MNOs, SMS A2P, grey route traffic and future competition

How will this market develop in the future?

Contents

The past year has seen the value of the security and efficiency of A2P SMS services take centre stage like never before.

Introduction

As the Covid-19 pandemic swept around the globe, leaving a trail of devastation to people's lives and across business operations, digital communication channels became critical to society like never before.

A key component in this was SMS based A2P messaging, enabling brands to securely and easily send messages or confirm actions with their customers - like two-factor banking authentication.

Yet despite the potential scope this market still has for growth, Mobile Network Operators face several challenges when it comes to securing these lucrative revenue streams.

Firstly, they have to find a way to detect and reduce the volume of grey-market SMS traffic passing across their networks - traffic that is earning organisations other than them revenue despite flowing across their share of radio spectrums.

Secondly, but linked to the first, they must find ways to stop fraudulent A2P SMS reaching their customers. If they can't do this, then the trust consumers and enterprises have in this channel will erode, and with that erosion will come decreased usage and less revenue.

This topic was the focus of a recent webinar featuring HAUD's Head of Global Market Intelligence, Joanna Kuligowska (you can read our report on the event here). The event garnered lots of attention from those working in the industry around how these challenges would play out, how the opportunities could best be taken advantage of, and where technology was taking the sector.

One of HAUD's core values is to share knowledge across our industry, to make progress towards better mobile network security and customer (subscriber) experience.

So, with that in mind, we have put together the following eBook to discuss in greater detail some of questions we were asked in the webinar, and to offer answers to some key questions our partners in the MNO community have about enabling A2P revenues, enforcing network security and unleashing the power of SMS and RCS.

HAUD
STAY IN CONTROL

1

What is the future you see and expect for this business as it fights against the grey routes? What is the HAUD solution with regard to SIM boxes and farms - is it only implemented within the HAUD firewall?

The future for A2P SMS is very positive - there are challenges certainly, and we've outlined some of them above - but it's even more full of opportunities.

The market is growing strongly - A2P is still trusted. It's been proven as a reliable and effective tool in critical communications, never more so than during the Covid-19 pandemic - and in fact the market grew 9% during that tumultuous period.

The sector is also seeing emerging new use cases. Two-factor authentication is morphing into three factors with biometrics used to help secure the channel, SMS is able to remind customers to complete online forms to help sales conversion, and market research done quickly and simply through SMS can help with product market fit - to name a few.

Grey route traffic remains an issue - but it's a solvable issue. The lessening ability of grey aggregators to evade the latest firewall techniques, alongside changes in regulatory regimes in some territories, will help swell A2P revenues and support further investment.

In terms of HAUD's solution to tackling SIM boxes, it's a case of using a variety of technologies to meet both local requirements and regulations, and the MNO's own strategy. For example, in some countries, there are restrictions on what content filtering MNOs can do - so there we have to do more probing on the network and work closely with authorities to understand what is allowed, and then couple those techniques with AI tools to spot patterns and volumetrics to track usage.

> A2P is still trusted. It's been proven as a reliable and effective tool in critical communications.

Ultimately, though, whatever combination of resources we use to detect and compartmentalise the traffic, the human element is critical. The expertise we have within HAUD is what enables us to develop our class leading tools - whether its specific algorithms designed to detect normal vs abnormal traffic flows, or monitoring SIM locations to detect legitimate P2P messages from disguised SIM boxes installed in vans so they appear to be moving (as real P2P senders usually do.)

2 What are your views on domestic leakage and how much is it impacting the MNOs?

Leakage of any sort is really just a missed revenue opportunity. HAUD's research has shown that in some markets international SMS leakage - traffic that is passing through grey routes and so failing to deliver any revenue for Mobile Network Operators - can be up to 50%.

But to answer this question, we first have to be clear on what we mean by domestic leakage and what is causing it.

Domestic leakage we define as A2P SMS traffic that is being sent to consumers by brands and which ought to be classified as international traffic, but which is instead arriving via domestic routes.

SMS Firewalls like HAUD's Smart NForce can assess, categorise, and monitor SMS traffic coming onto a network, separating the two traffic types (International and Domestic) - allowing the MNO to price messages differently.

However, therein often lies the problem. If the pricing between domestic and international A2P is too great, and in some markets any difference, then traffic will take the cheapest option – and will pass through domestic channels first. MNO's end up seeing international traffic rate drop off and domestic grow – it's a difficult balancing act.

On local or domestic leakage - and by this we mean traffic which we consider to ought to be direct domestic connections - the problem is equally as big and in many ways at the core of the problem.

There's a few interconnected issues here. Firstly, grey route aggregators typically use local entry points into MNO networks to get around international rates. We regularly see OTT international traffic, for instance, that should be coming onto networks and accruing the appropriate international termination rates, hitting networks via local country SIMs. The grey route aggregators even remove the global branding and names from, say, social media giants' messaging, to help the A2P traffic flow onto the network without being identified.

The second issue that compounds this domestic leakage problem is the proliferation of local or in-country all-you-can-eat SMS bundles, or bundles offering thousands and thousands of free SMS messages a month. When you couple these kind of loss-leading subscriber plans, with the increasing sophistication and reduced cost of SIM boxes, IMEI reprogramming and growing ability of grey route operators to evade detection, you can quickly see how the volume of grey route traffic is both hard to manage, detect or stop.

Because it's hard to stop, there's a third issue too - and that is that there is frequently very little enforcement on local rate traffic either.

HAUD's view is that all leakage can be stopped - or at least hugely reduced - and with that reduction will come increased, recurring, revenue. As such, MNO's need a monetization strategy that encompasses all entry points, rather than fragmented. The strategy needs to focus on capturing and maximising the revenue of every message - in an automated way, but which is simple to manage both for the MNO and it's paying-partners.

HAUD'S suite of tools - from our dynamic pricing platform SmartCharge to our SmartXChange direct to brand A2P connection platform - do just that. And our class leading SmartNForce firewall acts as the enforcer on the network - blocking fraud and malicious traffic, while simultaneously capturing the purpose and origin of each SMS so the MNO can be sure it is categorised correctly and the appropriate fees are paid.

We see it as our job to help our partners define the SMS A2P strategy that works best with their overall business strategy, and then to help deliver it in a cost-effective way.

3

In my experience, the main problem lies in the firewall deployment. The MNO doesn't always have all the knowledge, and the firewall is installed, ignoring specific considerations relating to local regulations and the local market. What can MNO's do if the local regulations are against blocking SIM box traffic?

The deployment of firewalls onto networks is still a work in progress. Some 48% of MNOs still don't have them deployed and where they are in situ, an even smaller percentage are the next generation managed firewalls like HAUD's that have greater detection and tracking capabilities.

You'd expect HAUD to say this, but given the need for continuous management, updating and R&D on how to ringfence network entry points with sophisticated, low impact, firewalls, there is significant value in partnerships here. The cost involved in developing an in-house firewall and constantly evolving it, and tracking latest threats and evasion approaches, is expensive. There is obvious cost efficiency in working with a partner with deep knowledge and specialist experience to deliver this. That partner should also be able to help the individual MNOs navigate the regulatory requirements they need to be aware of in any specific country or region.

In terms of regions where regulators don't allow the blocking of SIM box traffic - or rather, the blocking of any SMS traffic, then again as stated above, there are solutions that can help here. HAUD's filters are able to keep track of what is being shared in SMS messages, and to highlight traffic that seems to be either fraudulent, or that is in violation of SIM card policies. In those instances, while we might not be allowed to block the individual SMS messages - we can work to block the SIM cards, or IMEI devices, sending that traffic.

What we've found, after many years of building out our systems, is that you need a multi-layered approach to tackling SIM box traffic. You need a variety of technological solutions and human oversight to identify and stop illegitimate messages - but crucially, you also need the ability to work with regulatory authorities, and indeed other MNOs, to highlight the issue, the problems it causes, and develop combined industry solutions.

48%

OF OPERATORS DON'T HAVE A FIREWALL DEPLOYED *

43.75%

OF OPERATORS USE A BLEND OF MANAGED AND HOSTED SERVICES **

31.25%

OF OPERATORS HOST THE FIREWALL THEMSELVES**

* The impact of fraud on A2P SMS monetisation / Mobilesquared

** Protecing A2P SMS revenues in the roaring 20's / Mobilesquared

4

With the advent of eSIMs, and the ending of the physical SIM card market, will SIM farms and SIM boxes have the same impact as they currently do?

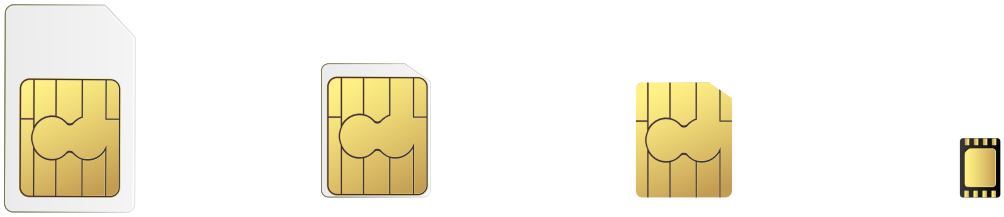
This is a great question, partly because as an industry we are still trying to figure out the answer.

The short answer is that, yes, it will make illegitimate SIM box usage harder. Without easy access to PAYG SIMs, and with more checks on identity before eSIMS are provisioned and usable, SIM box operators are going to find it harder to access networks in ways that are easy and competitive, and which therefore make undermining the legitimate SMS traffic simple. It will also make the job of unprovisioning eSIMs that are being used for illegitimate messaging, much easier too. This, though, does require that all MNOs in each territory or country operate with the same levels of diligence - because as we said above, traffic will naturally end up flowing through the cheapest channel.

However, there are also dangers with eSIMS that still need to be closed off. Again, starting with SIM box operators. Experience suggests that those building SIM box technology, or the operators of the devices, will find creative ways around the eSIM evolution. How and where they will do this is yet to be seen, but certainly there are threats like cloning, identity theft and re-using discarded eSIM enabled IoT devices that have to be addressed.

While over-the-air provisioning of subscriber profiles and allowing all ecosystem participants to connect to an online service might improve usability and convenience, it also opens a door to hacking opportunities that deliver access to private information, trade secrets, and even personal data that can be exposed to a skilled network penetrator and used for fraudulent purposes.

SIM Cards evolution



> Experience suggests that those building SIM box technology, or the operators of the devices, will find creative ways around the eSIM evolution.

Ultimately, it's going to depend on how eSIMs are designed, secured and remotely installed onto devices - and what on-going checks are in place throughout each eSIMs lifetime of use. If there are robust and frequent checks on the identity of the subscriber using the eSIM, then many concerns will be negated. But if this scrutiny isn't put in place, then - coupled with the expected increase in connected cellular devices fuelled by the IoT revolution - the industry will continue to see the same levels of abuse that it currently experiences with physical SIMs.

5 eSIMS are on the way, and RCS is being actively promoted by Google as a replacement for A2P - what will be the impact of all of this on SMS?

Undoubtedly, RCS will become a very important communication channel in the future. It is also clearly being seen both by MNOs, and OTT messaging service users like Google, as a natural development of SMS, given its ability to offer more content-rich communications. With that added complexity come opportunities for more detailed services - from branded experiences to 1-2-1 chat services - and all of this combined with deeper analytics.

But therein lies an opportunity too - and it largely comes back to both pricing and intent. If you are a bank wanting to send a 2FA code, why would you use a more complex system when A2P SMS works well and its relative simplicity makes it efficient and - with the right firewalls on networks detecting fraudulent activity - secure. Time and again we also see open rates for A2P SMS in the 90% region - far above any other form of corporate communication - so it's a channel that works to deliver messages effectively.

We also see open rates for A2P SMS in the 90% region - far above any other form of corporate communication.

So, it will depend on what partners want to do with each message they want to send. For MNOs to be worried, it would suggest they haven't developed their strategy for RCS yet, and are not investing enough into future RCS business cases that they can then monetise. Pricing and standardisation will be the key to RCS' success.

Eitherway, it will be just as critical to future revenue defense, and growth, that MNO's have in place robust firewalls that can monitor RCS traffic, detect fraud and in doing so, protect the security of messaging as a means to communicate with customers and wider audiences.

6

Due to the increasing cost for A2P SMS, many enterprises are moving to in-app notifications. What will be the impact on A2P SMS of this?

Historically, two of the biggest challenges around A2P SMS messaging have always been around pricing and managing the relationships with the brands that want to use SMS as a customer communication channel. The role of aggregators developed in part as a response to this. The core problem is the resource cost in managing both the relationships, the volumes of traffic and then pricing each message being sent according to a variety of factors (size of the brand commissioning it, intent of the message etc etc).

At HAUD, we've developed solutions that address these challenges for MNO, turning them into opportunities by simplifying the relationship model, automating the process and specifically in terms of the pricing issue, enabling more dynamic pricing models.

This ebook is not designed to be a product platform for HAUD, rather as we said at the beginning, a knowledge share - so we won't describe our solutions here, but you can read more if interested on these links: SmartCharge for dynamic pricing solutions and SmartXChange for our direct to brand relationship solution.

SMS is as an universal messaging delivery system – it works on pretty much any MNO network, and doesn't require end users to download specific, additional apps.

It's clear that a combination of these core problems outlined above has led to price increases over the past few years. However it's also clear that the further factor of increased demand for A2P SMS, fueled by new use cases, has also contributed both to the price, and to the operating expenses brands now spend on this form of communication.

Because of this, we have seen brands wanting to avoid the cost (and, who also don't want to pay money into the grey market) and move their messaging into apps - either their own apps or OTT platforms like Viber for Business or Whatsapp for Business. But this proliferation is unlikely to replace SMS in the near to medium future, because of its limitations - either a need for a wifi connection, or strong and stable mobile data signal with the data priced at reasonable rates, two things that are still absent from large parts of the world. Where customers do rely on wifi to connect to their apps for messages, they also run the risk of connecting through malicious public free wifi services, managed by cyber criminals - posing considerable security risks.

SMS is also uniquely placed as a universal messaging delivery system - it works on pretty much any MNO network, and doesn't require end users to download specific, additional apps - something consumers increasingly shy away from given storage limits on devices.

There are other security issues too for in-app messaging, from data theft to whether information is being shared across platforms and to other businesses.

It is likely in-app messaging will take a share of the market - but SMS remains a universal and attractive option.

7 What would you suggest to a small MNO – to forge a partnership with an SMS Firewall provider – revenue share model, or OPEX model?

In general, we believe the revenue share model is the best one - simply because it pushes the firewall provider to continuously build the best systems possible as they are incentivised to support growth in the sector through innovation. It is also more costly, and less of a capex drag, to bring in partner technology.

There are, though, a number of partnership routes open to MNOs looking to bring in expert ring fencing specialists, with typically the return on investment growing as the vendor supports the MNO with SMS monetization, rather than just pure protection. That's partly down to the cost efficiencies of working in a more connected way with MNOs - the more you understand their operating model and IT systems, the more insight you can deliver around areas like revenue defence and new business models.

8 What is the best experience for MNO protection - to have the firewall deployed in the cloud /point of international interconnection, or in the MNO premises directly?

While a cloud implementation is possible, in many cases it would be advisable to implement an on premise implementation. This is because for proper protection and traffic categorisation all traffic sources incoming to the MNO, need to be monitored and controlled including domestic on-net, domestic off-net and direct connections (SMPP).

In many cases it is also not feasible or possible, to route such traffic outside of the MNO network. In many countries, regulation dictates that traffic is not allowed to be sent outside of the country to be processed, monitored or sent.

9 What are the most important characteristics for a 'good' firewall solution?

A good firewall solution should do a number of things.

It should protect your network against illegitimate or fraudulent traffic - helping to block spam, SMShishing, unwarranted marketing, malicious content and other threats. By doing this it gives customers a better UX, which helps build brand loyalty and also reduces opex-costs around call centre complaints etc.

It goes without saying, but firewalls should be able to protect across varying types of protocols, including SS7 and Diameter. It also has to work across messaging formats - for example, the solution should be able to live monitor and filter Unstructured Supplementary Service Data (USSD) messaging, and test the veracity of these messages. →

The second thing a good firewall should do is support both revenue defence and revenue growth - and it should do this in a number of ways.

To start with, it should be able to not just detect illegitimate traffic and block it, but should also be able to spot SIM boxes in operation by identifying the SIM cards that are sending that traffic and communicating offending MSISDNs to the operator. Latest generation firewalls, like HAUD's SmartNForce also have the functionality to block the SIM cards - with the operators consent - themselves both on-net and off-net.

By blocking grey route traffic, it enables the MNO and its partners to draw more revenue from increased legitimate traffic on the network. When grey routes are shut down, both aggregators and MNOs benefit from redirected traffic onto direct routes.

Added security around messaging delivery should also be used to help push new A2P messaging user cases - offering brands new opportunities to connect with their customers, and for MNOs to attract more business - and therefore more revenue.

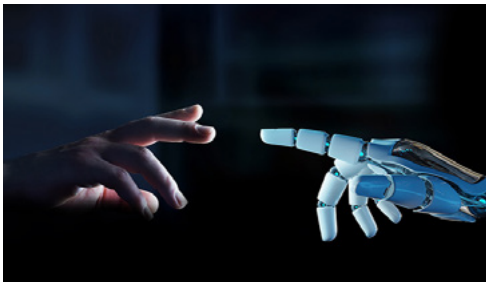
A great firewall solution should also work in unison with other defence capabilities the MNO might have or need. Smart NForce Signalling firewall solution integrates with the MNO's core network elements to provide comprehensive signalling protection on all the SS7 network security and Diameter operations and commands over internal, interconnect and international links.

You also need your firewall to be able to offer up analytics and diagnostics in real time, enabling you as the operator to quickly and easily see what traffic is moving across your network, and where you can take steps to optimise things. For example, by categorising the traffic partners are pushing onto the network, the MNO can be assured they are properly monetising the access they give.

However lastly, the key thing a good firewall solution needs is great management - humans ensuring the patterns spotted are right, updating protection algorithms, reporting back to the business on performance and optimisation.

10 Are there any AI or machine learning tools available within the firewall and monetization system at the moment?

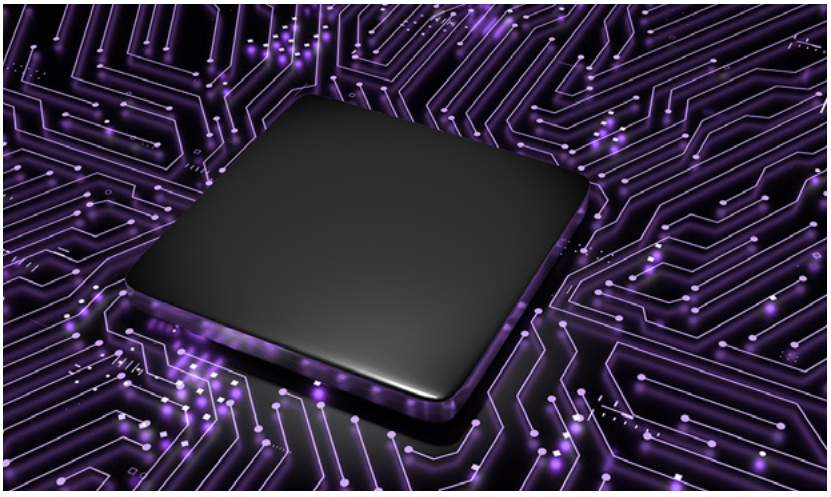
AI is used extensively - at least in HAUD's firewall solution - to help with detecting keywords and spot irregular patterns of usage that can identify, for example, where SIM boxes are being used. AI is a great tool for this, as it has the immediacy in response time to support MNOs to remove bad content from their networks before it makes it to the end user. Of course, as with all machine learning tools, the effectiveness of AI firewalls solutions still largely depends on the humans behind the technology - ensuring the correct algorithms are in place and adjusting search terms to meet the latest threats.



In short, right now, AI and ML are working as great tools for detection mostly, however we still feel that the human element is advisable for decision making when it comes to implementation of control rules on the traffic.

11 What technological developments are going to impact the A2P market in the long term?

We've already outlined a little of how AI and ML are being used in protection of the SMS ecosystem. However there many more areas where these technologies will prove themselves in the coming years - from natural language systems to supporting advanced marketing campaigns.



Some operators are already testing the ability for quantum computers to help in functions like real-time network optimisation for 5G traffic

Gazing a little way into the future, quantum computing has the potential to shake up the A2P industry quite dramatically. Some operators are already testing the ability for quantum computers to help in functions like real-time network optimisation for 5G traffic - helping increase network stability and giving end users a better mobile data experience. In the A2P space, certainty the algorithmic ability of qubits in areas like encryption will help secure both networks (preventing any eaves dropping, for example) and the messages being sent across them. Any reduction in fraud will be greatly valued.

Blockchain usage is also taking foot in the industry. Specifically, it can allow for smart contracts between groups of operators - stabilising the supply and demand issue. Although, there remain issues here around the scalability of these systems, and the speed with which transactions can be logged onto blockchain contracts.

12

Would you say that MNOs are becoming greedy now to recover their past years of lost revenue, and are spiking rates beyond market-acceptable rates? If yes, what will be the impact of this behaviour on the A2P industry overall?

Greedy is going too far. MNO's are increasingly seeing greater monetary value in A2P SMS, and accordingly are trying to secure their share of the revenue. The value A2P delivers to both brands and their customers is reliant on the networks the operators manage, build and develop - so it is entirely appropriate that they see adequate ROI on their spend.

There remains a question around pricing - and certainly in most cases A2P SMS is still more expensive than either email or in-app messaging services. However there are reasons for that - not least the security of the system and the engagement levels customers have with the service. Certainly if there was more pricing elasticity in the fees MNOs charge, then there could be more use cases and therefore more opportunities to optimise revenue without increasing prices. And, as we mentioned at the start of this ebook, when it comes to domestic leakage, close parity between domestic and international rates should help reduce any revenue loss from this area.

HAUD believes the future for A2P SMS is strong and likely to grow, but with that growth comes the opportunity for MNOs to work smarter around pricing strategies - and specifically utilising more dynamic pricing that relates more closely to both the sender of the message and its content. If MNOs can get that right - and here partners like HAUD can definitely help with solutions that make the process less resource heavy - then fees and chargers can be adjusted to ensure no-one is priced out of the market and that instead it thrives.

Stay in control

HAUD generates revenues for mobile operators from recoverable A2P traffic while eliminating fraud and spam traffic, maximising network performance and reducing subscriber churn.

HAUD
STAY IN CONTROL

GET IN TOUCH

WEBSITE: haud.com
EMAIL: sales@haud.com
LINKEDIN: @haud

HAUD SYSTEMS LTD

230, First Floor,
Eucharistic Congress Road,
Mosta, MST9039
Malta

OFFICES WORLDWIDE

Singapore
Jakarta, Indonesia
London, United Kingdom
Upsala, Sweden