Arelion

Monetization Services

True monetization of business messaging

How can MNOs enhance service quality and increase A2P messaging revenue? Arelion, a globally recognized leader in networking and connectivity, offers A2P messaging traffic and fraud control to secure optimal monetization outcomes

What are the challenges?
Messaging is a very effective communication channel in B2B and B2C markets and SMS will remain predominant for the coming years, even for networks implementing 5G technologies. According to the MEF report published in January 2021, the global fraud levels were estimated at 64% of traffic.
The top 3 A2P monetization issues are all fraud related and as such, MNOs need to apply corrective measures to both secure networks and monetize traffic streams.
MNOs still consider SMS firewalls and managed services to be the principal means of protecting A2P revenue, but are also exploring more collaborative approaches such as traffic profiling, constant pentests, market intelligence and consultancy.

Arelion Monetization Services
As an international carrier, Arelion plays an important role in the service chain, by providing MNOs with platforms and service analytics to drive true traffic monetization. Arelion offers a unique proposition for supporting MNOs in combatting messaging service fraud. Through providing best in class testing and analytical systems to detect illegal termination together with robust security (SMS firewall and frequent penetration testing) Arelion is improving message service quality and enhancing the MNO enterprise customer offering. Operators connected to Arelion Monetization Services have seen boosted revenue and customer experience from day one.

Benefits in brief

SMS firewall
Network protection and fraud prevention to ensure optimal traffic control

Analytics
With the network protected, our analytics tool supplies detailed data on traffic profiles to better steer monetization strategies

Constant monitoring
Penetration tests and market monitoring to maintain network security vigilance

SS7 carrier
Arelion's SS7 carrier status provides superior visibility and protection for the MNO

Improved commercial agreements
Reviewed bilaterals, mutual forgiveness routes, P2P traffic, and pricing

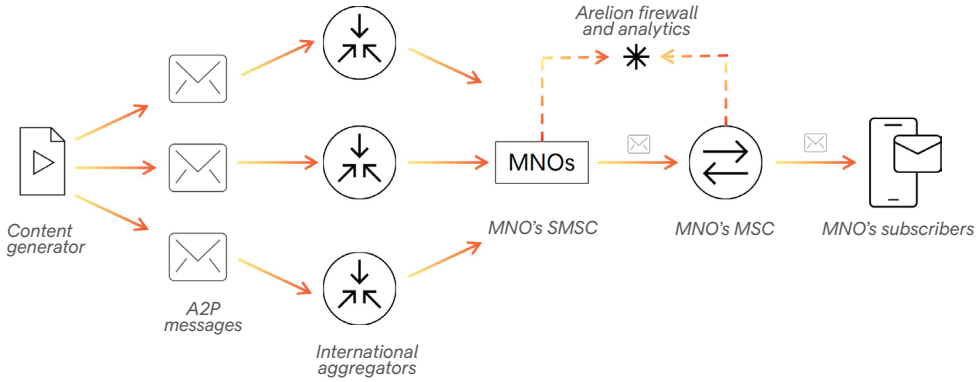


Figure 1: Arelion's Monetization Services

Arelion

Monetization Services

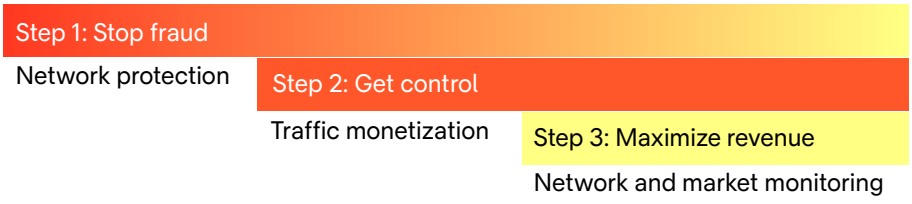
Three steps for true monetization

Step 1 - Stop fraud
MNOs require the most suitable SMS firewall provider to offer and implement a security platform for fraud identification and mitigation. This step alone will not guarantee optimal monetization outcomes – the assumption that the network is permanently protected, and traffic control secured once a firewall is installed is dangerous. A firewall setup can quickly become obsolete as fraudsters seek to exploit other means of bypass.
Two further steps are necessary to ensure maximum protection.

Step 2 - Get control of your traffic
To minimize then eliminate grey termination, MNOs must regain business control through being certain that most of their traffic is terminated on official routes. For many operators, this will represent the first true visibility of their total business potential with a thorough insight into their traffic and revenue profile.
Selecting the right partner will positively impact the MNO: no grey route exploitation, high service quality, no traffic dumping/trashing, enhanced user experience and consistent business growth.

Step 3 - Validation and testing
The steps above will likely produce good initial results, but traffic decreases can be encountered from one day to the next. By definition, the SMS firewall will not alert what it cannot register – traffic bypass will not trigger an alarm on the firewall. It is therefore critical to employ a second security layer to validate and control that the firewall is indeed blocking grey termination or is able to identify the A2P SMS traffic streams that avoid the official routes.

This 3rd step is the most complex as it is dependent on constant monitoring effort requiring experienced, dedicated resources for messaging services, fraud scenarios, signalling engineering and commercial expertise.



Use cases

A real customer case
With the opportunity to conduct a full analysis of an operator's messaging traffic after a firewall had been installed by their long-standing SMS provider, **we were able to detect SS7 grey termination,** as well as the presence of local SIM boxes. Traffic was measured at 140k messages per day. The systems in place lacked the necessary data analytics capability to provide the operator with the necessary understanding of their A2P traffic profile.

Arelion's proposed solution was a best-in-class local firewall to control all entry points. Once this protection was in place, detailed traffic profiling could begin, allowing the MNO clear visibility of what lay behind their international SMS traffic.

Strong rules were applied to guarantee against leakage.
Arelion then began the validation process and new routes were proactively identified. Security was further enhanced following the findings of the penetration tests.

The results were outstanding, with an 300% increase in traffic volumes via official routes in the first year