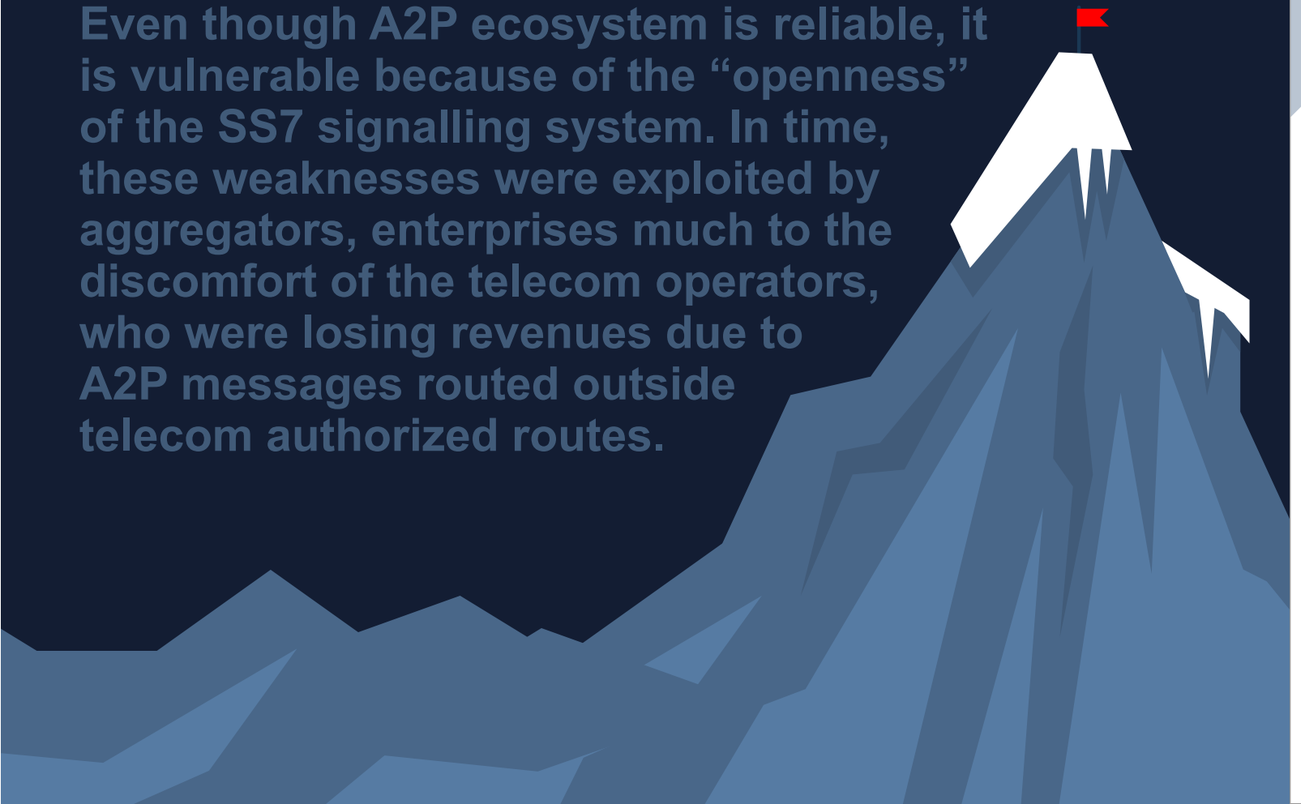


At the core of this enterprise connectivity, is the A2P network, which operators have approved, and in many cases monetized for commercial and non-human generated traffic.

In a typical A2P monetization scenario, the recipient operator, on whose network the message terminates, charges the sending operator a small fee in lieu of processing the SMS. When A2P messages are routed outside operator authorised A2P routes, the operator on whose network the message is terminated loses out on additional revenues in the form of message termination fees.



Even though A2P ecosystem is reliable, it is vulnerable because of the “openness” of the SS7 signalling system. In time, these weaknesses were exploited by aggregators, enterprises much to the discomfort of the telecom operators, who were losing revenues due to A2P messages routed outside telecom authorized routes.

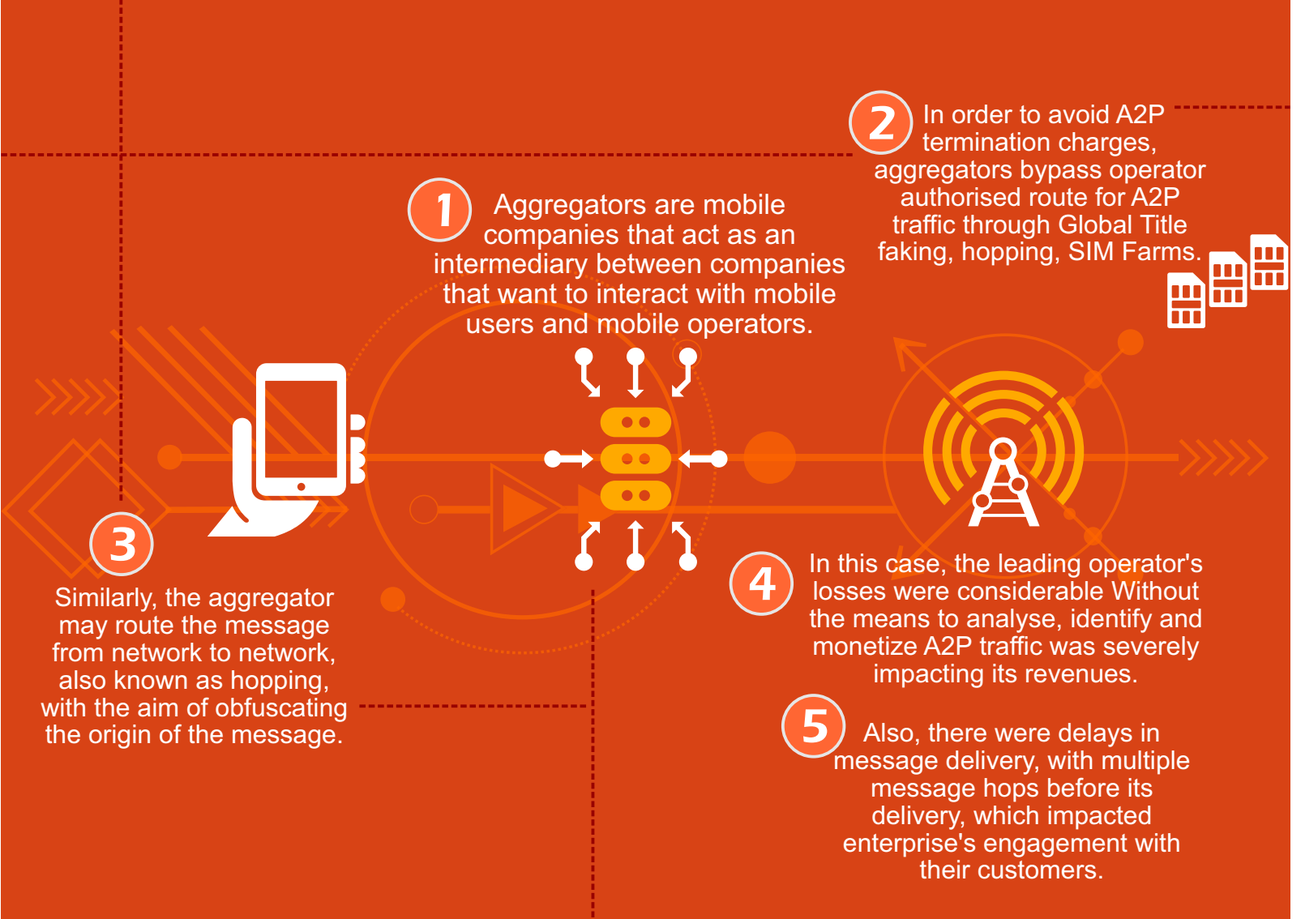


CHALLENGE #1

LOST REVENUE OPPORTUNITY DUE TO GREY ROUTES

1 Aggregators are mobile companies that act as an intermediary between companies that want to interact with mobile users and mobile operators.

2 In order to avoid A2P termination charges, aggregators bypass operator authorised route for A2P traffic through Global Title faking, hopping, SIM Farms.



3 Similarly, the aggregator may route the message from network to network, also known as hopping, with the aim of obfuscating the origin of the message.

4 In this case, the leading operator's losses were considerable Without the means to analyse, identify and monetize A2P traffic was severely impacting its revenues.

5 Also, there were delays in message delivery, with multiple message hops before its delivery, which impacted enterprise's engagement with their customers.

CHALLENGE #2

LOST CUSTOMER EXPERIENCE (CX) OPPORTUNITY DUE TO A2P SPAM

Some aggregators hide behind telecom global titles forcing telecom operators faces the brunt of aggregator originated scams.

Poor customer experience - customers were bombarded with UCC messages almost on a daily front.

Customer churn, as many of these messages were smishing or attempted hacks to prise out information.

CHALLENGE #3

INABILITY TO RISE UP THE DIGITAL VALUE CHAIN

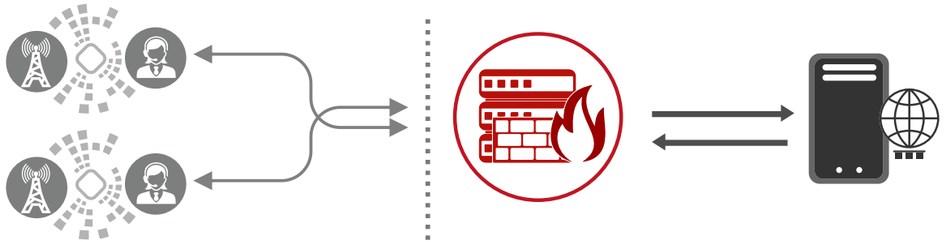
On an altogether different plane, some of the aggregators may hide behind telecom global titles for spamming purpose. Invariably, in such cases, it is the telecom operator that faces the brunt of aggregator originated scams.

In this case, the client was faring very poorly on the customer experience front, as its customers were bombarded with UCC messages almost on a daily front. This was harming the operator on multiple fronts. Firstly, it was harming its reputation, as the customer was inconvenienced by these messages. Secondly, it was leading to customer churn, as many of these messages were smishing or attempted hacks to prise out information.

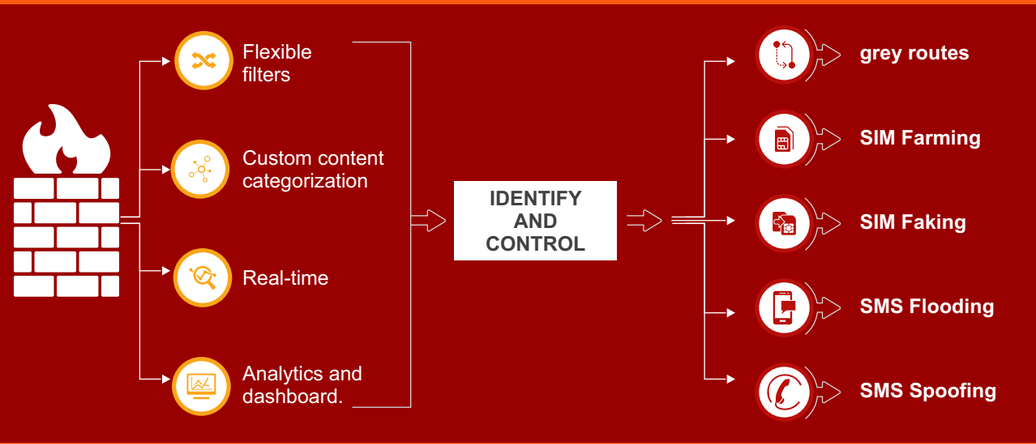
Client required a mature solution that could:
(A) Protect network with right technology and business processes
(B) Guarantee reach via global connections to A2P messaging users.

COMVIVA'S MESSAGING FIREWALL SOLUTION

The most comprehensive network-based and content based messaging security solution enabling operators to effectively monetize on their A2P traffic and protect consumer and enterprise customers against the growing threat of mobile abuse.



Comviva's solution uses **innovative ways to track** and **analyze** the incoming **message traffic**, **validate** the message's **source** and **filter** them according to the content.



AI/ML FOR NEW THREATS

The client had a need for further customization to stop new and emerging threats.

Comviva's solution was a **fully managed service capability** designed to ensure that the platform is operated, configured and updated with latest security rules on an ongoing basis.

AI-powered SMS filters that utilize **deep learning artificial intelligence systems** to identify and filter spam SMS before they reach the end user. **Artificial intelligence technique called guided machine learning**, combines advanced machine learning algorithms to build classification models better than either machines or human beings alone.

KEY DIFFERENTIATORS

Unidentified Cluster Analysis for Brand Recognition

Inline URL/domain analysis with support for tiny URLs to effectively curb cases of phishing and malware exposure

Subscriber consent verification with Subscriber Management and Do Not Disturb Modules to effectively curb spam

NFV enabled solution

Flexible Rule and Counter Management with monitor mode, exception rules and time based controls

ML based Content Categorization with vernacular language analysis support

AI Based Reputation and Risk Analysis to detect bad sources that could create a damaging experience

Built-in report suite with customization options like report query builder and integration with BI platforms

NEW REVENUES WITH DIFFERENTIAL CHARGING

Since each message carries a different value for the customer, there was a need for differential charging for messages carrying a higher value for the customer.

This would not only help the operator to:

- → rise up the value chain
- → strengthen the A2P Messaging ecosystem by prioritizing traffic on the basis of immediacy adding value to the recipient.

Comviva helped the client **analyse, assess** and **monetize** the A2P traffic in a phased manner.

At the first stage, A2P traffic terminating on its network was analysed to identify A2P traffic originating from OTT providers. Traffic was assessed on various parameters, such as volume, which helped in fixing value, and informing the stakeholders in the market.

One of the key elements of a robust SMS firewall is ensuring customer experience. The operator has to exercise restraint while blocking any type of traffic on its network.

{ For example, blocking P2P traffic is a strictly no-no. However, in the endeavour to stop grey route traffic, operators may sometimes block unknown traffic on its network. }

To help the situation two rules were fixed:

- → Allow unknown traffic coming through its telecom gateway to pass
- → Block enterprise traffic through non-telco gateway

RESULTS

A2P MONETIZATION

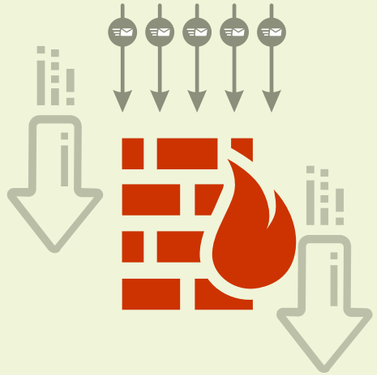
10x increase in A2P revenues

24 hours from go live

COMPREHENSIVE **ANTI SPAM** SOLUTION

Comviva's Messaging Firewall offers:

- → network defense against attack
- → significant reduction in unsolicited commercial messages
- → reduced network load
- → management of SMS termination fee liability with its comprehensive product offering
- → capable managed services



GREY ROUTE BLOCKING

Messaging firewall increases A2P revenues by arresting Grey Routes. Comviva's Grey Route Detection and Blocking Operations Model can 'Analyze' and 'Assess' traffic whilst taking appropriate 'Action' to block or allow any specific traffic to effectively monetize A2P messages.

EFFECTIVE **A2P** MONETIZATION

With Comviva's Managed Services and Messaging Firewall Reporting module, Operators can locate potential revenue leakages and monetize new brand leads.

REDUCED
SUBSCRIBER CHURN

Messaging Firewall has achieved 15% reduced Customer Care complaints on issues regarding spam from its previous deployments.

Messaging Firewall deploys pattern detection with threshold and counter management, and real-time analytics to protect network from spam and fraud.

REDUCED
OPERATIONAL COSTS

Previous deployments have shown to need 30% lesser resource - time - effort utilization for managing operations.