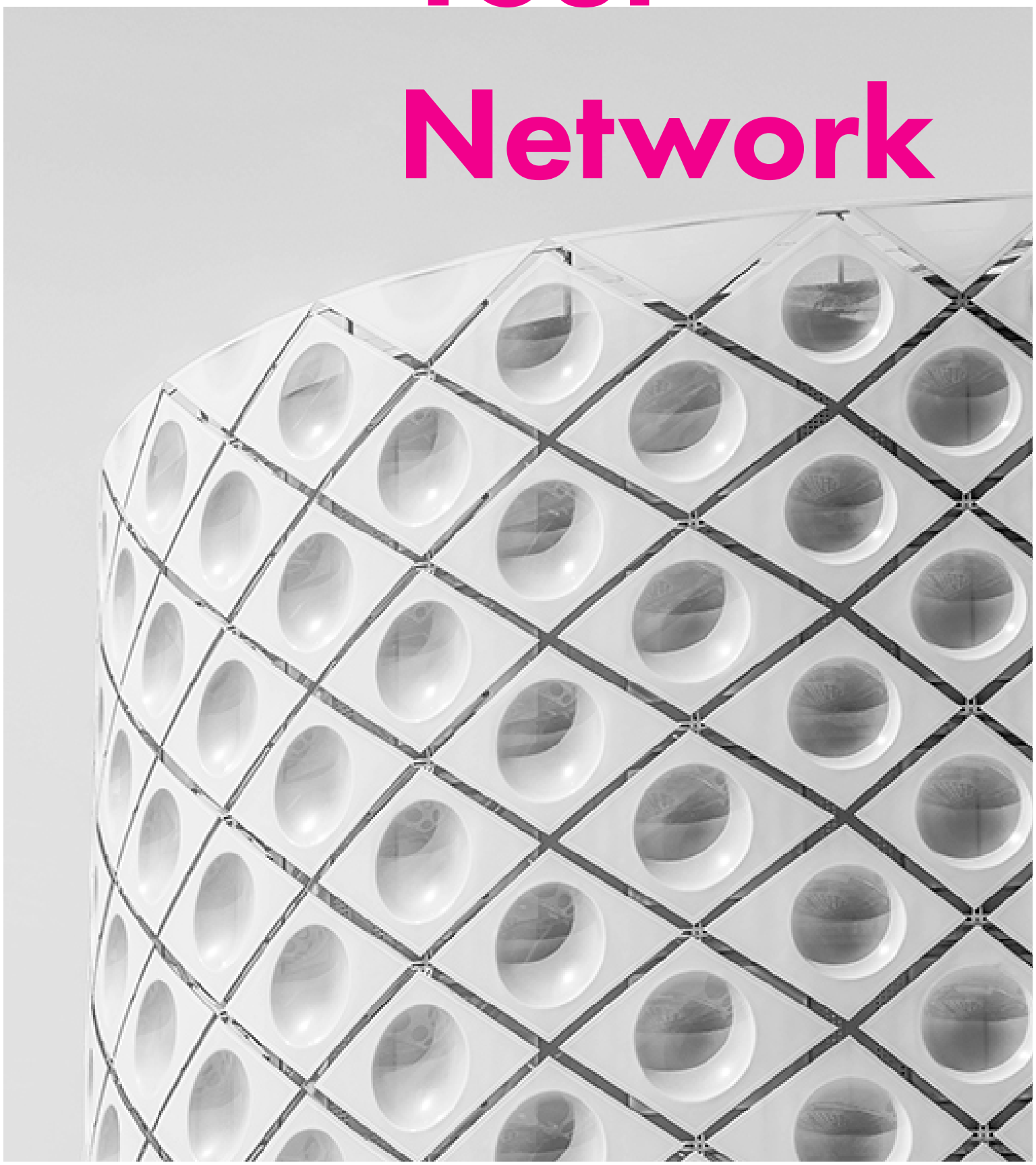
Ring-fence Your Network



Stay in Control: Ring-fence your Network.

WHITE PAPER

First version published in January 2016

INTRODUCTION

With more than 3.7 billion unique mobile subscribers around the world[1], the mobile sector is entering a golden age of A2P messaging. By 2020, the global A2P SMS market is forecast to be worth more than $70.32 billion USD[2], offering plenty of opportunities for operators to grow their business.

The threat to operators' A2P revenues from messaging service providers utilising grey routes and least cost routing is well documented, and awareness of the issue is growing in the industry. International SMS roaming, interworking and hubbing services agreements, such as AA.60, AA.13 and AA.71., have traditionally been subjected to misuse, while SS7 vulnerabilities have also been exploited to avoid paying termination fees.

---

[1] **GSMA**: GSMA Intelligence https://gsmaintelligence.com/

[2] **Transparency Market Research**: A2P SMS Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014 – 2020 http://www.transparencymarketresearch.com/global-a2p-sms-market.html

ONE DOOR CLOSES AND OTHER OPENS

Many MNOs have responded to this by putting in place filtering systems to control inbound SMS traffic from SS7 and international routes, the traditional source of grey route traffic.

However, with international routes more commonly becoming blocked, an increasingly diverse set of new low cost routes have started to become exploited.

RING-FENCE YOUR NETWORK

Local SMPP protocols and Off-Net interconnection traffic are being used to by-pass network filters and now pose the most pressing threat to A2P revenues for operators, as most are not equipped to even analyse the type and volume of traffic coming through these channels.

On top of all this, there is the ever present challenge of spoof or fake SMS traffic and other fraudulent activity that operators need to overcome, to protect their customers and safeguard their brand reputation.

To prevent this from happening, operators need to take the ring-fence approach to controlling their network. To achieve this, traffic management systems need to be capable of effectively controlling not just international messaging gateways, but all access points, including local SMPP connections as well.

Ring-fencing the network in this way can make sure operators take control of each entry point to their network, levelling the playing field for both themselves and aggregators, creating fair market conditions.

STAY IN CONTROL

Operators have invested in their network to provide high-quality services, so it's only right that they are properly compensated for delivering traffic. By effectively ring-fencing their networks from undesired traffic, operators can ensure they successfully stay in control and monetise their A2P traffic, stop revenue leakage and protect their brand image in the eyes of customers.

If you'd like to talk one of our experts about how to ring-fence your network, get in touch at info@haud.com

Stay in Control, stay in touch

haud.com
linkedin.com/company/haudsystems
twitter.com/haudsystems

info@haud.com
Malta: +356 9994 2342
Singapore: +65 6836 6995

For more resources visit haud.com/knowledge-centre