Secure Networks Key to A2P Monetisation

SMS firewalls: the first step in unlocking A2P revenue potential

A whitepaper by

mobile squared

Sponsored by

tyntec

Contents

Executive Summary

This Whitepaper sets out to identify the A2P SMS opportunity for mobile operators. Findings are based on an online mobile operator survey and one-to-one interviews with the A2P SMS community. All data and research in this Whitepaper is from mobilesquared unless stated otherwise.

Key stats

- Majority of mobile operators are experiencing year-on-year A2P growth of between 6%-36%.
- More mobile operators have experienced A2P messaging traffic growth in the last 12 months (surveyed in Sep. 2015) compared to the same period in 2014, with 56% of mobile operators reporting an increase compared to 49% over the prior 12 months.
- Less than 25% of mobile operators have deployed an SMS firewall since 2012.
- Grey routes account for two-thirds of A2P SMS traffic; meaning only one-third of A2P traffic can be monetised by mobile operators.
- The most popular near-term monetisation strategy identified by mobile operators is domestic and international A2P SMS, followed by phone number portability and verification information, Internet of Things and M2M, and lastly A2P messaging via operator-owned OTT apps.
- Mobile operators consider spamming the greatest threat to their networks, followed by spoofing, and virus distribution.
- Two-thirds of mobile operators using SMS firewalls reported a huge reduction in unauthorised messaging traffic.
- The main driver for mobile operators considering SMS firewall deployment is network security, anti-spam and fraud prevention, ahead of A2P messaging monetisation opportunities.
- Primary criteria for mobile operators selecting an SMS firewall solution are operational simplicity and performance. Secondary criteria include total monetary cost (initial investment and recurrent cost over the lifetime of the firewall) and total cost (total monetary cost and cost of internal set-up and operation).

The bigger picture

- Mobile operators are undergoing brand consolidation and endeavouring to protect their brand reputation by focusing on reducing spam on their networks and maintaining healthy subscriber relationships. This strategy is ultimately paving the way for explosive “clean” and “legitimate” A2P messaging growth.
- Mobile operators need to expand their OTT monetisation focus to include the broader enterprise A2P SMS opportunity.
- Enterprises are learning how A2P messaging can be successfully used to drive customer engagement, and beginning to explore various possibilities.
- Mobile operators are slow to capitalise on A2P opportunities, as grey routes still dominate the space. This indicates A2P messaging is still a nascent, even immature, market.
- Mobile operators can now see the return of investing in SMS firewall to ensure legitimate A2P traffic is delivered to their customers.
- By closing grey routes, and upgrading their SMS firewalls, mobile operators are opening the doorway to unlocking the potential of A2P enterprise messaging.

Less than 25% of mobile operators have deployed an SMS firewall since 2012

Introduction

Mobile network operators (MNOs) are starting to see beyond their narrow focus on protecting their messaging revenues from the OTT messaging apps, and targeting the entire enterprise A2P SMS opportunity.

The likes of Facebook Messenger, WhatsApp, WeChat, LINE — are just a few of the hundred messaging apps now available — that have been eroding away at MNO P2P SMS traffic, and therefore prompting MNOs to explore ways of monetising OTT traffic. Meanwhile the rise of enterprises using SMS to communicate and engage with customers has created a multi-billion dollar market.

Today the A2P SMS industry is worth around $55 billion[1] and projected to be worth $60 billion[1] by 2018, yet mobile operators are only monetising an estimated one-third of that revenue, possibly less given the uncertainty surrounding the volume of illegitimate A2P SMS traffic.

Part of the reason for this uncertainty is that the A2P SMS traffic is divided into three streams: white route traffic, black route traffic and grey route traffic. In short, white route traffic is based on a direct route for the SMS traffic with a set price — as opposed to black, which is indirect and illegitimate and grey, which is somewhere in between (for complete definitions see box, page 5). Importantly, both black and grey routes do not require pricing agreements and suppliers can effectively set their own cost-per-SMS rate.

Outside of white route traffic — with its pre-set termination agreement — it is impossible for MNOs to bill for SMS traffic. In the absence of such agreements — as is the case with grey and black route traffic — MNOs have no visibility regarding the SMS traffic terminated on their network.

Without implementing SMS revenue assurance platforms and SMS firewalls, MNOs cannot monetise SMS traffic and remain open to illicit traffic, spam, and other SMS-based attacks. However, that does not mean MNOs do not use grey routes themselves when there are no viable alternatives to make interconnectivity work. But to fully realise the potential of A2P SMS, white routes are the only monetisation option for MNOs.

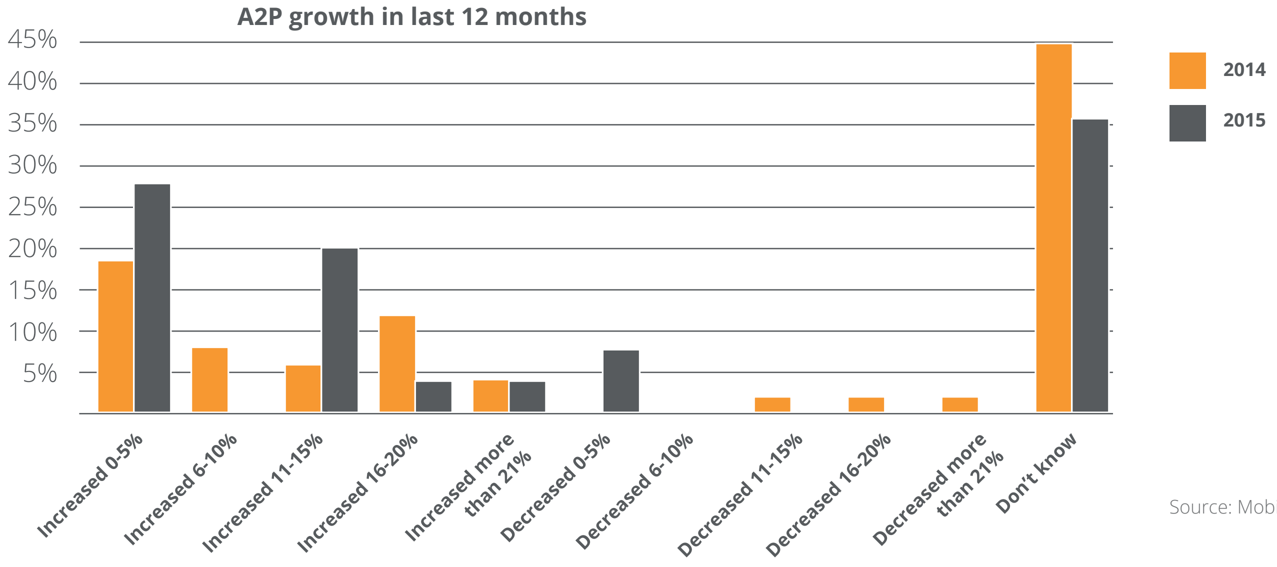
Presently it is the SMS aggregators that are capitalising on the A2P SMS opportunity, by purchasing the SMS traffic wholesale from mobile operators and monetising it via either white or grey routes. Tier 1 aggregators often have direct connections to the SS7 network enabling them to provide a quality of assurance (white route traffic) matched only by the mobile operators themselves. Aggregators without such assurances will typically pursue grey routes.

The implementation of SMS revenue assurance platforms and SMS firewalls has decreased A2P SMS traffic over grey routes. However, even today grey route traffic accounts for approximately 65% of total A2P SMS traffic[2].

[1] Source: Juniper Research

[2] Source: Mobilesquared research 2015

Grey route traffic accounts for approximately 65% of total A2P SMS traffic



Source: Mobilesquared

What are white, black and grey routes?

White routes are when both the source and the destination have entered into a termination agreement covering both price and traffic. This can be between two mobile operators, or a mobile operator and an aggregator (typically Tier 1) acting as a hub to other mobile operators. White routes represent direct connections providing reliability ideal for time-critical communications, and in the wholesale and bulk-messaging world of A2P, typically command a termination fee.

Black routes are illegitimate. They lack any agreement from either the source or destination and SMS traffic via such a route is deemed illicit. These are indirect connections, without reliability, and massively undercut white route cost-per-SMS rates.

Grey routes represent a middle ground between white and black routes, with one official connection at either the source or destination. Grey routes deliver low-cost international messaging via indirect, non-interconnected routes, and are primarily used by low-cost SMS aggregators (Tier 2 & 3). Typically, an A2P SMS supplier will use an MNO-to-MNO P2P SMS route for A2P SMS traffic. Consequently, only destination MNOs with a termination agreement will generate revenues, those MNOs without will experience revenue leakage. Grey routes have emerged as MNOs separate A2P from P2P traffic commercially, which is why this type of route is not considered white.

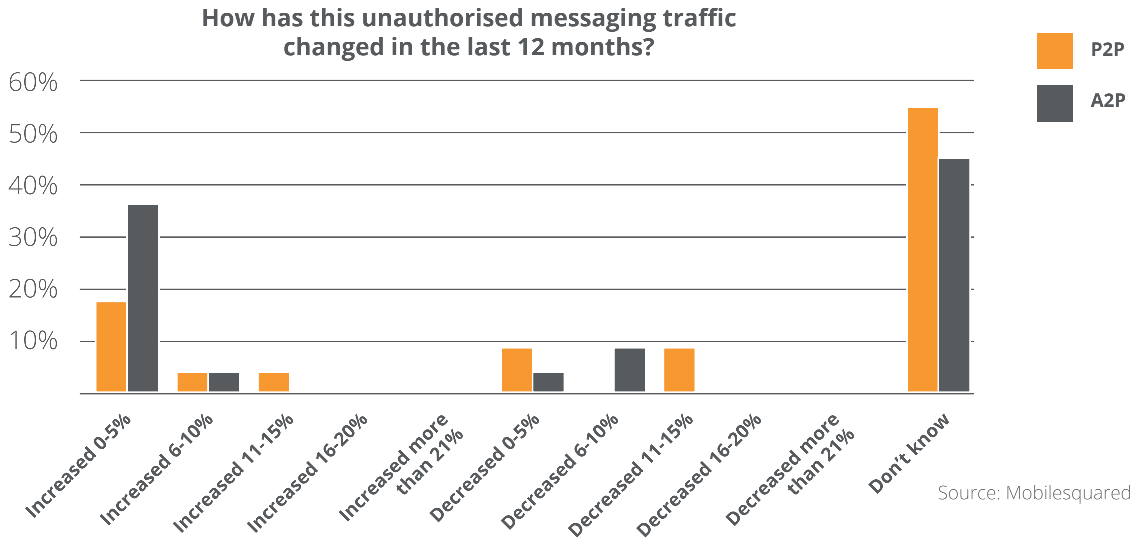
<25% of MNOs have invested in the necessary SMS firewall required to transform grey routes into white routes

The high grey route traffic is not surprising considering it's estimated that less than one-quarter of mobile operators have invested in the necessary SMS firewall required to transform unauthorized grey routes into authorized white routes[3].

Most responding to the 2015 MNO survey believe the majority of their P2P and A2P traffic comes from an authorised source. For example, 23% of MNOs believe that 90% or more of their P2P traffic is authorised, compared to 54% for their A2P traffic. Also, less than one-fifth of MNOs believe that their network did not carry any unauthorised A2P messaging traffic. That leaves just over one-third of mobile operators unaware of any potential unauthorised A2P messaging traffic (see chart, *What percentage of your messaging traffic is from unauthorised sources?*).

In light of the market data outlined above, these MNO responses clearly highlight a disconnect with the reality of A2P traffic.

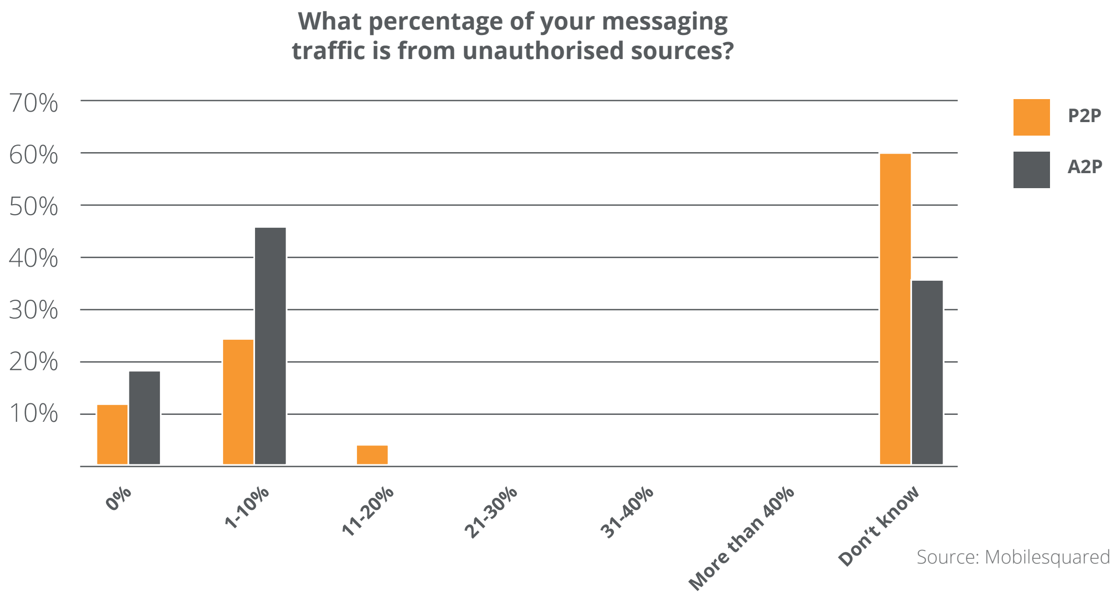
MNOs' lack of understanding in their A2P traffic was also prevalent when the survey asked how unauthorised messaging traffic had changed over the last 12 months. Just over one-third of respondents claimed to have experienced an increase in unauthorised A2P messaging traffic, with most citing an increase of 1-5%.



Source: Mobilesquared

[3] Source: Mobilesquared research 2015

Looking beyond OTT



Source: Mobilesquared

Almost one-fifth of mobile operators believe that unauthorised P2P messaging traffic had decreased. But the majority of mobile operators did not know whether their unauthorised A2P messaging had changed or not over the last year, once again highlighting the lack of MNO visibility into A2P traffic (see chart page 6, *How has this unauthorised messaging traffic changed in the last 12 months?*).

Within three years mobilesquared estimates that the A2P SMS market could grow to more than half the size of the P2P SMS market, possibly larger assuming MNOs can have greater visibility into their traffic data by using next-generation firewalls. So the time is now for MNOs to attain that messaging visibility.

Given that the discussion around grey routes has been prevalent since 2012, it remains baffling that three-quarters of mobile operators have yet to act[4]. Especially given that the mobile operators that have deployed SMS firewalls enjoyed multi-million dollar returns on their investment[4].

MNOs looking beyond OTT to bigger A2P opportunity

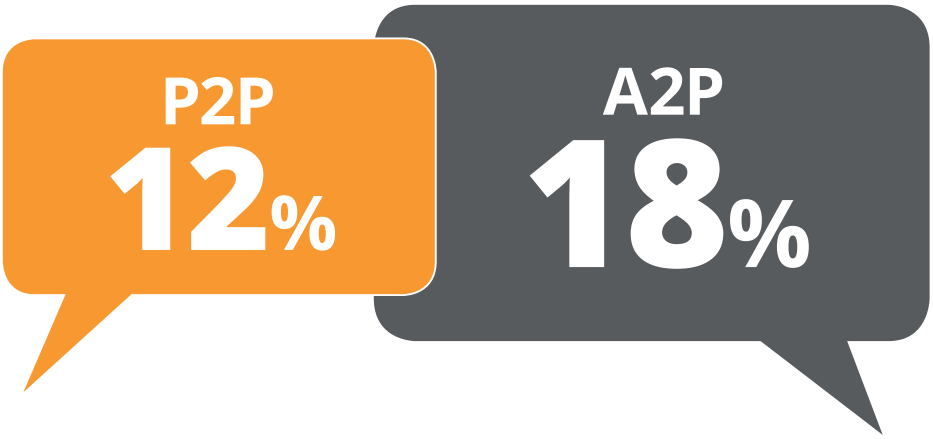
There are a number of explanations as to why MNOs have been slow to jump on the A2P SMS bandwagon. Theses include hampered decision-making due to having messaging teams across multiple internal divisions, staffing shortages, simply failing to prioritize A2P, and an unwillingness to invest in messaging infrastructure. However unfortunate timing could also be to blame.

The unfathomable popularity of OTT messaging apps forced mobile operators to try a multitude of strategies to combat the growth of OTT services and protect their P2P

[4] Source: Mobilesquared industry research 2015

MNOs have been focusing on protecting P2P messaging revenues [and not] driving the A2P messaging opportunity

Percentage of mobile operators reporting that they carry authorized A2P traffic only



messaging revenues. By 2011-2012 the tactics employed by MNOs ranged from blocking OTT traffic or introducing an OTT-related data usage tariff, developing their own white-label OTT-based offering, to looking to provide an advanced range of messaging services, such as SMS forwarding, SMS signature, and SMS blacklist for unwanted SMS.

In 2012-2013 the strategies included ways of capitalising on the OTT communications opportunity, such as OTT-to-SMS on-net termination and, more recently, efforts to partner with OTT providers.

In 2014 mobilesquared research revealed that three-quarters of mobile operators claimed to have had an OTT communications strategy in place. But did this OTT mobile operator strategy come at a price? That price being their delayed entrance into the enterprise A2P SMS space.

Around the same time in 2012 when mobile operators were intent on facing their OTT competitors head-on, the key to unlocking the multi-billion A2P SMS opportunity was introduced. The 2015 A2P industry research points to 2012 as the year when the first next-generation SMS firewall (or filter) was launched, with the capability of detecting grey route traffic and illicit types of SMS traffic. (The inference here is that SMS firewalls developed before 2012 are incapable of providing the message visibility required.)

Therefore, MNOs have suffered from a misallocation of resources, focusing on protecting P2P messaging revenues as opposed to driving the A2P messaging opportunity.

But with billions of dollars in the offing, it's never too late.

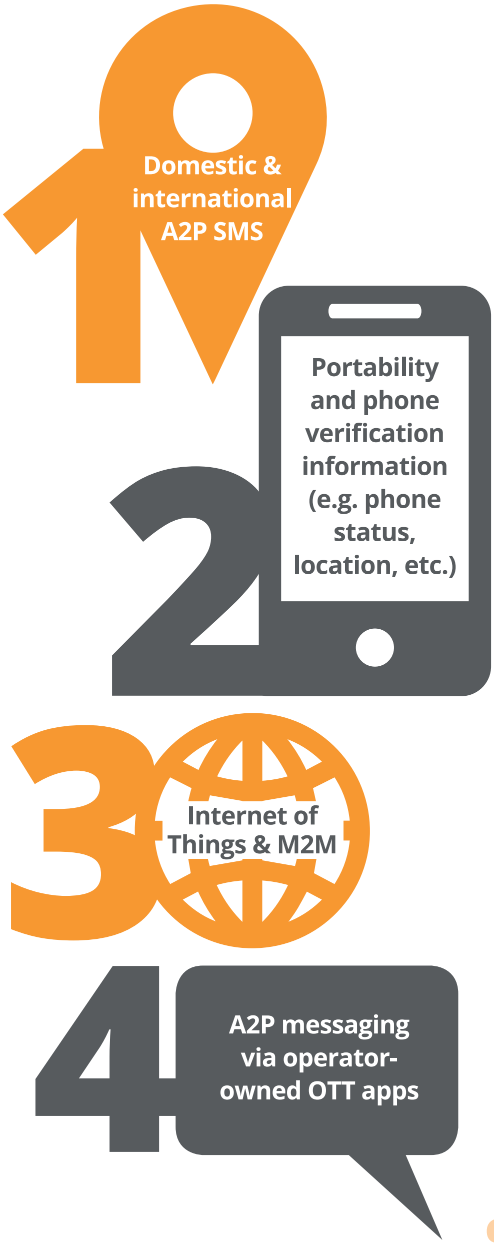
Unlocking A2P

Unlocking the A2P goldmine

A reflection on this shift in the MNO mindset — beyond OTT to include enterprise A2P — is highlighted by the fact that the most popular near-term monetisation strategy identified by MNOs surveyed was domestic and international A2P SMS, followed by phone number portability and verification information, Internet of Things and M2M, and lastly A2P messaging via operator-owned OTT apps, based on the four monetisation models outlined in the research (see chart, *Which monetisation strategies will be the most relevant for you in the next 12 months?*).

Mobilesquared research reveals that the number of mobile operators to have either introduced or updated an SMS firewall in the last 3 years is anywhere between 100-200[5] — and like the markets they are addressing, this figure is a little "grey". Regardless, even at 200 this figure still leaves more than three-quarters of the approximately 850 mobile operators around the world yet to address their revenue leakage via grey routes and alternative illicit SMS traffic. But change appears imminent as MNOs looking to invest in their messaging infrastructure. By 2017, it is forecast that the messaging security gateway market will be worth almost $375 million[6].

Which monetisation strategies will be the most relevant for you in the next 12 months?


1
Domestic & international A2P SMS
2
Portability and phone verification information (e.g. phone status, location, etc.)
3
Internet of Things & M2M
4
A2P messaging via operator-owned OTT apps

[5] Source: mobilesquared industry research 2015

[6] Source: Infonetics Research

SMS Channel

SMS is the channel that keeps on giving

SMS has become something of an anomaly within the telco space, as its much-heralded and anticipated demise has yet to materialize. Based on the findings of the MNO survey, 52% reported that their P2P traffic had actually increased over the last 12 months, up from the 39% of MNOs experiencing P2P SMS growth in 2014.

On the whole, the SMS market is in better health than the mobile industry suggests. The global SMS market was worth around $113.5 billion in 2014 and is only expected to fall to $112.9 billion by 2019[7]. In developed countries where smartphone penetration is high, messaging apps are abundant and clearly impact MNO messaging revenues as peer-to-peer traffic migrates from SMS onto IP. But in developing markets P2P SMS traffic continues to grow.

Given the stats associated with SMS — including mobilesquared's own finding that 90% of all messages are read within 3 minutes[8] — not to mention the fact that SMS has total mobile ubiquity, it should not come as a surprise that enterprises[9] are rapidly adopting SMS as a means to communicate with customers across all verticals — including financial, retail, health (and medical), food and drink, logistics, entertainment, utilities, transport, gaming, broadcast and so on.

Most noticeably, 56% of MNOs surveyed in 2015 identified growth in A2P traffic over the last 12 months, compared to 49% of respondents in our 2014 survey. Even disregarding the organic growth in enterprise SMS, by deploying an SMS firewall and converting grey route traffic into white route traffic, each individual MNO is unlocking the A2P traffic potential that already exists within their network.

Estimates indicate A2P SMS accounted for 24% of total messaging traffic in 2014[10]. The number of A2P messages sent each day is already in the billions and projections place A2P traffic at 1.99 trillion by the end of 2015, 2.12 trillion in 2016, and 2.21 trillion in 2017, by which point it will represent 31.3% of total messaging traffic[11].

Based on 2015 A2P traffic estimations of 1.99 trillion, each of the 3.76 billion[12] mobile subscribers around the world will receive on average 1.45 A2P SMS messages per day this year. Which in relative terms seems incredibly low.

In fact, research into the A2P messaging space revealed that retailers, for example, were under-utilising the messaging medium based on the number of messages opt-in users would welcome from their favourite retailers[13]. This research ultimately revealed that mobile users welcomed communications from companies provided there is a value exchange, which could take the form of a discount or voucher from a retailer or restaurant chain, or information about a delivery, or an appointment reminder. As companies become more accustomed to communicating via SMS, their propensity to send messages to their customer database should increase exponentially.

[7] Source: Juniper Research [8] Source: Mobilesquared 2010 [9] For the purposes of this Whitepaper "enterprise" is the catch-all term for brands and companies of all sizes [10] Source: Ovum [11] Source: Ovum [12] Source: GSMA Intelligence Sept 2015 [13] Source: Mobilesquared client research 2013

Security Threats

From an MNO perspective, the time is now to make the necessary investment in order to maximise revenue generation potential from this boom in enterprise A2P activity in the long term.

But there is a need to remain vigilant. As one challenge is quashed, others emerge, highlighting not only the dynamism present within the grey route market, but also how MNOs need to keep up with the evolving tactics adopted by these rogue companies. The A2P SMS sector has very few barriers to entry, especially if a company intends to operate over grey (or black) routes. And now alternative options are emerging as these grey routes become closed.

SIM farms

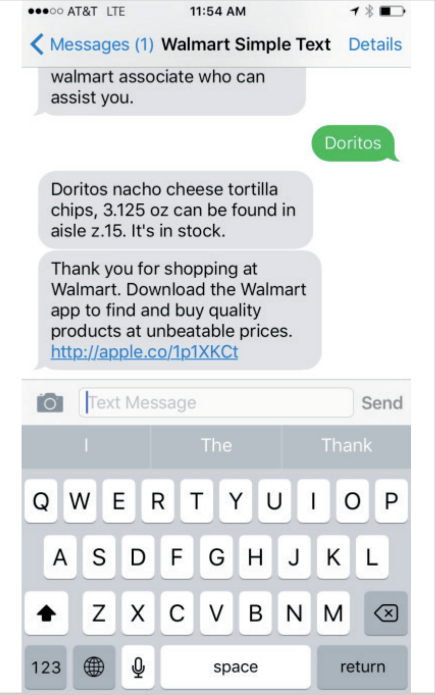
A consequence of grey routes being closed down and businesses intent on getting their messages to the end user are SIM farms. Not surprisingly, SIM farms have become associated with illicit activity, not just spam, but non-compliant activity such as malware and virus distribution, primarily because they can provide a cost-per-SMS at virtually no cost.

This is possible by loading hundreds of consumer prepaid SIM cards — typically with unlimited SMS — to a computer system hooked up to a server connecting to a mobile network. SIM farms will look to exploit the unlimited SMS capability of each SIM card

Walmart Simple Text

Walmart Simple Text helps users easily navigate through and find items at their local Walmart store. By texting a simple “Hi” along with a keyword search term to a specified phone number, users can receive the exact location of the product they are looking for and information on whether it’s in stock. If the user needs any additional help, Walmart Simple Text can connect you with a store representative — all through SMS.

The retailer believes that Walmart Simple Text could potentially transform the way its customers shop by providing them with a convenient, faster service that not only saves them time, but also makes their shopping experience more enjoyable.



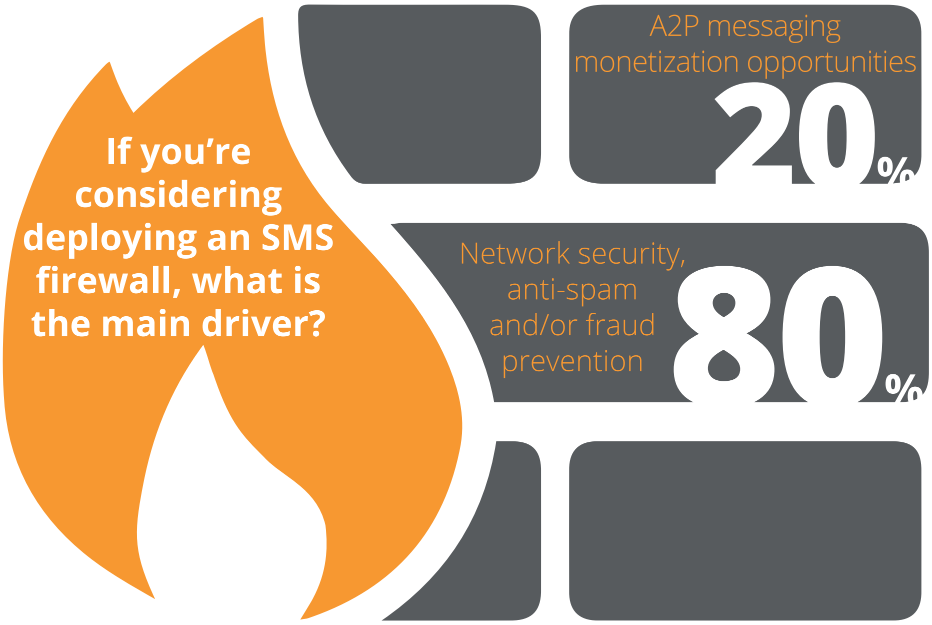
walmart associate who can assist you.

Doritos

Doritos nacho cheese tortilla chips, 3.125 oz can be found in aisle z.15. It's in stock.

Thank you for shopping at Walmart. Download the Walmart app to find and buy quality products at unbeatable prices. http://apple.co/1p1XKCt

80% of MNOs state network security, anti-spam and/or fraud prevention as their number 1 driver



Definitions

Spamming Unwanted messages delivered to subscribers

Flooding Massive amount of messages sent to nodes and subscribers

Faking The illegal use of SMSC identity by a foreign system

Spoofing Messages sent illegally by simulating a roaming subscriber

Smishing Deceptive messages attempting to acquire subscriber information

Virus distribution Messages luring subscribers to a download site with viruses

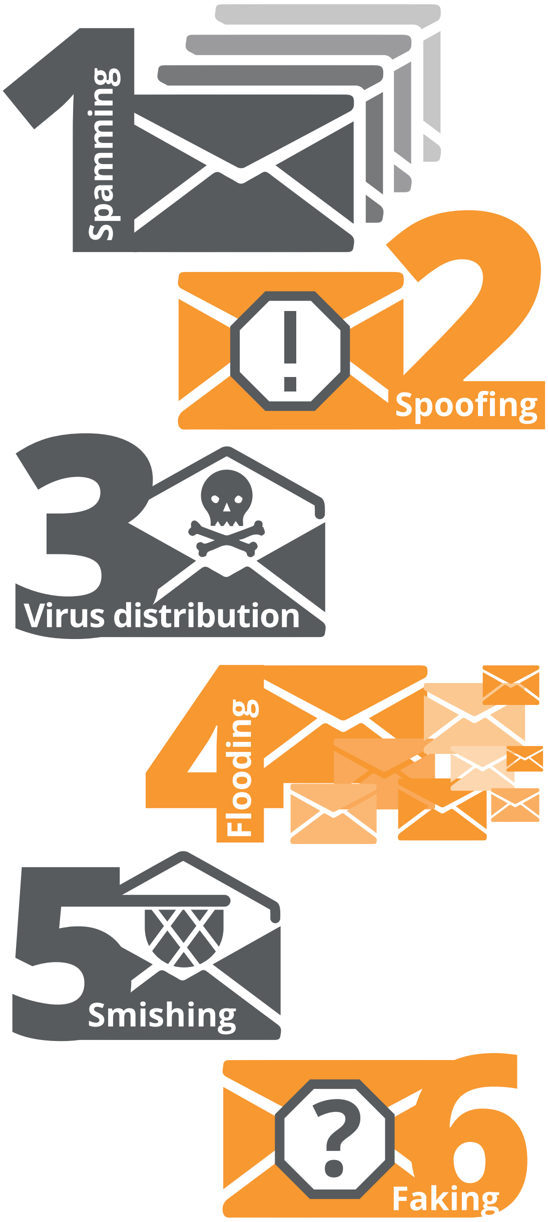
MNOs need to keep up with the evolving tactics adopted by rogue companies

until it becomes blocked by the MNO, at which point the SMS farm will simply replace it with a new SIM. This means attempts by MNOs (and some Tier 1 aggregators) to block are short-term at best, as it is literally days until the SIMs are replaced.

Anyone operating a SIM farm will be in breach of the "fair usage" policy allocated to every SIM card by the MNO, but a savvy SIM farm operator will look to run illicit SMS campaigns below the MNO threshold set for consumer SMS activity to remain undetected.

Ultimately, SIM farms do not have the infrastructure and therefore do not have the redundancy to deal with thousands upon thousands of messages, unlike a legitimate SMS provider. For the delivery of illicit messages, the poor reliability and delivery failure by SIM farms will not impact the company funding the activity. For an enterprise, it's a different story. And like an MNO, spam and a bad user experience, can be very damaging for the brand.

What is the greatest threat from messaging to your network?



Two-thirds of MNOs measure the success of the SMS firewall by the level of unauthorised messaging traffic it blocks

Spam, spoof and virus

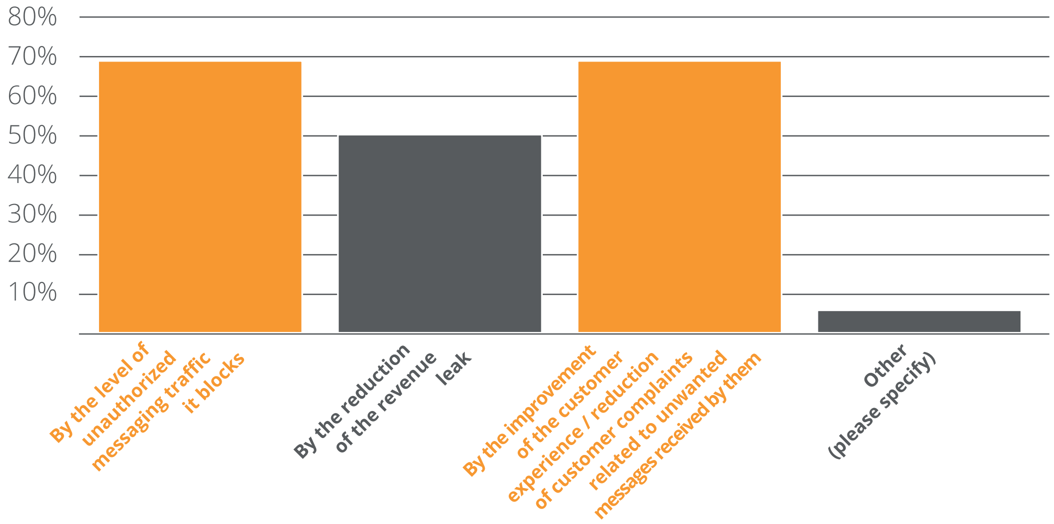
While A2P presents a tremendous opportunity for MNOs, not surprisingly, they are also concerned about the impact this will have on their network. Their number one concern is spamming which they perceive as the greatest network threat, followed by spoofing, virus distribution, and then flooding. The illegitimate activities viewed least threatening, though equally as damaging for any mobile operator should this occur over their network, are smishing and faking (see chart, *What is the greatest threat from messaging to your network?).*

Spam has also caught the eye of the regulators in a number of markets. Indeed, the 2015 MNO survey revealed complying with regulatory requirements as another driver for deploying an SMS firewall.

In India, to support the initiatives introduced to limit spam by the Telecom Regulatory Authority of India (TRAI), it was mandated for MNOs to deploy SMS firewalls. TRAI has tried on numerous occasions since 2011 to limit the number of spam messages to 100 per SIM, per day.

While SMS spam has now dropped considerably below that threshold, research reveals that the spam traffic in India has migrated from SMS onto IP-based messaging, and WhatsApp in particular. Similar efforts to thwart SMS spam were made in 2013 by the Federal Trade Commission in the US, and the Ministry of Industry and Information Technology (MIIT) in China.

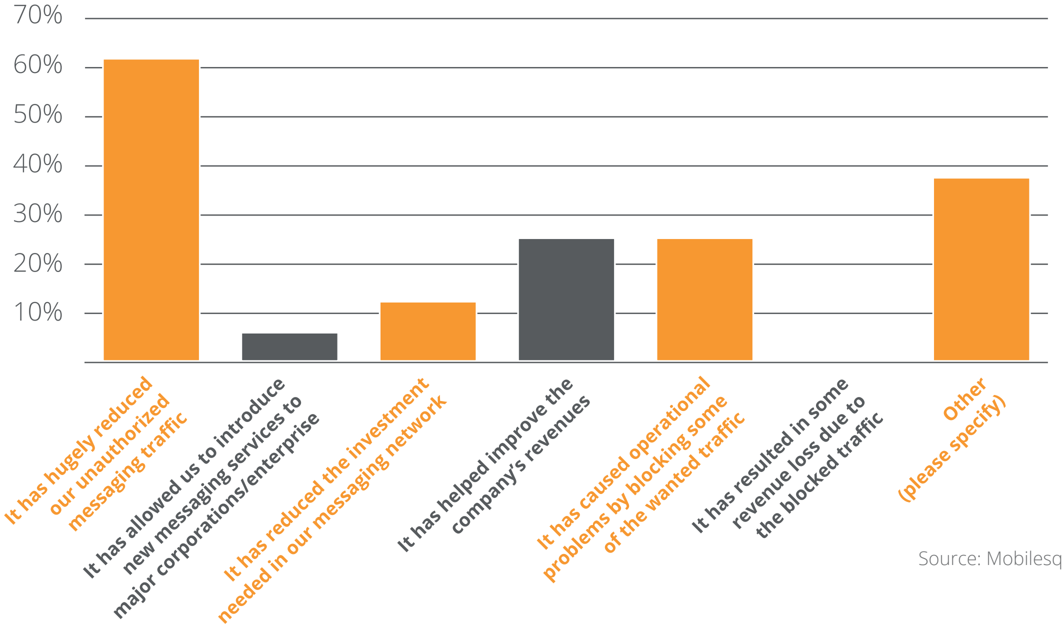
How do you measure the success of your SMS firewall?



Source: Mobilesquared

Firewall Impact

What impact has the SMS firewall made to your SMS business?



Source: Mobilesquared

In 2013, it is estimated that more than 300 billion spam messages were sent, with the average mobile user receiving at least one per day.

The lessons emanating from India should provide a stark warning to the rest of the world: Spammers find a way. And any evolutionary roadmap for firewalls must look to incorporate OTT messaging apps, such as WhatsApp, as their spam permeates into other markets including the UK.

Protecting subscribers from unwanted messages is critical to every MNO, especially as they enter a period whereby enterprise A2P SMS traffic is likely to overtake P2P SMS traffic, and potentially open the floodgates to spamming which could damage the MNO's brand in the short-term and cost it subscribers in the long term, not to mention the credibility of SMS as a communications channel. Spam associated to an enterprise can be equally damaging. For both sectors, it can impact revenues and increase complaints to contact centres, among other issues.

Measuring success

Regardless of when an MNO adopted an SMS firewall, presently two-thirds measure the success of that SMS firewall by the level of unauthorised messaging traffic it blocks, and the improvement of the customer experience as well as the reduction of customer complaints related to unwanted messages received. The reduction of the revenue leak is viewed as a secondary issue for the majority of mobile operators, further accentuating the MNO concern relating to spam.

Network security is the main driver for MNOs considering implementing an SMS firewall within the next 12 months

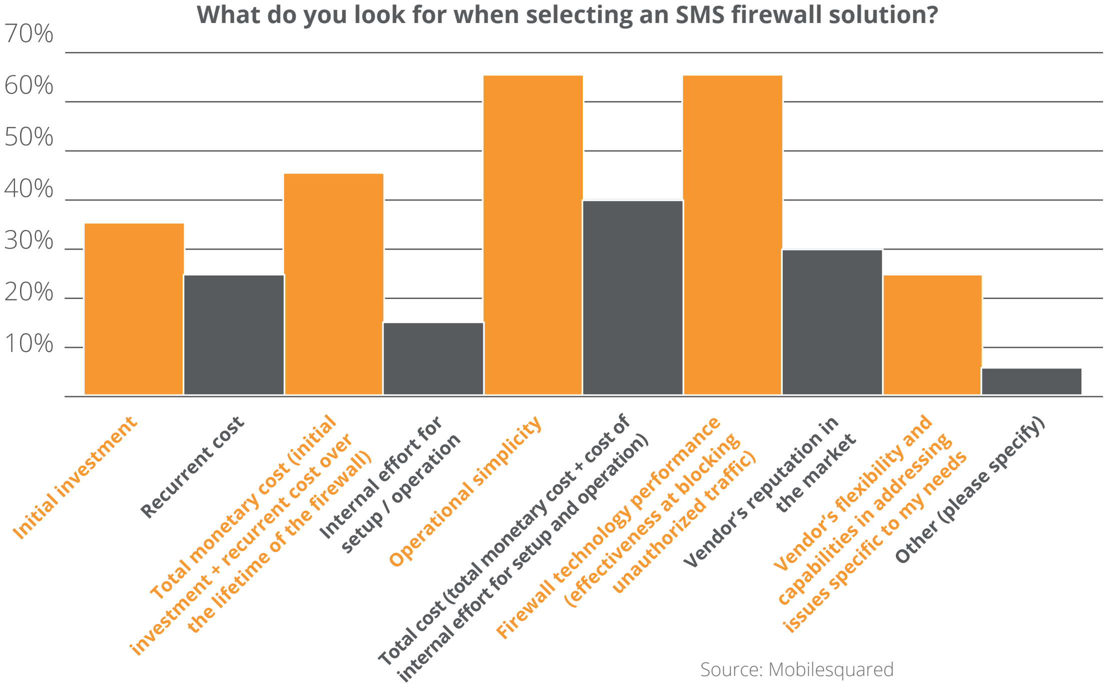
In fact, two-thirds of MNOs claimed their SMS firewall had hugely reduced unauthorised messaging traffic, regardless of whether it was deployed within the last 3 years or not. One-quarter of mobile operators claimed the deployment of an SMS firewall had improved the company's revenues, while the same percentage stated that the SMS firewall had caused operational problems by blocking legitimate messaging traffic.

Of those mobile operators that have deployed an SMS firewall, the research revealed that based on the criteria of blocking unauthorised traffic, reducing revenue leakage, and improving customer experience, they would score their providers 3.6 out of 5.

Of those MNOs that would consider implementing an SMS firewall within the next 12 months, the main driver is network security, anti-spam and fraud prevention, ahead of A2P messaging monetisation opportunities, as this is usually considered a consequence of controlling the traffic.

The main criteria upon which MNOs will base their selection for an SMS firewall solution are operational simplicity and firewall performance, followed by the total monetary cost (initial investment and recurrent cost over the lifetime of the firewall) and total cost (total monetary cost and cost of internal effort for set-up and operation).

What do you look for when selecting an SMS firewall solution?



Source: Mobilesquared

Conclusion

Mobile network operators are in protection mode. As the findings of the 2015 MNO research reveal, they are taking stock of their core assets, with particular focus on securing their networks and preserving customer relationships.

The secure and reliable nature of the MNO networks is attracting the business community intent on driving customer interactions through communication channels such as A2P SMS traffic. But the majority of this traffic is not being monetised by the MNOs. Presently, 75% of MNOs cannot convert that traffic into revenues.

In recent years, MNOs have been focused on countermeasures against OTT players, but to capture the total A2P opportunity they must address the entire market of which enterprise A2P messaging presents even bigger potential.

In order for MNOs to seize the total A2P opportunities, they must put security in place to provide messaging traffic visibility, and the level of control necessary for changing needs.

By deploying next-generation firewalls, MNOs can secure their networks and generate revenues from legitimate A2P use cases. However, deployment of the infrastructure alone will not deliver the full revenue potential, it will require constant vigilance to keep pace with ever changing security threats — and partnerships to implement new business models for A2P monetization.

Methodology

Research was conducted by mobilesquared during August and September 2015. Primary research involved an online survey of 25 mobile operators, and interviews with the A2P messaging ecosystem. This was supplemented with secondary and tertiary research (primarily online based), and mobilesquared's in-house market data.

Job titles of respondents partaking in the 2015 research include: Support Manager Messaging Services, Customer Strategy Manager, DGM VAS, Director OTT Partnerships and Application Development, Senior Engineer, Director of Product and Services, Director Core Network and VAS, SMS Manager, Marketing & Strategy Director, Head Data and Device Partnerships, Strategic Partner Director, Customer Value and Intelligence Specialist, Principal Strategist, Voice & Data Product Manager.

This is the fifth year mobilesquared has run the mobile operator OTT/messaging research. The first wave of mobile operator research was conducted in 3Q2011. The research in this Whitepaper is based on on-going research involving mobile operators representing over 70 markets.

About us

tyntec

tyntec is a telecom-web convergence company that connects the immediacy and convenience of mobile telecom with the power of the Internet. Partnering with mobile network operators around the world, tyntec enables enterprises and Internet brands to power their applications, authentication, and mission-critical communications with universal mobile services such as SMS, voice, and phone numbers in the cloud.

Founded in 2002, and with more than 150 staff in six offices around the globe, tyntec works with 500+ businesses including mobile service providers, enterprises and internet companies.

For more information:
www.tyntec.com

mobilesquared

mobilesquared provides intelligence and insight on the mobile sector. We've been analysing the mobile space for two decades, so our expertise has been earned, not learned. Our instinctive ability to ask the right questions uncovers invaluable nuggets of insight, which we interpret to help shape truly effective strategy for our clients. Our experience is recognised by the industry — we sit on judging panels for the prestigious GSMA Awards, EMMA awards, and the MEFFYs.

For more information:
www.mobilesquared.co.uk

A whitepaper by

mobile squared

www.mobilesquared.co.uk

Sponsored by

tyntec

www.tyntec.com