Mobilesquared
Communicating data

Protecting A2P SMS revenues in the roaring 20's

A review of the last decade and what we can expect in the next decade

• January 2021 •

VOX CARRIER
VOICE OF THE FUTURE

WINNER **"BEST ANTI-FRAUD INNOVATION"** MESSAGING & SMS **GLOBAL AWARDS** 2019

Table of Contents

January 2021

Section 1:

Key findings

Starting from just the one mobile operator investing in a next-generation SMS firewall in 2011, this had risen to 188 mobile operators by 2015, accounting for one-quarter of total mobile operators. By the end of the decade that figure had surpassed half of total mobile operators, with 391 (52.1%) having made the investment.

There was a resurgence of grey-route traffic in 2018-2019., attributed to sections of mobile operators unable to maintain their next-generation SMS firewall to ensure it was fully-protecting their network and subscribers from aggregators using “blended rates” of grey and white traffic to bring wholesale rates down to bulk-buying global brands.

If grey routes were eradicated altogether from the get-go, the A2P SMS sector could have generated total revenues of $252.21 billion during the decade. Instead, it amassed a total spend of $119.97 billion – or an average annual spend of $11.47 billion.

Between 2020-2024, Mobilesquared forecasts a total of 151 mobile operators will deploy a next-generation SMS firewall, taking the total to 542, or 72.3% of total mobile operators.

During the same timeframe, revenue leakage to grey routes remains unacceptably high, with a cumulative loss of $37.1 billion, or an annual average leakage of $7.69 billion.

Over the same timeline, grey route traffic accounted for 100% at the start of 2011, before dropping to 65% of total A2P SMS traffic in 2015, and 39.6% at the end of 2019.

Mobilesquared estimates that grey routes cost the mobile operator ecosystem revenues of $132.25 billion between 2010 and 2019. That is an average of $13.74 billion in revenue leakage from the legitimate A2P SMS each year, or mobile operator ecosystem.

As we entered the second decade of A2P SMS business messaging, 48% of mobile operators (359) were yet to have deployed a next-generation SMS firewall, although a further 74 deployments have taken place during 2020. That still leaves 38% of mobile operators with an unlocked and unsecure network.

Of the almost 2 trillion A2P SMS projected to be sent in 2024, just under one-quarter of these (23%) will be via grey routes. Total spend will reach $21.14 billion, with mobile operators projected to receive over 85% of this.

The total opportunity for A2P SMS could be $27.48 billion in 2024 (based on 100% white route traffic), which would represent average revenue of $36.64 million for every mobile operator.

Section 2:

Introduction

How research defined the last decade

It is almost 10 years since the first nextgeneration SMS firewall was deployed and the term "white route" traffic entered the parlance of A2P SMS business messaging. At the time the market was dominated by grey, illegitimate, and often fraudulent traffic, with mobile operators losing out on potentially billions of dollars in revenues.

In 10 years the A2P SMS market has thrived and become a key revenue stream for mobile operators monetising white route traffic via their next-generation SMS firewalls. A little over half of mobile operators are doing so today, which means much work is still to be done to make every network secure and every subscriber safe.

Transformation, Innovation and **Monetization**

Expanding reach, optimising operations, enhancing user experience, and fighting fraud

How research defined the last decade

The last decade has been dominated by the emergence of over-the-top (OTT) messaging apps, and the impact these would have on mobile operator services and revenues. It was not until midway through the decade that A2P SMS started to take on more prominence for mobile operators as they saw their P2P SMS revenues eroded by the likes of WhatsApp, Viber, LINE and WeChat.

In 2011, Mobilesquared research revealed that 68% of mobile operators believed P2P SMS was the operator service traffic most threatened by OTT messaging apps, compared to just 19% that said voice. Even at this early point in the decade, 70% of mobile operators believed that their revenues would decline as a result of increased use of OTT messaging apps. Yet more than half of mobile operators (54%) were not even close to developing a counter-strategy to the threat confronting them.

Of the 46% that had a strategy, the most popular action was "rolling out IMS/LTE to offer RCS", as well as "partnering with" OTT providers.

Jump forward 12-months to 2012 and little had changed other than more mobile operators (74%) had identified the threat posed by OTT messaging apps to SMS revenues, with the same percentage (74%) believing their revenues would fall. At least by this point the majority of mobile operators had entered a reactionary stage, with three-quarters actively exploring ways to ward off the increasing threat. Almost half (47%) claimed they were "rolling out IMS/LTE to offer RCS", or were "looking to enter partnerships" with the OTT providers.

The development of OTT messaging countermeasures by the mobile operators were slow to materialise, although the number monetising A2P SMS traffic was starting to increase and was becoming a more prominent feature of the research.

Introduction

By 2015, one-quarter of mobile operators (25%) were actually monetising A2P SMS traffic, with 49% of these experiencing year-onyear growth of between 6% to 36% in A2P SMS traffic. Around two-thirds of these mobile operators (63%) said that it had "hugely reduced unauthorised traffic" ... but not completely.

At the time, the driver for mobile operators investing in a next-generation SMS firewall was that it was simple to use and provided highperformance network security by blocking spam and fraudulent traffic.

At the opposite end of the messaging spectrum, mobile operators that were not monetising A2P SMS traffic were experiencing big increases in unauthorised grey-route A2P SMS traffic. By the end of 2015, grey route traffic still accounted for 65% of total A2P SMS traffic.

Despite the threat from OTT messaging apps and the subsequent decline in P2P SMS revenues, mobile operators were slow to jump on the A2P SMS bandwagon. At the time, the research revealed reasons such as "hampered decision-making due to having messaging teams across multiple internal divisions", to "staffing shortages", or "an unwillingness to invest in messaging infrastructure", and simply "failing to prioritize the A2P SMS opportunity".

But it could be something simpler still. During the first half of the decade, mobile operators were intent on facing their OTT rivals head-on and protecting their P2P SMS revenues, and this came at the expense of driving the A2P SMS opportunity.

> Of the 25% of mobile operators monetising A2P SMS traffic in 2015, **the majority were experiencing y-o-y growth of 6%-36%**

2010-2019 A2P SMS forecasts

At the start of the decade the A2P SMS market was worth $6.8 billion, but without nextgeneration SMS firewalls the market was overrun with grey route (and often fraudulent) traffic, with mobile operators seeing very little of that brand spend.

It was not until 2011 with the deployment of the first next-generation SMS firewalls, with the capability of detecting grey route traffic and illicit types of SMS traffic.

The inference here is that SMS firewalls deployed prior to this were incapable of providing the message visibility required. This means that mobile operators could only truly start monetising white route A2P SMS traffic from 2011. As more mobile operators started investing in next-generation SMS firewalls, spend in the sector accelerated.

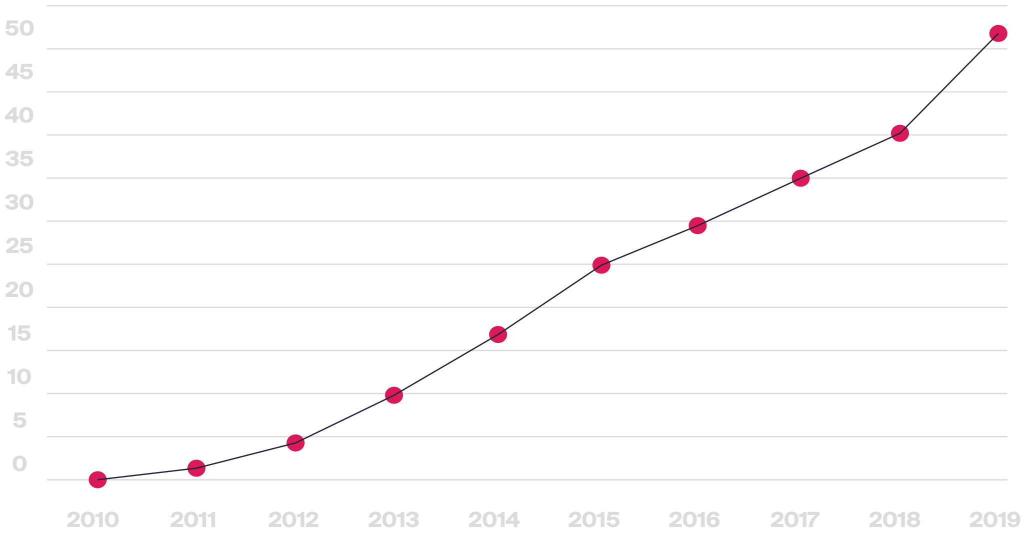
The emergence of the **next-generation SMS firewall**

Starting from just the one mobile operator investing in a next-generation SMS firewall in 2011, this had risen to 188 mobile operators by 2015, accounting for one-quarter of total mobile operators. By the end of the decade that figure had surpassed half of total mobile operators, with 391 (52.1%) having made the investment.

The most aggressive adoption took place between 2012 and 2015, with CAGR for the period between 2010 and 2014 at 179%. Mobile operator adoption of NGSF slowed down in the latter five years of the decade, with CAGR dropping to 16%. For the whole decade, CAGR stood at 87%.

Introduction

Next-generation SMS firewall deployments, 2010-2019



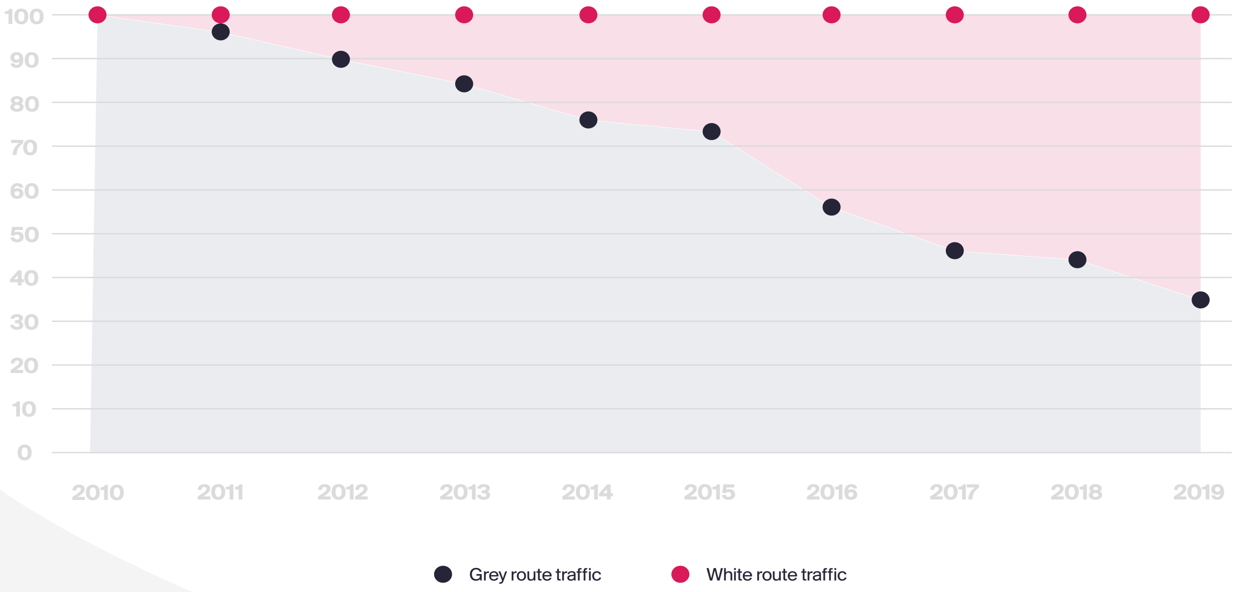
Impact on grey traffic

In total, as more mobile operators deployed next-generation SMS firewalls, grey route traffic during the decade dropped from 100% to 39.6% at the end of 2019.

Despite the continued increase in the deployment of next-generation SMS firewalls by mobile operators throughout the decade, there was a resurgence of grey-route traffic in 2018-2019. This was attributed to sections of mobile operators unable to maintain their nextgeneration SMS firewall to ensure it was fullyprotecting their network and subscribers from aggregators using “blended rates” of grey and white traffic to bring wholesale rates down to bulk-buying global brands.

For example, SIM-boxes continue to pose a significant threat to both national and international A2P SMS traffic, with the capability of sending high volumes of traffic via a bypass route in a short amount of time. This presents a high risk to the mobile operator, especially in markets where there is high mobile penetration and multiple types of unlimited bundled subscriber offerings.

White vs grey route traffic, 2010-2019



Section 2:

Introduction

Similarly, international hubs pose significant risks to mobile operators, with the identified threat coming from a high delivery rate for very low-cost hubs, SIM-box termination, and content manipulation. The threat of this bypass activity is high, even more so when combined with termination via SIM-box operators or termination via offending local hubs, aggregators, or content providers.

In both examples of on-going threats, these bypass tactics can escalate high levels of greyroute traffic in short amounts of time and have an extremely negative impact on the mobile operator and its subscribers.

The belief is that just to process the messaging traffic on a mobile operator's network requires a dedicated NOC team of multiple people managing the firewall on a 24/7 basis. The majority of mobile operators do not have the internal resource to manage such a process, which does mean not all SMS firewalls today are providing 100% protection from grey route traffic.

A third-party specialist not only has the resource to manage the firewall, but importantly, has the intelligence collated from multiple sources (such as mobile operator firewalls, aggregator partners), constantly expanding their fraud database with continuous penetration testing of hubs, the SS7 network, and SIM boxes for example.

Couple this with machine learning and artificial intelligence, content filtering and analytics, all combine to feed the SMS firewall with the intelligence that can then be applied to each mobile operator's firewall. Mobilesquared estimates that grey routes cost the mobile operator ecosystem revenues of $132.25 billion between 2010 and 2019. That is an average of $13.74 billion in revenue leakage from the legitimate A2P SMS each year, or mobile operator ecosystem. If grey routes were eradicated altogether from the get-go, the A2P SMS sector could have generated a total of $252.21 billion during the decade. Instead, it amassed a total spend of $119.97 billion – or an average annual spend of $11.47 billion.

By the end of 2019, the A2P SMS market was worth $16.73 billion. Between 2010 and 2019 the CAGR was 9%, peaking in the first fiveyears at 13%, before falling to 5%. In the formative years, the market was growing yearon-year at around 20% but has since dropped to around 5%.

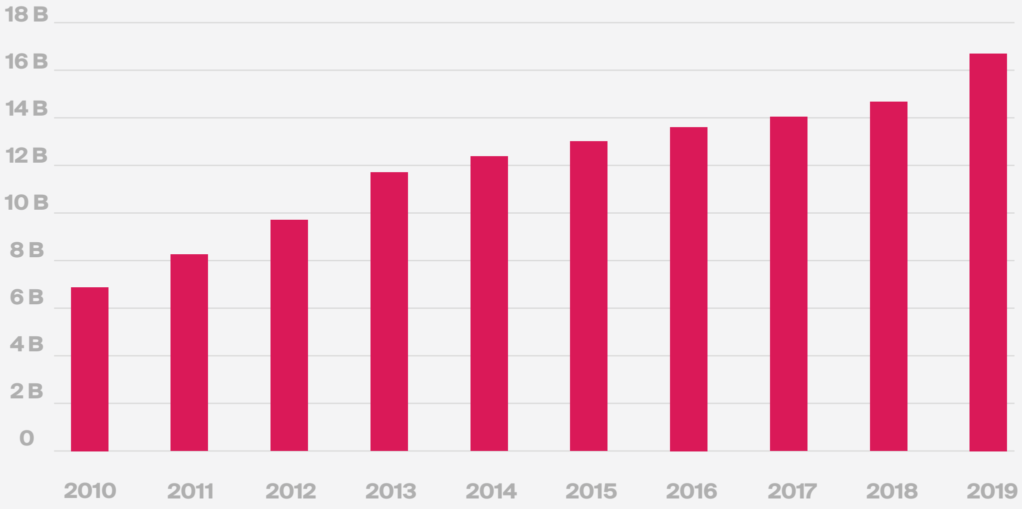
Impact for operators

- Revenue loss
- Fraudulent cost
- SMS fraud/spam
- Degradation of network performance
- Incrased CAPEX and OPEX
- Customer complaints
- Operator reputation damage
- Subscriber churn

Impact for subscribers

- SMS fraud/spam
- Low delivery rates
- Poor customer experience
- Decreased subscriber loyality

A2P SMS revenues (US$), 2010-2019



Introduction

2020-2024 forecasts

As we entered the second decade of A2P SMS business messaging, 48% of mobile operators (359) were yet to have deployed a nextgeneration SMS firewall, although a further 74 deployments have taken place during 2020. That still leaves 38% of mobile operators with an unlocked and unsecure network.

But there is encouraging news. In the ensuing five-year period between 2020-2024, Mobilesquared forecasts a total of 151 mobile operators will deploy a next-generation SMS firewall, taking the total to 542, or 72.3% of total mobile operators. Of the almost 2 trillion A2P SMS projected to be sent in 2024, just under one-quarter of these (23%) will be via grey routes. Total spend will reach $21.14 billion, with mobile operators projected to receive over 85% of this.

During the same timeframe, revenue leakage to grey routes remains unacceptably high, with a cumulative loss of $37.1 billion, or an annual average leakage of $7.69 billion. While this is significantly lower compared to the previous decade, it still represents a phenomenal wastage at a time when mobile operators are facing expensive 5G network rollout costs and continued pressure from OTT messaging and voice providers.

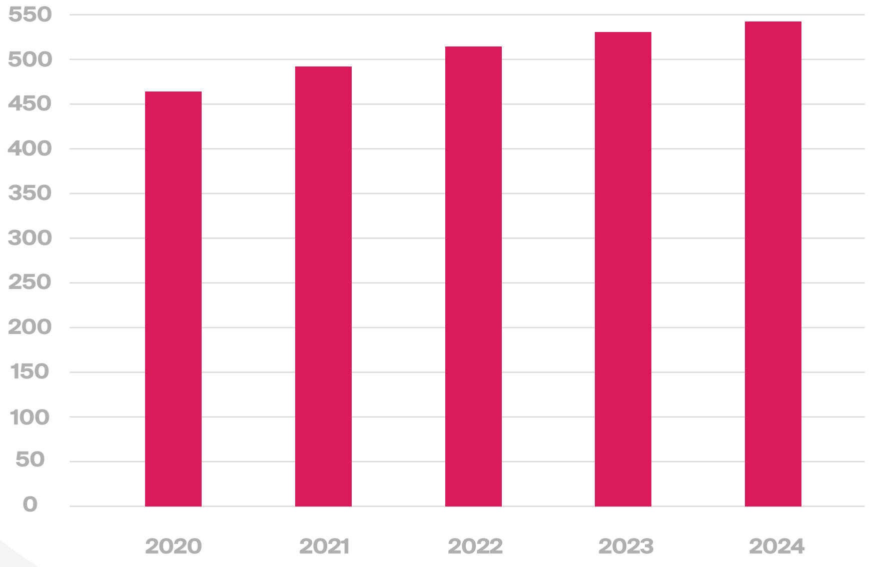
The total opportunity for A2P SMS could be $27.48 billion in 2024 (based on 100% white route traffic), which would represent average revenue of $36.64 million for every mobile operator.

23% of A2P SMS traffic between 2020-2024 will be via grey routes.

A2P SMS market worth $21.1billion in 2024

Revenue leakage to grey routes will mean a cumulative loss of **$37.1 billion between 2020 - 2024.**

Next-generation SMS firewall deployments, 2020-2024



Annual average revenue leakage **of $7.7 billion**

Section 3:

SMS Firewalls in action

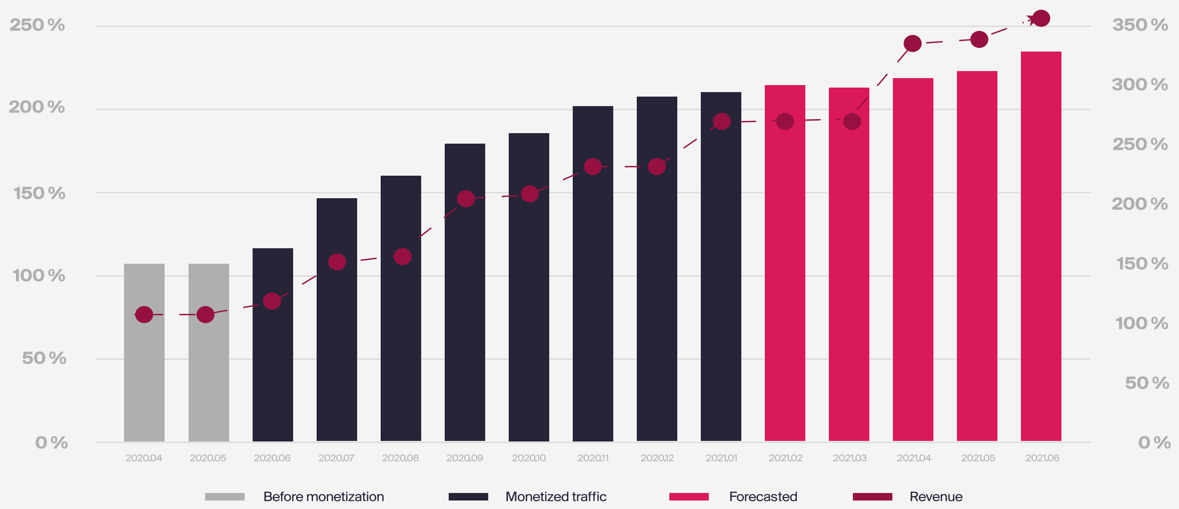
Case Study 1

Latin America

For TIM Brazil, monthly A2P SMS revenues doubled within one quarter of deploying a next-generation SMS firewall. In the 6-months following deployment, the mobile operator enjoyed over 250% revenue uplift. Within one year, that uplift is expected to increase to over 350% and over 700% within two years.

Monthly A2P SMS revenue increase over 300% in the 1st year

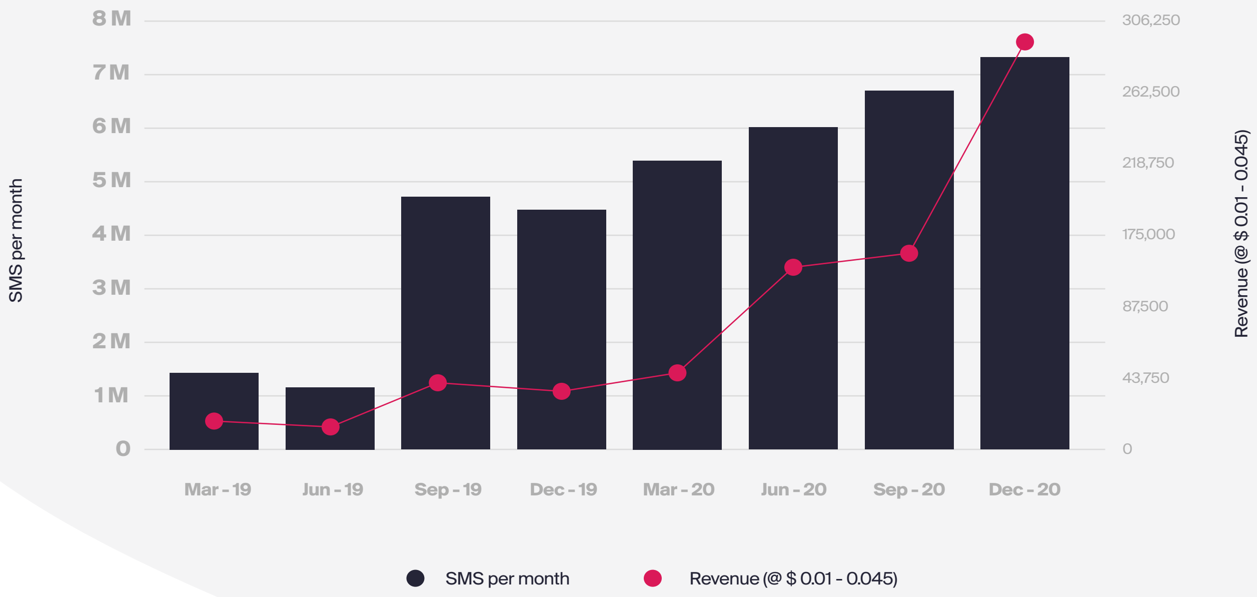
Region: South America | Subscribers: 50 mil | Mobile broadband: 97% | Prepaid ratio: 63% | Market share: 23% | ARPU: 1.5 USD



Case Study 2

Asia

If we look at one mobile operator in Asia, their monthly A2P SMS revenues quadrupled within one-quarter of deploying a next-generation SMS firewall. If we compare A2P SMS revenues pre-deployment compared to the 12-months post-deployment, and the mobile operator experienced a 515% uplift in revenues. In the second year following deployment, revenue uplift was at 1,361%.



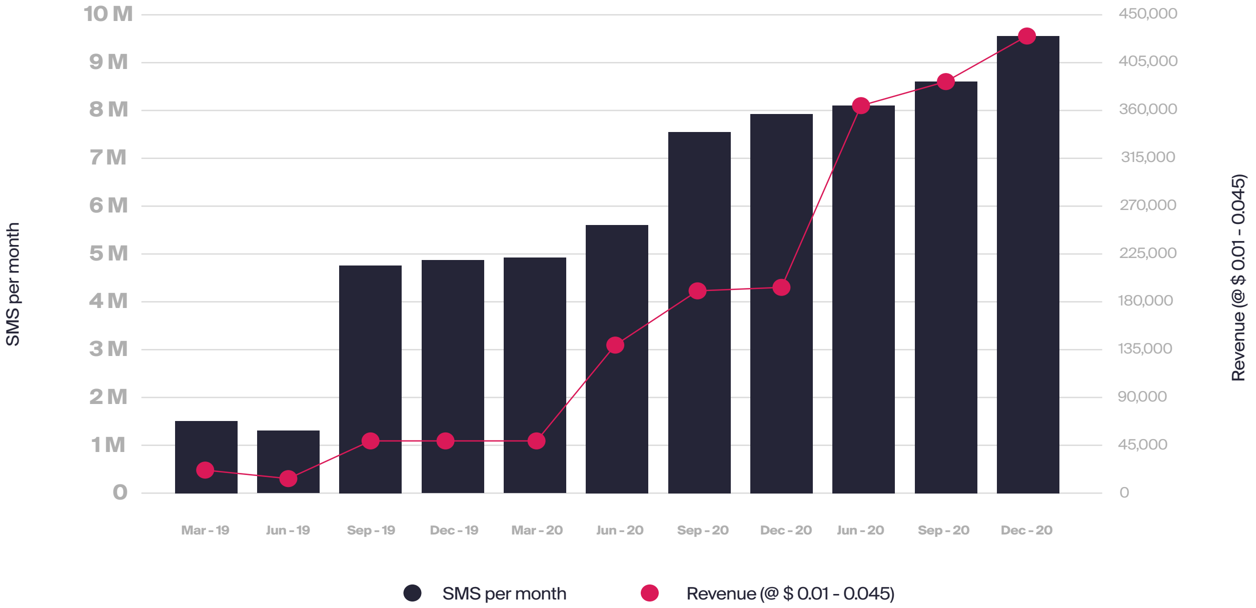
Section 3:

SMS Firewalls in action

Case Study 3

Africa

If we apply the same process to a mobile operator in Africa, their monthly A2P SMS revenues also quadrupled within one-quarter of deploying a next-generation SMS firewall. The mobile operator experienced a revenue uplift of 374% in the 12-months following deployment. Within two years, that uplift had jumped to 2,194%.



Across the three mobile operator examples, **the average immediate uplift in A2P SMS revenues,** following the deployment of a next-generation SMS firewall is **413%, rising to 1,425% in the second year.**

Section 4:

The VOX customer journey

1 STEP Establish a partnership

This entails a free network assessment & market analysis, defining a customized commercial model, and defining high-level solution deployment.

2 STEP Solution Implementation

Sign-off detailed technical deployment, is followed by deployment of the VOX solution including VOX analytics & reporting; configuring the VOX AI engine with as much data as possible (2-4 weeks of traffic learning); apply filtering & protect network; sign-off testing; go live; handover to operation and activate billing.

3 STEP Operation & Support

This involves 24/7 Monitoring, traffic management; rules management & update; block fraudulent traffic; and incident management

4 STEP Partnership & Management

A quarterly/bi-annual business review (of traffic & pricing) and service review, analysis of escalation management and change management.

VOX Managed Services

VOX Managed Services

Analytics

Traffic analysis to identify potential bypass or other risks.

Market intel DB

Information about fraud sources and fraud types collected from the market.

SMS Firewall

Traffic control, rules management.

NOC

Systems monitoring, traffic monitoring, alarms handling.

Penetration testing

Constant traffic testing of bypass to verify firewall's settings and identify new potential breaches.

Reporting

Traffic reports trends, volumes, brands, bypass, blocked and passed traffic, sim boxes.

Section 5:

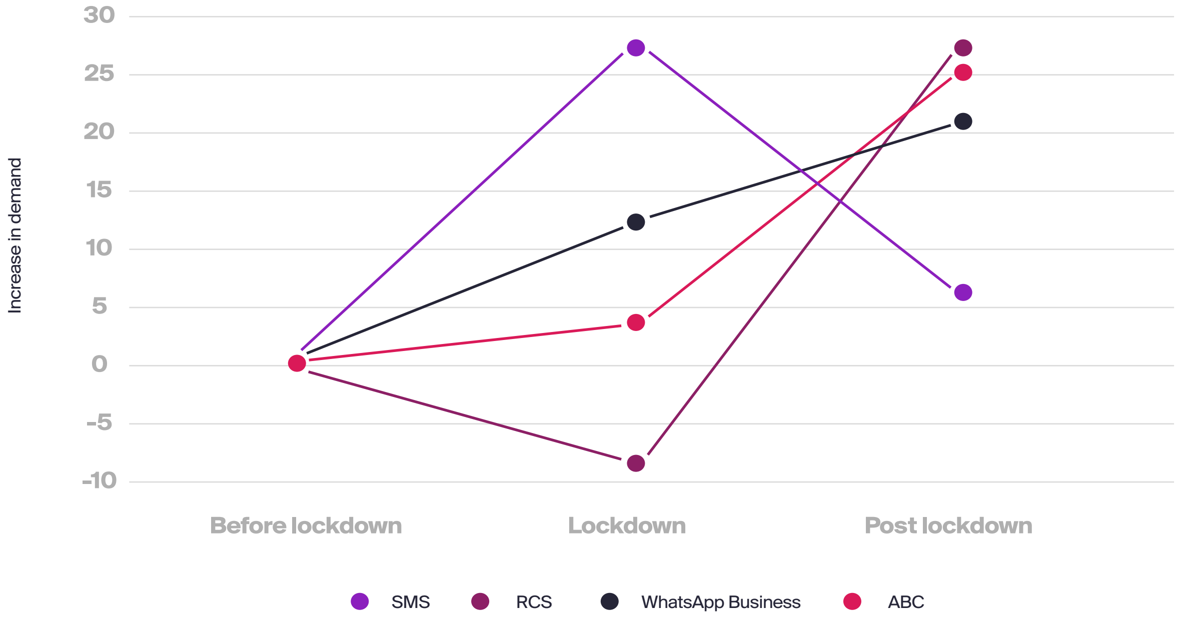
Expectations for the next decade

The start of the new decade has been hugely impacted by the Pandemic. The impact of limited face-to-face contact, working from home, allied with the expedition of digital transformation among businesses, have become key components in the emergence of business messaging becoming the ideal channel to communicate with consumers.

The advancement of SMS was always going to be the platform upon which future iterations of messaging would be based, but during the Pandemic businesses turned to SMS in order to communicate with customers, as demand for the channel increased significantly.

*To track the appeal of each channel during lockdown and beyond, we have created the Net Demand Score (NDS), whereby we have subtracted the number of responses selecting "less demand" from those selecting "more demand" and divided by the total number of responses for that question. We have applied the NDS to both lockdown and expectations for post-lockdown. We have assumed that at the start of lockdown everything was equal (or 0).

Business messaging Net Demand Score*, concertinaed view



The upshot of Pandemic is that business messaging is on the cusp of big growth as virtually every business looks to survive in the “new normal”.

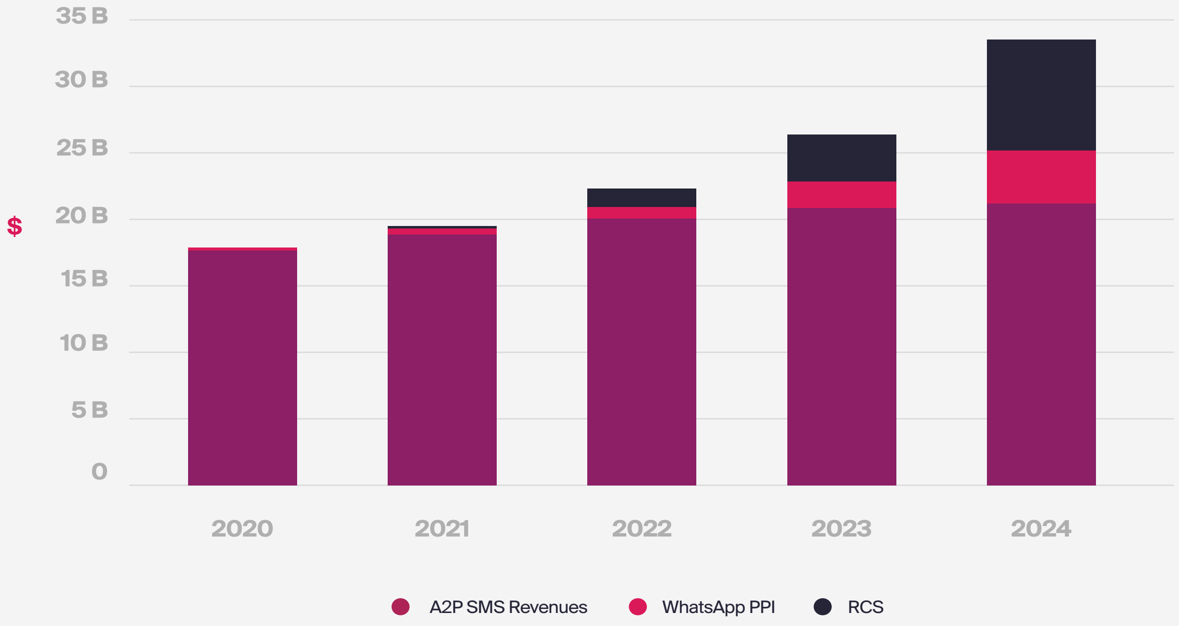
Using Mobilesquared data we have explored the impact post-lockdown would have on business messaging based on mid-term and long-term expectations, to chart anticipated demand for each channel (See above). In the mid-term all four channels are clustered together, which is indicative of brands pursuing an omnichannel messaging strategy. But in the long term, each messaging channel will become more defined in terms of the types of messages each brand will use that channel for.

SMS will remain the bedrock upon which all richer forms of messaging will grow. What we are already identifying is that rich messaging channels are providing a supplementary service compared to SMS, with the emergence of new and different use cases.

Expectations for the next decade

For instance, WhatsApp Business and Apple Business Chat (ABC) are targeting the inbound customer care model, which has largely remained untouched by SMS. RCS has long been earmarked to become the rich messaging channel offered by mobile operators. Even at an early stage, RCS has demonstrated exceptional levels of engagement. In a direct comparison with SMS, data revealed that for every 1 SMS sent by a business or brand, that same message would generate at least 3 messages on RCS, creating a massive uplift in the number of messages (and ultimately) revenues generated on RCS.

Total business messaging revenues (US$), 2020-2024



However, developments throughout 2020 have seen RCS verging towards becoming an OTT messaging platform, as Google rolls out its Google Guest Cloud offering globally effectively circumventing mobile operator involvement. Unless, of course, should the mobile operator decide to partner with Google. But at the time of writing, it is widely believed that Google will not interconnect its RCS platform with third-parties, which means that RCS will become a rival messaging channel to mobile operators similar to that WhatsApp and WeChat and LINE and so on.

This places even more emphasis on A2P SMS revenues today, as mobile operators look to safeguard existing messaging-based revenue, at least until their role in the rich messaging space, and 5G messaging in particular, becomes clearer.

Regardless, mobile operators must not only now consider today's revenues, but the future. A fully-managed SMS firewall must protect and monetise today but also be in a position to evolve to protect 5G messaging, whatever form that might take, whether RCS or something different.

The fact remains, that whether it is RCS or not, RCS has been meticulously developed via the standardised process to be a safe and secure platform for messages to traverse, but rogue traffic has, and will inevitably penetrate its defences one way or another, which makes the need to lock down the network from the off critical.

Mobile operators are in the driving seat when it comes to business messaging, and they need to protect their existing revenues and ensure longevity by investing in a fully-managed business messaging firewall that futureproofs today's and tomorrow's network and subscriber.

About

Mobilesquared
Communicating data

#1 FOR BUSINESS MESSAGING INTELLIGENCE

Mobilesquared is the go-to partner for definitive business messaging market intelligence. We own the most comprehensive independent global messaging market forecasts in the industry, trusted by brands including Mastercard, Google, Vodafone, LivePerson, and PwC for accuracy and impartiality. If you need targeted messaging market insight and future-proofed strategy, we can help.

mobilesquared.co.uk

VOX CARRIER
VOICE OF THE FUTURE

Protect & Monetize MNOs assets

Vox Carrier optimises, accelerates and simplifies International Voice and Messaging through innovation in technology, platforms and processes. We serve operators, service providers, carriers, aggregators and enterprises worldwide, delivering an array of services such as Voice, A2P Messaging, service monetization and operational outsourcing. Vox Carrier's technologies initiative, Vox Technologies, has also launched Vox360, which won 'The Best Anti-Fraud Innovation' at the 2019 Messaging and SMS Global Awards. Vox360 is an anti-fraud solution designed to simplify the fight against fraud in telecommunications.

www.voxcarrier.com

DISCLAIMER

For a full methodology relating to the forecasts included in this report please contact Mobilesquared directly. Not all views included in this report represent Mobilesquared's views.

This publication may not be:
(i) copied or reproduced; or
(ii) lent, resold, hired out or otherwise circulated in any way or form without the prior permission of Mobilesquared Ltd.

Whilst reasonable efforts have been made to ensure that the information and content of this publication was correct as at the date of first publication, neither Mobilesquared Ltd nor any person engaged or employed by Mobilesquared Ltd accepts any liability for any errors, omissions or other inaccuracies. Data and assumptions relevant as of Sept-2020. Please note, Mobilesquared frequently updates its market forecasts based on fluctuating market conditions and developments. Companies should independently verify any facts and figures as no liability can be accepted in this regard – companies assume full responsibility and risk accordingly for their use of such information and content.

Mobilesquared
Communicating data

VOX CARRIER
VOICE OF THE FUTURE

WINNER **“BEST ANTI-FRAUD INNOVATION”** MESSAGING & SMS **GLOBAL AWARDS** 2019

January 2021