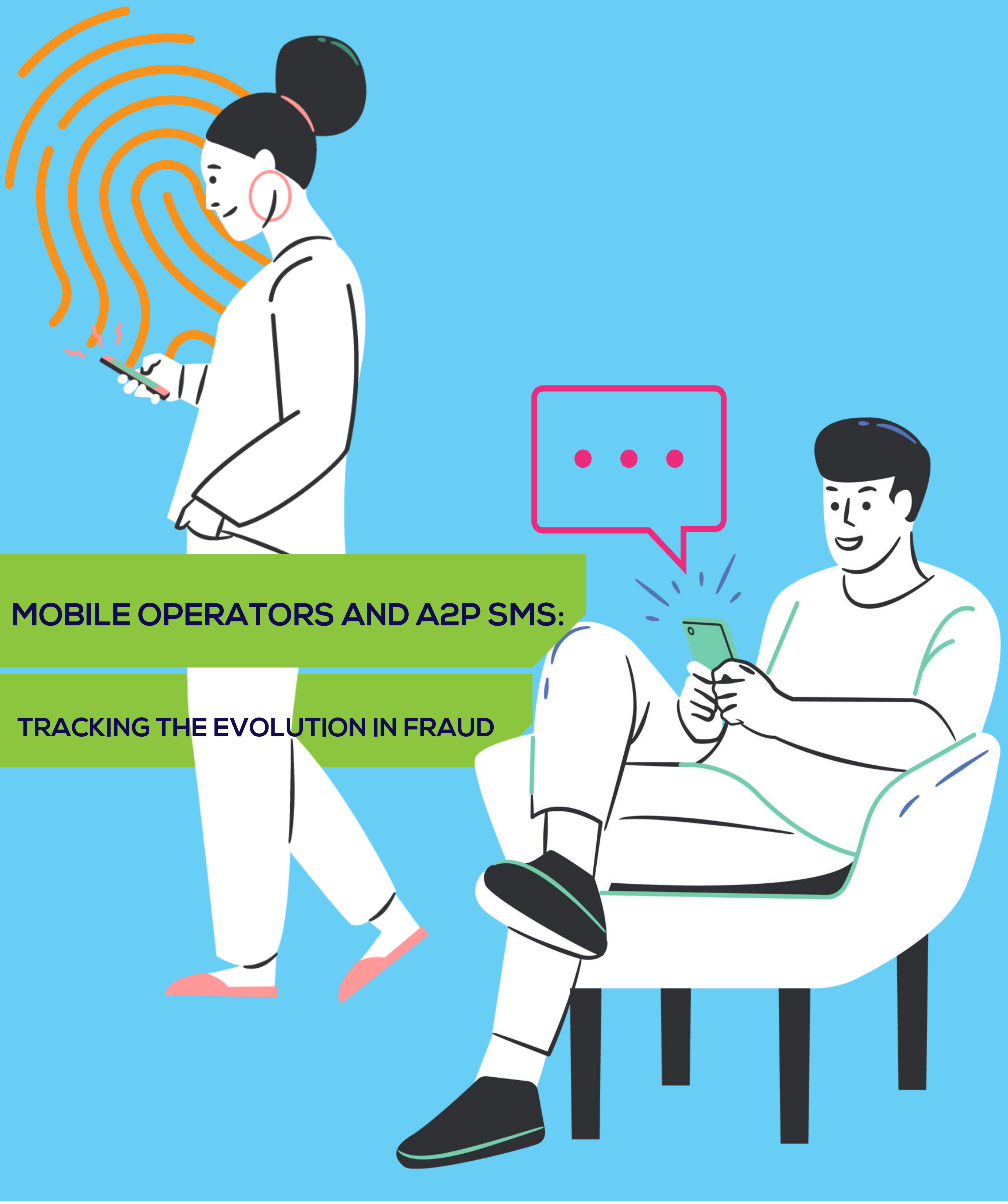
MOBILE OPERATORS AND A2P SMS:

TRACKING THE EVOLUTION IN FRAUD



MEF FUTURE OF MESSAGING PROGRAMME

anam

TATA COMMUNICATIONS

A report by: Mobilesquared Communicating data

CONTENTS

If your work has anything to do with the Application-to-Person (A2P) messaging market, then you need to read this report. The sustainability and success of Business SMS is inextricably linked to the ability to protect users from both spam and fraud attempts, and ultimately to both enable and protect the monetisation of it for those market players that act with integrity.

This is not the first time that the Mobile Ecosystem Forum (MEF) advocates the need to clean up the SMS market, and neither will it be the last. This is the third survey on A2P SMS Firewalls since 2018 in which we investigate mobile operators' uptake and understanding of these solutions. During this timeframe, whilst we have seen we are still far from a fully protected Business SMS market

MEF continues to champion SMS Firewalls and anti-fraud solutions. They absolutely should be implemented by all mobile network operators (MNOs), yet one in four is still leaving their SMS traffic unpoliced. Things are however improving with 45 more operators implementing anti-fraud solutions during 2021. Penetration at 75% in 2021 is progress from the 68% we reported in 2019, and the 34% in 2018. There is still much work to do though, but the trend is encouraging.

It's encouraging there are plenty of solution options around for even the smaller or low-income MNOs. Whether choosing an **in-house solution or managed one, the market is very competitive and affordable**. **Solutions are evolving, with far more than just a basic firewall available today.** The solutions are enriched with new services and features. It is important to see how other features play an important role in today's security planning. Some mobile operators are getting much more sophisticated in their requirements.

It would be remiss of me not to mention how the survey picks up that 60% of operators are also welcoming SMS Registries (MEF and its members have created a Sender ID registry in the UK, Ireland and Singapore) as well as codes of conducts and more regulation. Please do sign up to MEF's SMS Code Of Conduct, the central piece of our 'Trust in Enterprise Messaging' scheme. It's important to mention that the Code is open to both members and non-members to sign.

If you have questions or comments on A2P Anti-Fraud and Market Development, we at MEF would like to hear from you. MEF is a not-for-profit global trade association supporting the industries that present mobile opportunities globally. MEF members truly appreciate the importance of ecosystem-wide debate and cross industry initiatives.

Finally, I'd like to thank MEF members **ANAM** and **Tata Communications** for supporting this survey and making it available to all for free. The ecosystem is working together to fight A2P Fraud so come and join in!

DARIO BETTI

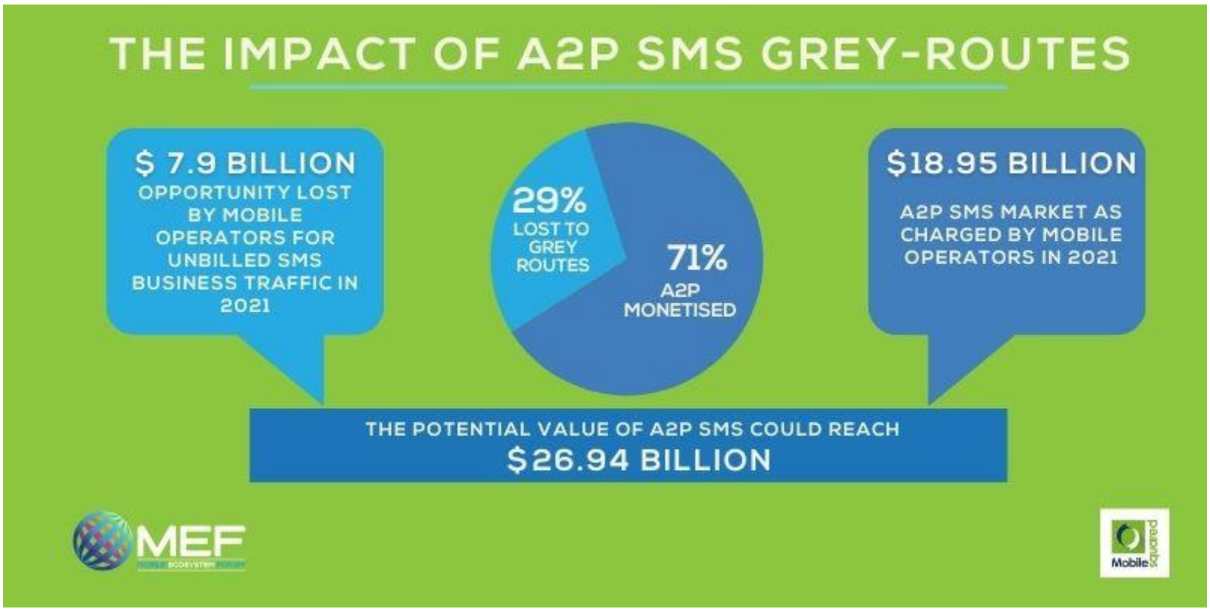
MEF CEO

01

INTRODUCTION

The business messaging market will be worth $19.4 billion in 2021[1], with around 97.5% of that spend coming from A2P SMS (US$18.95 billion). But it could be worth so much more. **The total A2P SMS market could be worth US$26.94 billion**[1] **if all A2P SMS traffic was monetised**. This means US$7.9 billion will be lost to grey routes in 2021[1]. Or put another way, that is US$21.6 million lost to potentially fraudulent traffic every day. Or, if that figure were divided between every mobile operator, they would receive an additional annual payment of US$10.5 million.

Figure 1: Opportunity lost to grey-routes

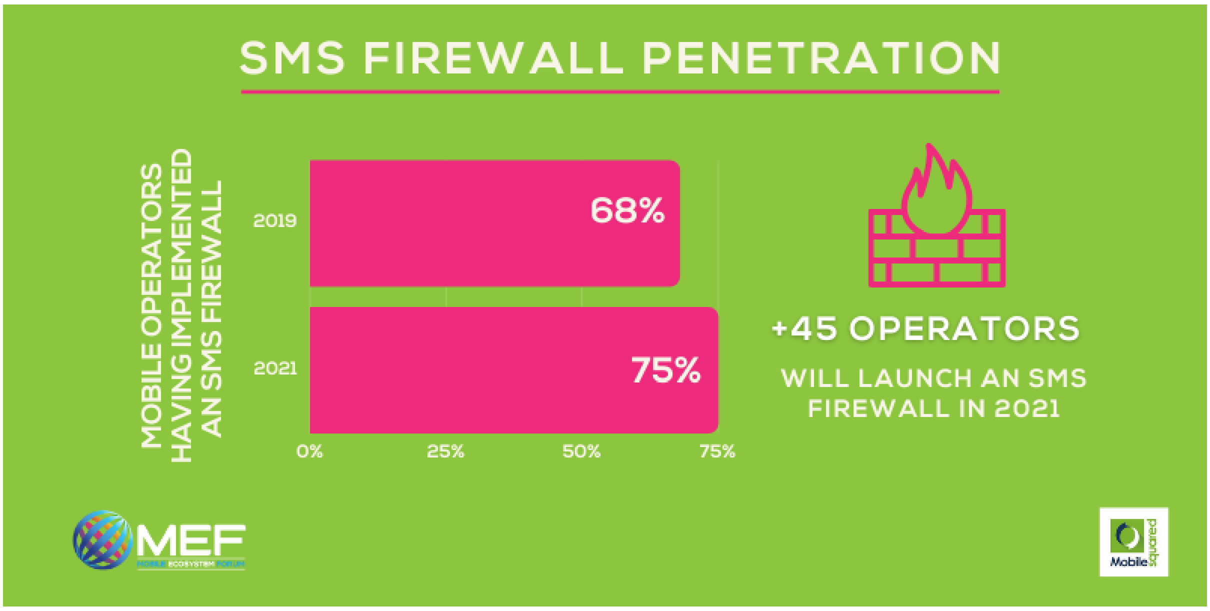


Source: Mobilesquared

According to Mobilesquared data, one of the main reasons for this revenue leakage is that **almost one-third of mobile operators have not invested in a messaging fraud detection** solution leaving their network open and vulnerable to fraudulent traffic. In 2021, Mobilesquared projects a further 45 mobile operators out of 633 mobile operators will invest in an SMS firewall as they look to protect their network from fraudulent traffic and monetise the A2P SMS opportunity, taking the total to **75% of total mobile operators by the end of the year**.

[1] Based on Mobilesquared Global A2P SMS Databook 2019-2024, published October 2020, and Global RCS forecasts, 2019-2024, published October 2020.

Figure 2: SMS Firewall Deployments



Source: Mobilesquared

To ascertain how mobile operators are reacting to the threat posed by fraud, MEF has once again teamed up with Mobilesquared the to look at the impact fraudulent A2P SMS traffic had on the business messaging ecosystem in 2020, and how this might affect the opportunity in 2021.

This report explores the key findings from the exclusive mobile operator research and follows on from a similar project conducted by Mobilesquared for MEF in 4Q 2019.

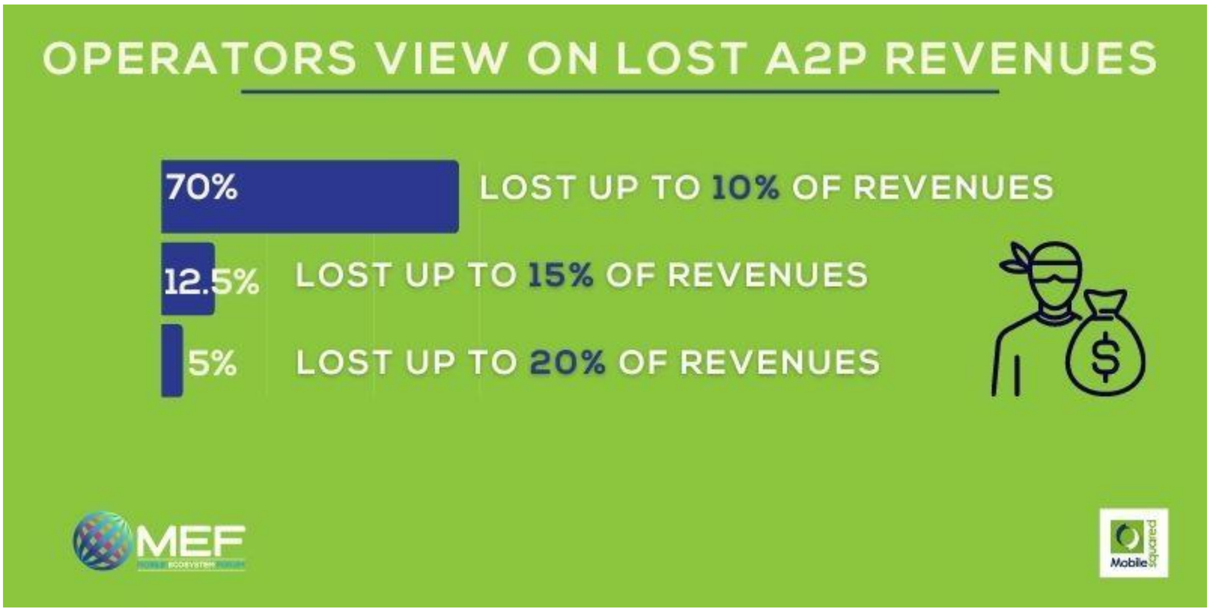
The research of mobile operators was an online survey running from December 2020 to April 2021. In total 66 mobile operators participated in the research, including Polkomtel, Unitel, Libyana, Deutsche Telekom, eir, Hutchison Drei, MegaFon, Omantel, Millicom, Tunisie Telecom, Bell Mobility, Etisalat, Nuevatel PCS, Sunrise, China Mobile, Bharti Airtel, Telia (multiple markets), Telefonica (multiple markets), Deutsche Telekom, AT&T mobility, Vodafone (multiple markets), MTN (multiple markets), Swisscom, Telenor (multiple markets), True Corporation, Bouygues Telecom.

02

MNO MINDSET TOWARDS MESSAGING FRAUD

The fight against messaging fraud is an on-going battle for every mobile operator. The survey of mobile operators revealed that 70% of respondents believe they lost up to 10% of their annual A2P SMS revenues to fraud in 2020. More alarmingly, 12.5% believe they lost up to 15%, and 5% estimate that figure was closer to 20%, with 8% not knowing.

Figure 3: Expected fraud level



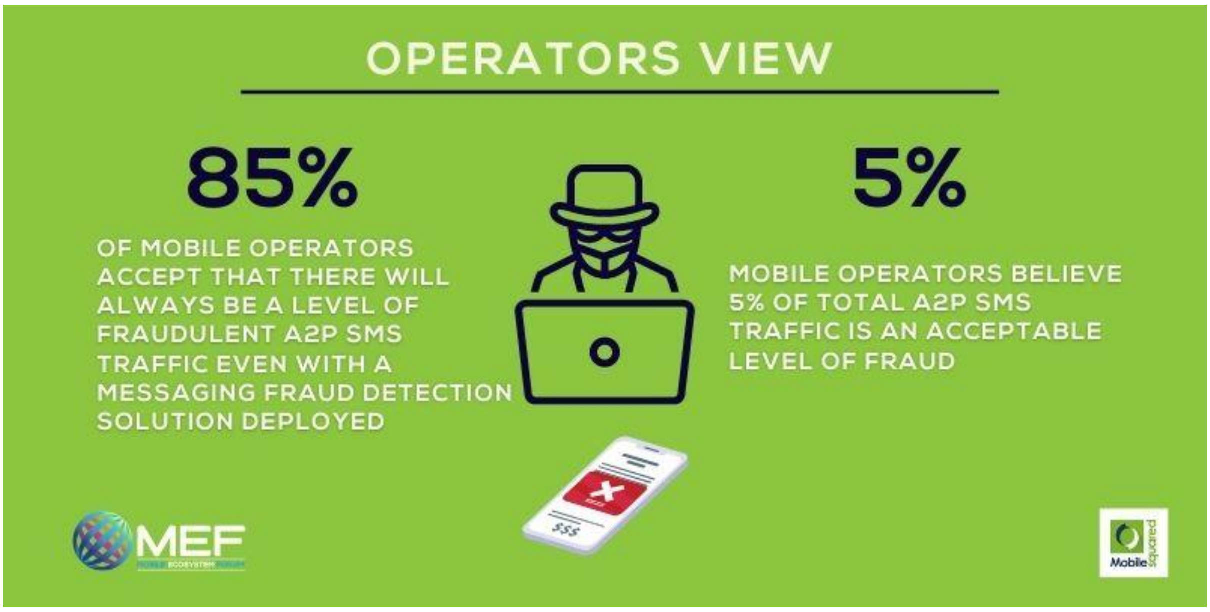
Source: Mobilesquared/MEF research

If we apply the percentage findings from the survey to Mobilesquared market data, it puts a nominal value on what each mobile operator is knowingly losing each year. For example, we know that the average mobile operator in West Europe generated annual A2P SMS revenues of $23.3 million[2] in 2020. Based on the survey findings, 70% of mobile operators in West Europe would have lost up to $2.3 million each, and 20% would have experienced revenue leakage of between $3.5 million to $4.7 million.

Based on the survey findings, a whopping 85% of mobile operators believe there will always be a level of fraudulent traffic traversing their network even when they have deployed a messaging fraud detection solution. Further still, the majority of mobile operators believe 5% of fraud is an acceptable level on their network.

[2] This figure is based on our Global A2P SMS Databook 2019-2024, published October 2020

Figure 4: Operator Survey Expectations



OPERATORS VIEW

85%

OF MOBILE OPERATORS ACCEPT THAT THERE WILL ALWAYS BE A LEVEL OF FRAUDULENT A2P SMS TRAFFIC EVEN WITH A MESSAGING FRAUD DETECTION SOLUTION DEPLOYED

5%

MOBILE OPERATORS BELIEVE 5% OF TOTAL A2P SMS TRAFFIC IS AN ACCEPTABLE LEVEL OF FRAUD

Q18: Do you accept that there will always be a level of fraudulent A2P SMS traffic even with a messaging fraud detection solution deployed?

Q19: What is an acceptable level of fraud as a percentage of total A2P SMS traffic even with a messaging fraud detection solution deployed?

Source: Mobilesquared/MEF research

The survey findings are not stating that fraud has become acceptable. Far from it. However, there is a widely held acceptance throughout the messaging industry that fraud will never be zero percent of traffic, as fraudsters are always probing potential network weaknesses or vulnerabilities. It is the function of the SMS firewall to identify and prevent these attacks from happening again; it is an ongoing game of cat and mouse.

The main point to raise here is that there are different fraud types, with some messages considered harmless, like a legitimate marketing message sent via a grey route. Obviously, this is what the 5% acceptance level is being applied to. The problem is that there is always the threat of malicious messages that can give a negative impact or experience to the consumer and permanently damage the brand image.

The more damaging non-MNO-revenue-leakage frauds like phishing and malware (e.g., Flubot), are prime examples. With such instances, this type of fraudulent traffic will potentially only impact a small number of subscribers, but the consequence can be severely damaging to brand reputation, especially when such attacks are covered in the mainstream media.

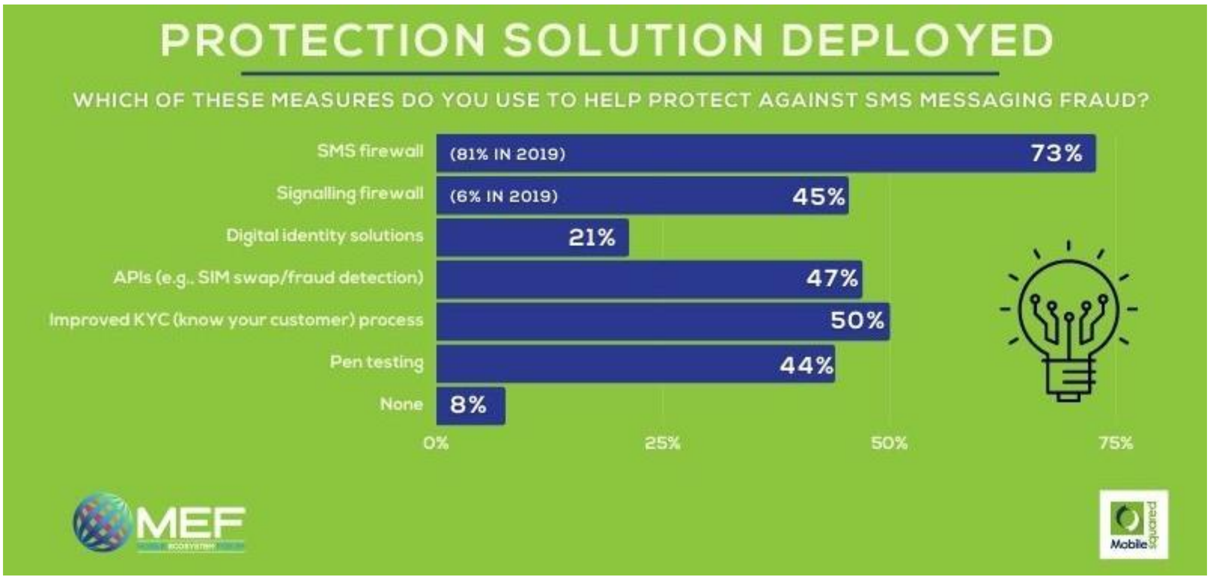
The safest stance for any mobile operator is to adopt a zero tolerance towards fraudulent traffic.

An effectively managed SMS firewall will be able to distinguish the different kinds of traffic, so it is then incumbent on the commercial practices and management of the firewall to ensure the fraudulent traffic detected is treated accordingly, hence the emergence of this "tolerance level".

What this does highlight, is that by applying this "acceptable 5%" figure to the previous question relating to percentage of revenue lost, a staggeringly high 92.5% of mobile operator respondents are experiencing unacceptable levels of messaging fraud. **As an industry, messaging fraud still represents a big problem**.

The majority of mobile operators do appear to be tackling the problem head on, at least in principle. According to the survey, almost three-quarters of respondents have already deployed an SMS firewall – which almost correlates with Mobilesquared's market data. Almost half of mobile operators (45%) have deployed a signalling firewall, while other fraud detection measures that have been deployed include improved KYC (know your customer), APIs, pen testing, and digital identity solutions.

Figure 5: Measured used to prevent SMS Fraud



Q5: Which of these measures do you use to help protect against SMS messaging fraud? (Select all that apply)

Source: Mobilesquared/MEF research

Table 1

Q5: Which of these measures do you use to help protect against SMS messaging fraud? (Select all that apply)	2019	2021
SMS firewall	81.25%	72.73%
Signalling firewall	6.25%	45.45%
Digital identity solutions		21.21%
APIs (e.g., SIM swap/fraud detection)		46.97%
Improved KYC (know your customer) process		50.00%
Pen testing		43.94%
None		7.58%
Other (please specify)	12.50%	12.12%

Source: Mobilesquared/MEF research

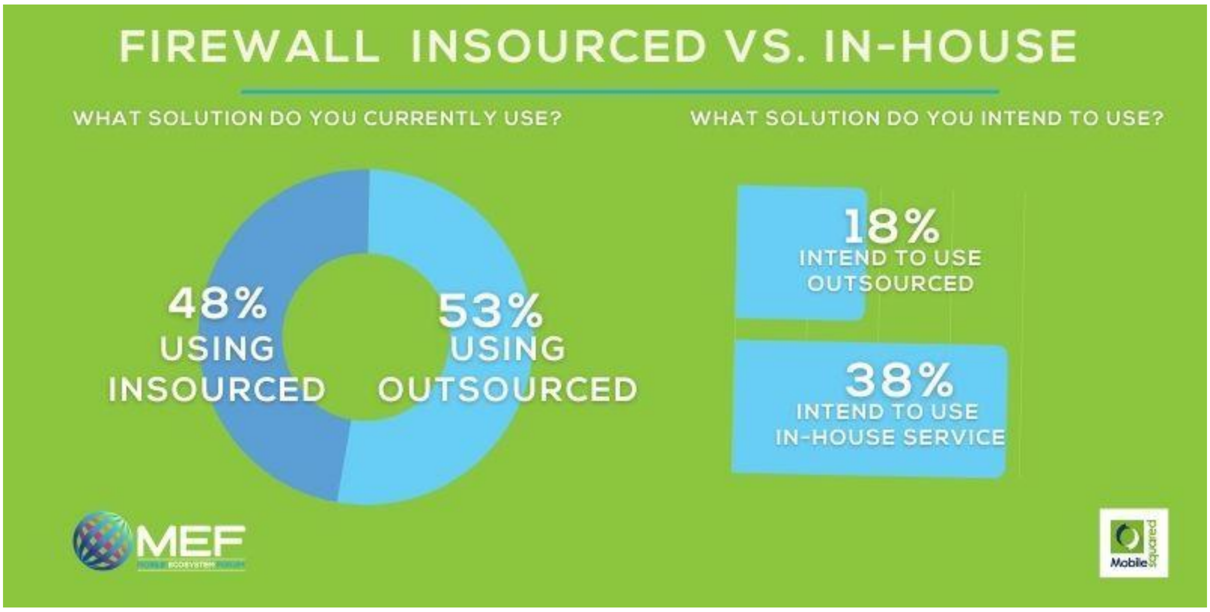
Respondents were then given the option to select one measure that they were most likely to additionally implement in 2021. SMS firewall came out on top with one-quarter of responses, with 18.2% likely to deploy a signalling firewall. Of the alternative measure available, digital identity amassed 19.7% of responses, followed by improved KYC (7.6%) and pen testing (6.1%).

While digital identity solutions are viewed as the next line of security to invest in, clearly mobile operators still see SMS firewalls as the priority to protect their network.

However, the survey has highlighted that a significant proportion of respondents are looking to update their existing SMS firewall solution. Based on the survey findings, **53% of mobile operators have been using an outsourced service** when it comes to managing their messaging fraud detection solution, with 47% in-house.

When this question was featured in our 2019 SMS firewall research, 43.8% of respondents used a blend of in-house and outsourced managed services, with 31.3% using a managed in-house solution, and 25% used an outsourced specialist managed service.

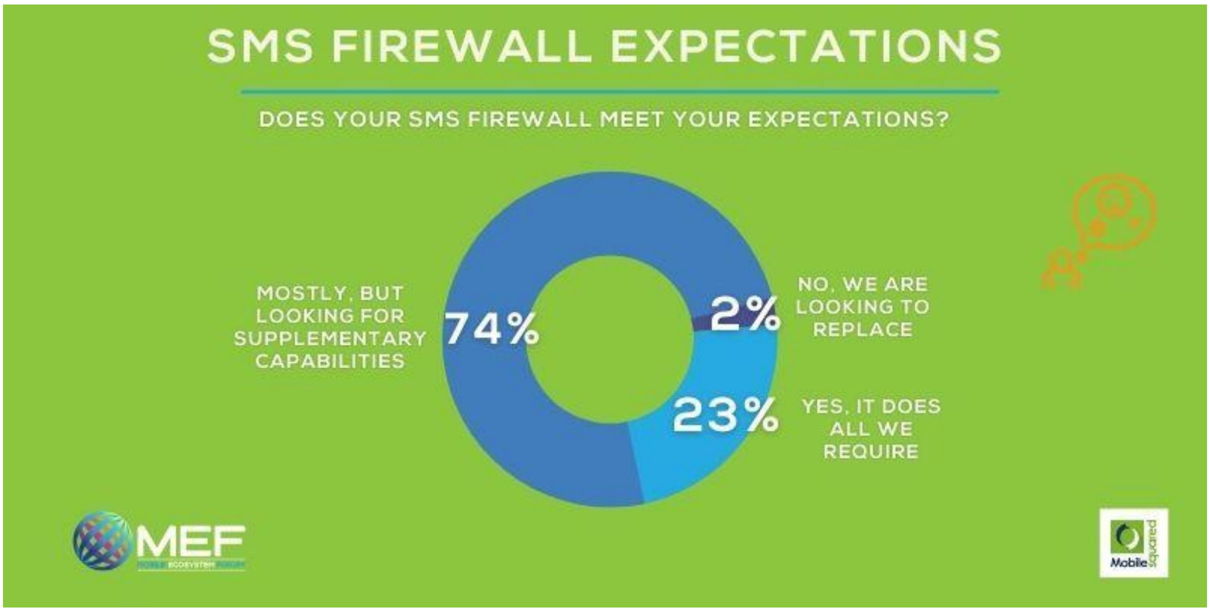
Figure 6: Service management



Source: Mobilesquared/MEF research

By the end of 2020 there has clearly been a shift in mobile operator mindset away from a blended solution towards managing the solution in-house. And this shift looks set to be more pronounced based on mobile operator intentions over the coming years, when 38% will potentially shift to an in-house solution, while 18% would traverse in the opposite direction. One of the reasons potentially driving this shift could be that m**obile operators are looking for supplementary capabilities from their SMS firewall,** according to three-quarters of respondents.

Figure 7: Satisfaction level for SMS firewall



Q24: Does your SMS firewall meet your expectations?

Table 2

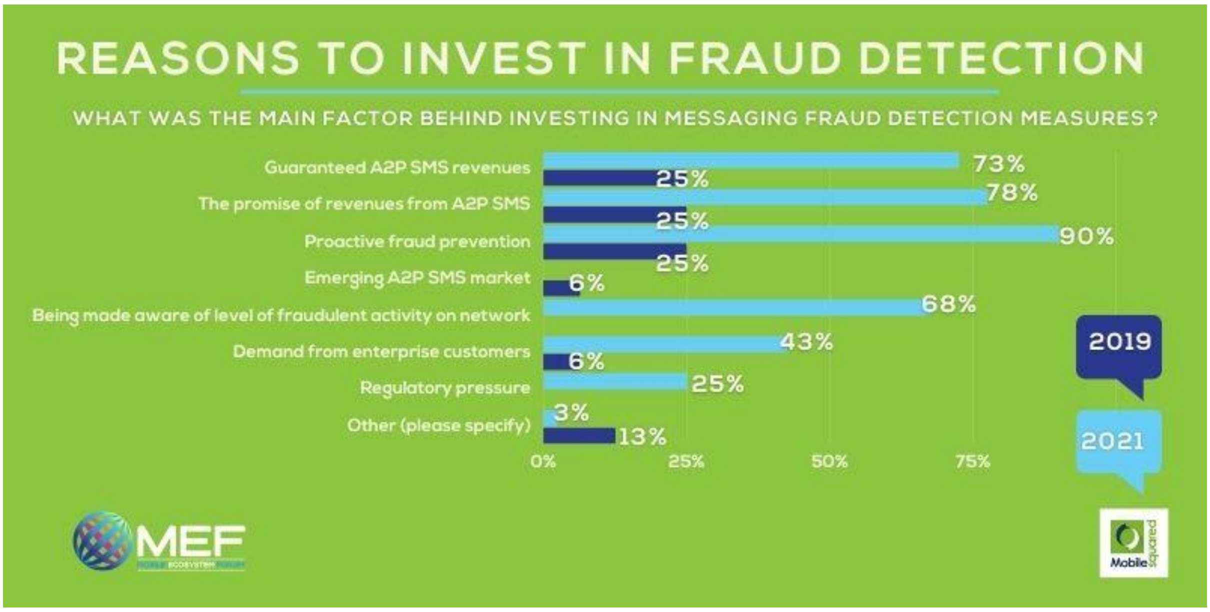
Yes, it does all we require	23.08%
Mostly, but looking for supplementary capabilities	74.36%
No, I'm looking to replace it	2.56%

Source: Mobilesquared/MEF research

Subsequently, the SMS firewall landscape could see 67% of mobile operators using an in-house solution by the end of 2025, leaving just 33% using an outsourced specialist managed service. This reflects a change in how mobile operators are looking to operate, and indicates that they are potentially looking to have more control of their A2P SMS business. It is worth noting that in doing so, the mobile operator will need to ensure that it has the in-house expertise and competency to implement security procedures, such as detection, analysis and updates, essential when managing SMS firewalls located in the network domain alongside network equipment like switches and SMSCs.

What has not changed is that proactive fraud prevention (i.e., the level of unauthorised messaging traffic it blocks) remains the main criteria for investing in a messaging fraud detection measures (MFDS), followed by the promise of guaranteed A2P SMS revenues – as they were in our 2019 survey.

Figure 8: Reason to invest in fraud detection



What was the main factor behind investing in messaging fraud detection measures?

Table 3

Q12: What was the main factor behind investing in messaging fraud detection measures? (Select all that apply)	2021	2019
Guaranteed A2P SMS revenues	72.50%	25.00%
The promise of revenues from A2P SMS	77.50%	25.00%
Proactive fraud prevention	90.00%	25.00%
Emerging A2P SMS market	n/a	6.25%
Being made aware of level of fraudulent activity on network	67.50%	0.00%
Demand from enterprise customers	42.50%	6.25%
Regulatory pressure	25.00%	0.00%
Other (please specify)	2.50%	12.50%

Source: Mobilesquared/MEF research

Interestingly, more than two-thirds of respondents also opted for "being made aware of the level of fraudulent activity on [their] network", which highlights the on-going levels of fraudulent traffic still prevalent on mobile operator networks. But SMS firewalls are not limited to just identifying fraudulent traffic, but also enhancing the subscriber experience. Around two-thirds of mobile operators identified the fact that there was an improvement in the subscriber experience and a reduction in the number of customer complaints relating to unwanted messages as a result of investing in an SMS firewall.

Figure 9: SMS Firewall success measure

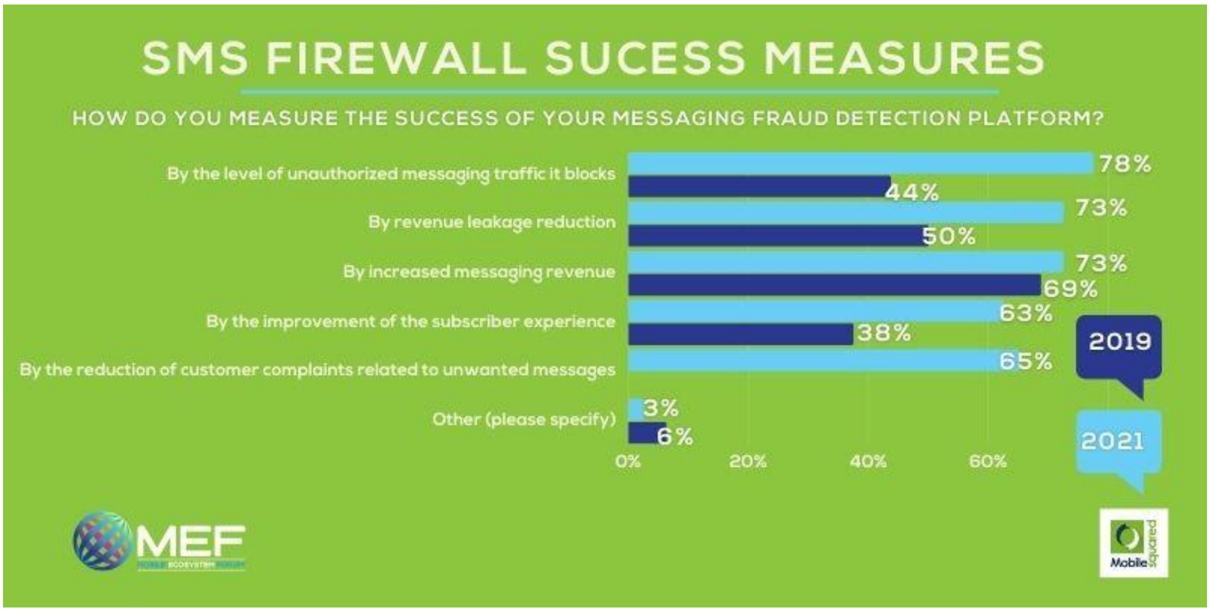


Table 4

Q13: How do you measure the success of your messaging fraud detection platform? (Select all that apply)	2021	2019
By the level of unauthorized messaging traffic it blocks	77.50%	43.75%
By revenue leakage reduction	72.50%	50.00%
By increased messaging revenue	72.50%	68.75%
By the improvement of the subscriber experience	62.50%	37.50%
By the reduction of customer complaints related to unwanted messages	65.00%	n/a
Other (please specify)	2.50%	6.25%

Source: Mobilesquared/MEF research

By going one step further and comparing across every option included in the question, the latest research reveals that an MFDS is having a significantly broader impact across mobile operators compared to 2019. For example, in 2021, on average, 70% of mobile operator respondents selected the five options available (excluding other), compared to an average of 50% of respondents in 2019. Therefore, a sound business messaging business can have a positive impact on customers and help generate brand loyalty. For instance, the improvement of the subscriber experience enjoyed strong growth (from 37.5% of respondents in 2019 to 62.5% in 2021). This suggests business messaging is now taking on greater importance, and a bad subscriber experience can hamper the brand image.

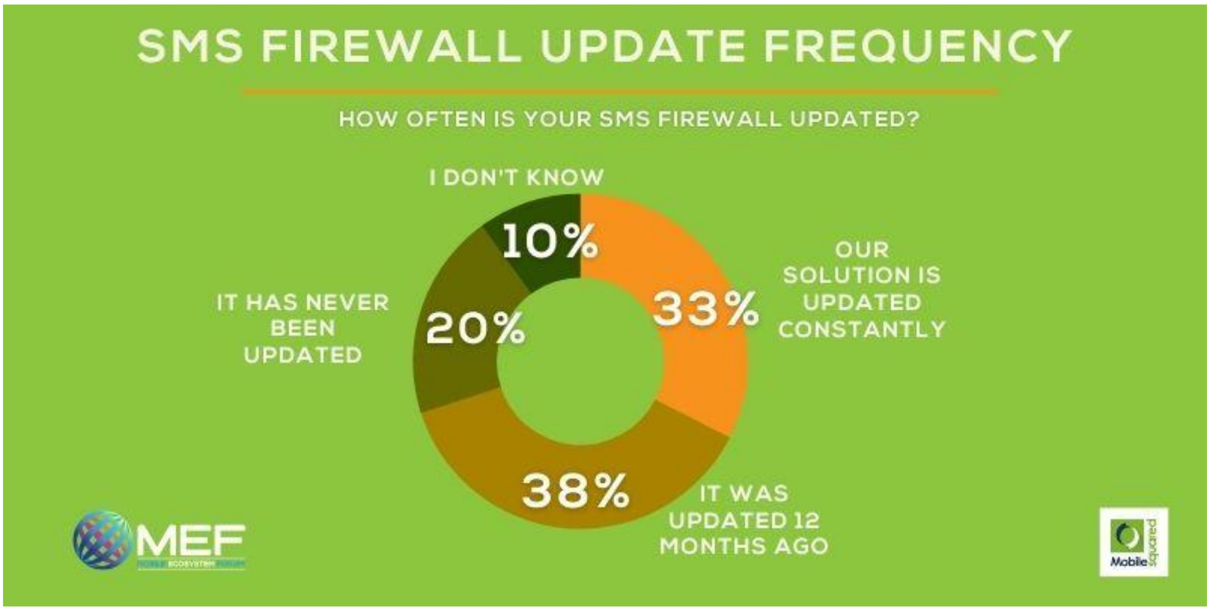
03

THE CHANGING FACE OF MESSAGING FRAUD

One of the possible explanations as to why messaging fraud is above "acceptable levels" is the fact that one-third of mobile operator respondents update their SMS firewall constantly. While a further 37.5% said that their system had been updated 12 months ago, that is a very long time in the extremely fluid environment of business messaging fraud where a lot can change in a short period of time, let alone one year.

Potentially, two-thirds of SMS firewalls are likely to be prone to the latest attacks due to a lack of data traffic intelligence. Indeed, one-third of mobile operators are vulnerable to attacks as 20% stated that their solution had never been updated and 10% did not know.

Figure 10: How often is your SMS firewall updated?



Q11: When did you last update your messaging fraud detection solution? (Select one)

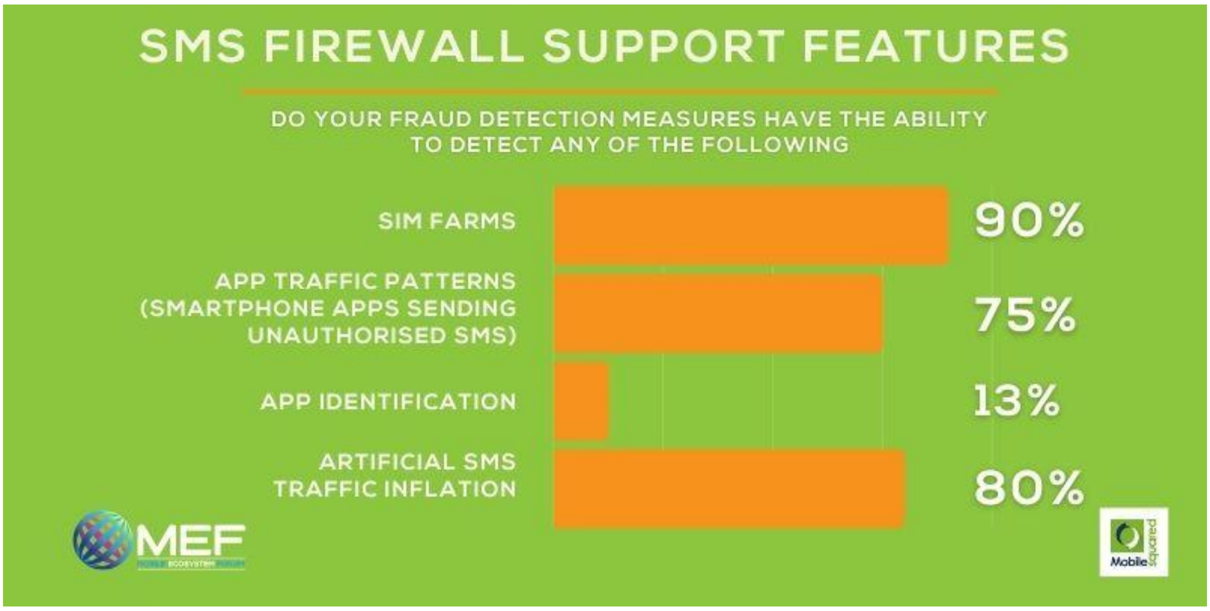
Source: Mobilesquared/MEF research

Despite the limited number of SMS firewalls being updated, it is grey routes that continued to be the biggest threat to revenues in 2020, as they were in 2019. What has changed since the last piece of research, was that spam and SIM farms were also viewed as the biggest threat to revenues. In 2020, just 28.1% of mobile operator respondents view SIM farms as having the biggest impact on

A2P SMS monetisation, and 25% spam. This suggests SMS firewalls are now performing effectively against SIM farms and spam.

In terms of what can be detected, on average, 81.7% of mobile operators said that their SMS firewall could detect SIM farms, artificial SMS traffic inflation, and app traffic patterns. Just 12.5% said that their SMS firewall could detect app identification. Very few respondents expressed an interest in revenue assurance and fraud management IT system, subscriber reporting, and traffic abnormality reporting.

Figure 11: Supporting features



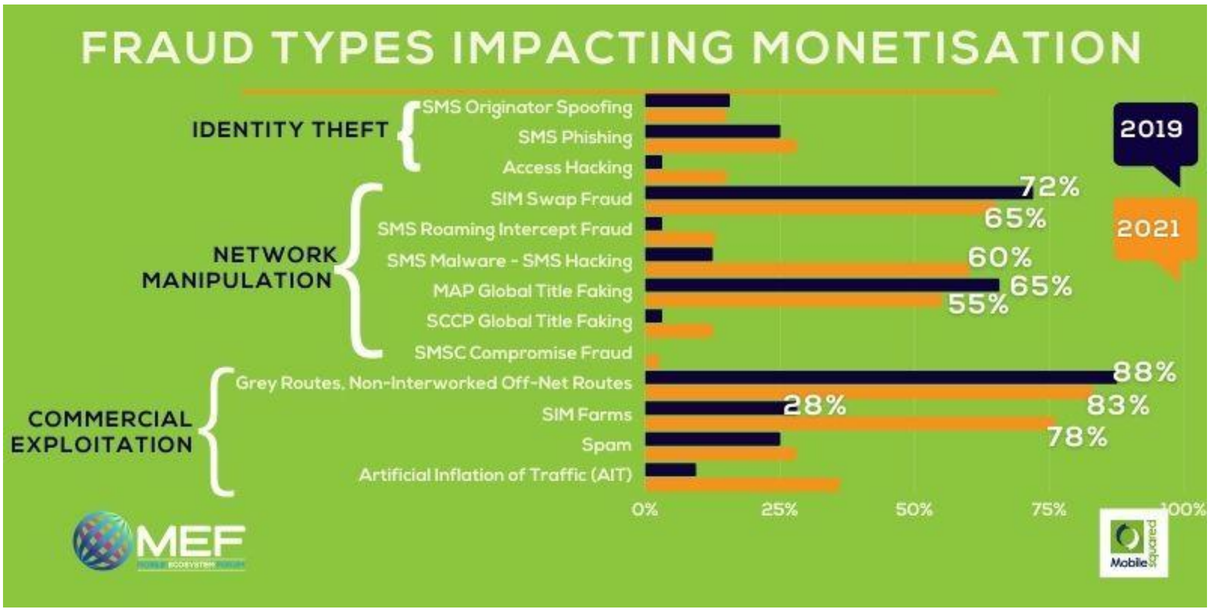
Q9: Do your fraud detection measures have the ability to detect any of the following: (select all that apply)

Source: Mobilesquared/MEF research

In 2020, after grey routes, the top fraud types impacting A2P SMS monetisation were SIM swap and MAP global title faking. The research clearly highlights how the threat is evolving, and why SMS firewalls need constant updating.

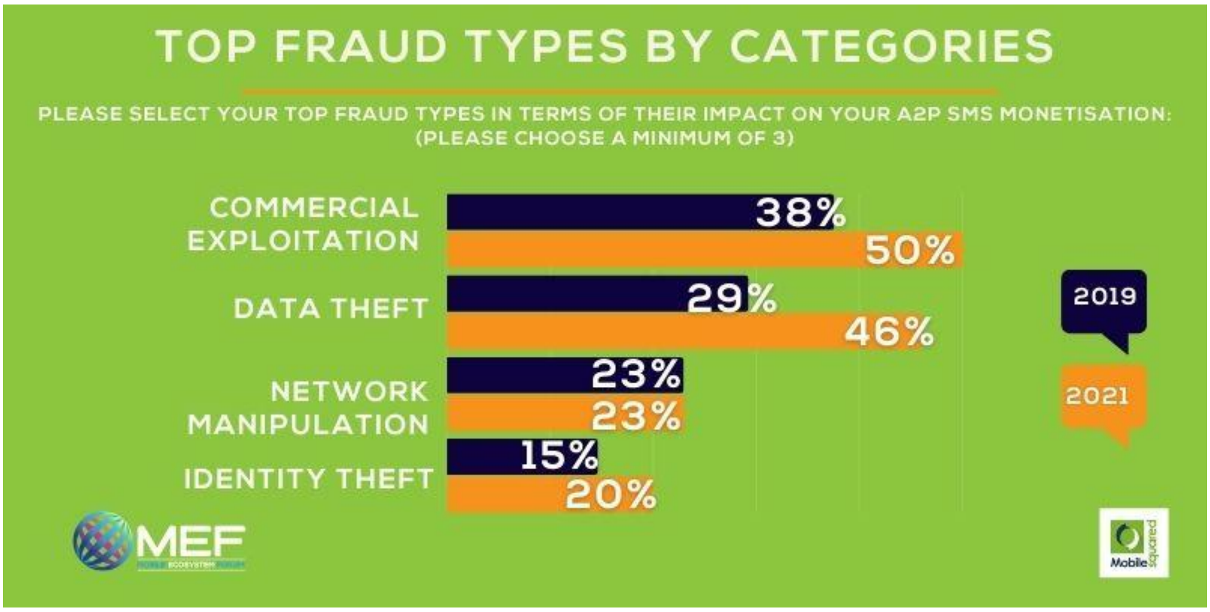
These three biggest impacts on A2P SMS monetisation are from three of the four fraud category types identified by the MEF; commercial exploitation, network manipulation and data theft, with the former viewed as having the most impact on revenues.

Figure 12: Fraud impacting A2P



Source: Mobilesquared/MEF research

Figure 13: Top Fraud Types



Q20: Please select your top fraud types in terms of their impact on your A2P SMS monetisation: (Please choose a minimum of 3)

Source: Mobilesquared/MEF research

Table 5: Risk by Fraud Types

	What fraud types pose the greatest risk?	2019	2021
Identity Theft	SMS Originator Spoofing	15.63%	**15.00%**
	SMS Phishing	25.00%	**27.50%**
	Access Hacking	3.13%	**15.00%**
Data Theft	SIM Swap Fraud	71.88%	**65.00%**
	SMS Roaming Intercept Fraud	3.13%	**12.50%**
	SMS Malware - SMS Hacking	12.50%	**60.00%**
Network Manipulation	MAP Global Title Faking	65.63%	**55.00%**
	SCCP Global Title Faking	3.13%	**12.50%**
	SMSC Compromise Fraud	0.00%	**2.50%**
Commercial Exploitation	Grey Routes, Bypass, Non-Interworked Off-Net Routes	87.50%	**82.50%**
	SIM Farms	28.13%	**77.50%**
	Spam	25.00%	**27.50%**
	Artificial Inflation of Traffic (AIT)	9.38%	**12.50%**

Table 6: Fraud Type – Top 3 Choices

FRAUD CATEGORIES (TOP CHOICES)	2019	2021
Identity theft	14.6%	19.17%
Data theft	29.2%	45.83%
Network manipulation	22.9%	23.33%
Commercial exploitation	37.5%	50.00%

Q21: Please select the top fraud types that you believe will pose the most risk to your network in 2021? (Please choose a minimum of 3)

Source: Mobilesquared/MEF research

If we remove the monetisation impact and just focus on what mobile operators believe will pose the most risk to their network in 2021, grey routes continue to come out on top, along with MAP global title faking which continues to be an area of concern, but so too are SIM swap and SMS malware. However, mobile operators also listed SIM farms as an area of concern despite claiming they were not one of the main fraud types negatively impacting their revenues in 2020.

While doing a direct comparison between the questions is difficult as the impact on 2020 was focused on monetisation, and the forward-looking impact in 2021 is restricted to their risk assessment, it does reveal that the impact on monetisation was largely limited to three fraud types in 2020, whereas the potential risk threat for 2021 has broadened to five fraud types.

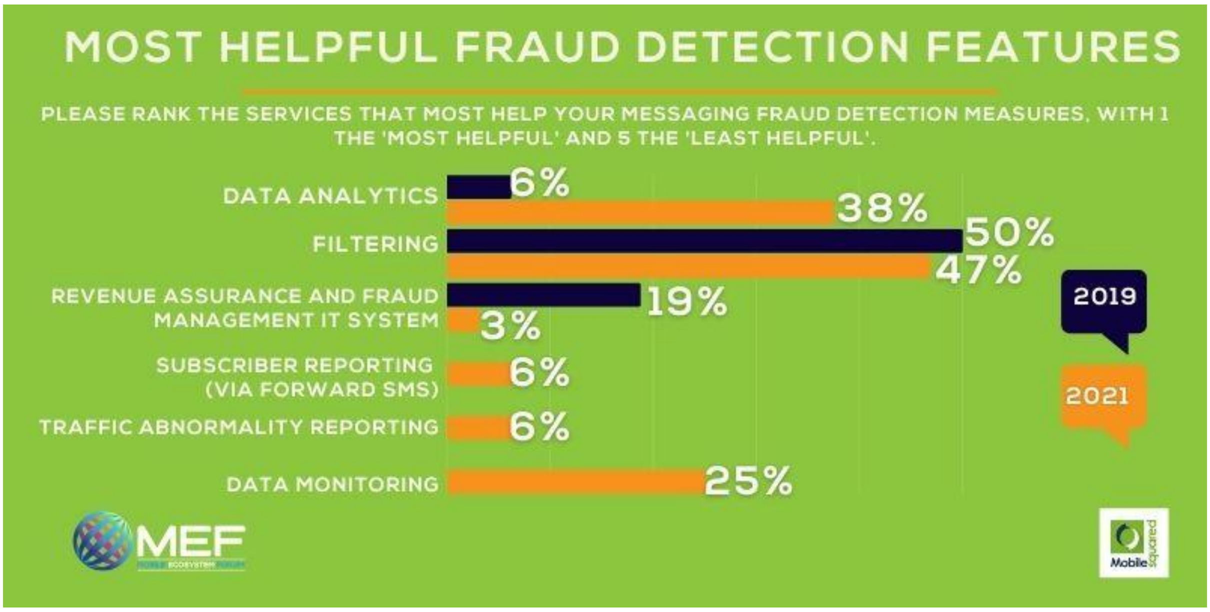
The research data suggests mobile operators are anticipating an increase in fraudulent traffic in 2021. And if we again look at the threat by categorisation, that provides the clearest indication of where the threat is likely to come from. On average, commercial exploitation (with 50% of mobile operator respondents selecting fraud types within this category) continues to pose the greatest risk, however, 45.8% of mobile operator respondents selected fraud types within data theft, compared to 29% for the monetisation impact question.

On average, an additional 16.7% of mobile operator respondents selected data theft fraud types compared to the previous monetisation impact question, an additional 12.5% selected commercial exploitation, and 4.6% identity theft. Network manipulation remained the same.

Mobile operators anticipate Identify theft fraud to increase marginally, expect an increase in commercial exploitation, and a big increase in data theft. Perhaps not surprisingly, data analytics looks set to play a defining role in the protection of networks moving forward.

Data analytics is now playing an instrumental role in MFDS, with a significant leap in mobile operator respondents identifying data analytics tools and data monitoring (37.5%) as key fraud detection measures compared to 2019 (6.3%). Although just as it was in 2019, filtering remains the most helpful of the messaging fraud detection measures. Regardless, data analytics is seen as key intelligence in the fight against an anticipated increase in fraudulent A2P SMS traffic in 2021.

Figure 14: Firewall Features



Source: Mobilesquared/MEF research

Table 7:

Q14: Please rank the services that most help your messaging fraud detection measures, with 1 the 'most helpful' and 5 the 'least helpful'. (Top 2 answers)	2019	2021
Data analytics tools	6.25%	37.50%
Filtering	50.00%	46.88%
Revenue assurance and fraud management IT system	18.75%	3.13%
Subscriber reporting (via forward SMS)	n.a.	6.25%
Traffic Abnormality reporting	n.a.	6.25%
Data monitoring	n.a.	25%

Source: Mobilesquared/MEF research

What measures would mobile operators like to see implemented to help tackle fraud in 2021? **Sixty percent of respondents selected sender id registry initiatives, with 42.5% selecting more regulation**. A quarter of respondents believe a joint code of conduct and an aggregator code of conduct would be beneficial, while 22.5% also selected a mobile operator code of conduct and mobile operator education. Responses clearly outline the need for a number of initiatives to help protect the marketplace, and of course, consumers.

Figure 15: What other measures should the industry do to tackle fraud?

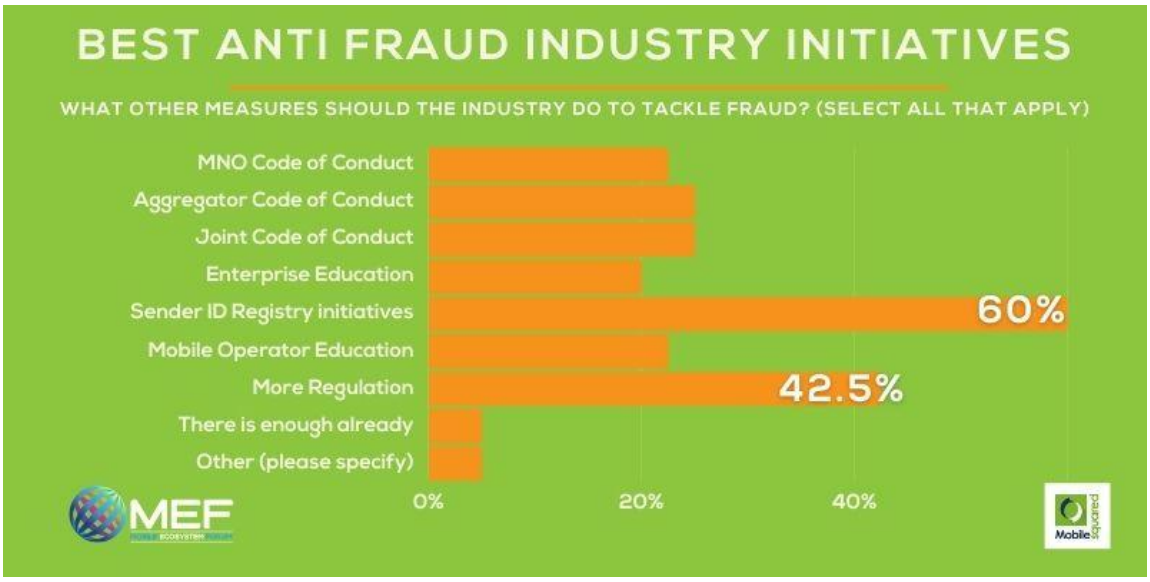


Table 8

Initiatives	2021
MNO Code of Conduct	22.5%
Aggregator Code of Conduct	25%
Joint Code of Conduct	25%
Enterprise Education	20%
Sender ID Registry initiatives	60%
Mobile Operator Education	22.5%
More Regulation	42.5%
There is enough already	5%
Other (please specify)	5%

Q23: What other measures should the industry do to tackle fraud? (Select all that apply)

Source: Mobilesquared/MEF research

The research from 2021 reveals that mobile operators are proactively tackling the threat posed by messaging fraud which they expect to escalate in 2021. Their strategy is shifting towards taking greater ownership of the SMS firewall solution by looking to bring its control in-house. Whether this is the correct strategy or not remains to be seen, but mobile operators should not operate in isolation, as this is a global problem that is not going away any time soon.

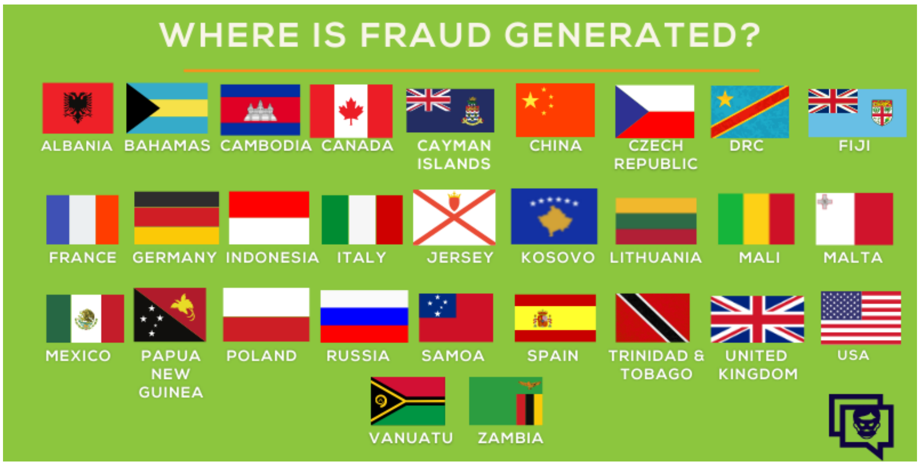
What is required, whether it is provided by an individual managed service provider or a trade body like the MEF or GSMA, is the amalgamation of network data intelligence from multiple global sources to ensure mobile operators are aware and in command of the threats and attacks to their networks.

To exacerbate the fact that network threats and attacks are a global problem, when asked wh**ere the fraud is generating from, the list of countries was long and varied,** not to mention the number of times regions were also stated as an answer. And of greater concern, a significant number of these countries are supposedly "locked down" with every mobile operator running an SMS firewall.

The countries reported Albania, Bahamas, Cambodia, Canada, Cayman Islands, China, Czech Rep, Democratic Republic of the Congo, Fiji, France, Germany, Indonesia, Italy, Jersey, Kosovo, Lithuania, Mali, Malta, Mexico, Papua New Guinea, Poland, Russia, Samoa, Spain, Trinidad & Tobago, UK, US, Vanuatu, and Zambia.

Regions listed as part of a response: Africa, Americas, Asia, Caribbean, CIS region, Europe, ex-USSR states, North Africa, Small islands.

Figure 16: Geographical origin of fraud attacks



Q15: What are the top 5 countries where SMS fraud originates? (Please list up to 5 countries)

Source: Mobilesquared/MEF research

04

APPENDIX

The research was an online survey of mobile operators running from December 2020 to April 2021. In total 66 mobile operators participated in the research, including Polkomtel, Unitel, Libyana, Deutsche Telekom, eir, Hutchison Drei, MegaFon, Omantel, Millicom, Tunisie Telecom, Bell Mobility, Etisalat, Nuevatel PCS, Sunrise, China Mobile, Bharti Airtel, Telia (multiple markets), Telefonica (multiple markets), Deutsche Telekom, AT&T mobility, Vodafone (multiple markets), MTN (multiple markets), Swisscom, Telenor (multiple markets), True Corporation, Bouygues Telecom.

Job titles of respondents include: Privacy Officer, Chief Engineer, Director Risk, Fraud and Security, interconnection Manager, Mobile Identity & Fraud Consultant, Senior Fraud Expert, Head of Fraud, Head of Wholesale Strategy & Services, Revenue Assurance & Fraud Manager, Fraud prevention and revenue assurance director, Engineer, Senior Manager, RA Manager, Security Executive Director, Senior Solution Architect, Director/Voice-Mobile Service & Interconnection, Network Security Specialist, Product Head, Sr Messaging Specialist, Product Strategy Lead, Head of Financial & Enabling Services, Chief Architect, Group Manager: Messaging Core Architecture, Fraud Manager.

Geographies covered in the research include: UK & Ireland, South Africa, Poland, Angola, Libya, India, Kazakhstan, Germany, Austria, Malta, Russia, Oman, USA, Tunisia, Canada, UAE, Bolivia, Switzerland, Brazil, India, France, Zambia, Yemen, Uganda, Syria, Sudan, Rwanda, Ivory Coast, Cameroon, Ghana, Afghanistan, South Sudan, Liberia, Guinea Bissau, Areeba Guinea, Eswatini, Congo, Benin, Nigeria, Iran, Thailand.

Established in 2000, the Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. As the voice of the mobile ecosystem it provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that delivers trusted services that enrich the lives of consumers worldwide.

Launched in 2015, MEF's Future of Messaging Programme is a dedicated industry programme that promotes a competitive, fair and innovative market for mobile communication between businesses and consumers. Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of messaging solutions
- Promote business messaging as a premium and trusted channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving messaging landscape
- Develop the value-chain to support new use cases

ABOUT MOBILESQUARED

The Mobilesquared team have been covering mobile since phones were brick-sized, and have tracked the evolution of mobile data and technology every step of the way.

We are immersed in the mobile industry – sitting on the judging panel for the MEFFYs, EMMAs, and Global Mobile Awards, delivering the Annual Market Review report for UK regulator Phone-paid Services Authority (PSA), and partnering with global mobile trade organisations including the Mobile Ecosystem Forum (MEF).

Anam is the world leading provider of Messaging security solutions and services for Mobile Operators. Specialising in grey route A2P monetisation, fraud detection & hubbing, our systems process billions of messages daily across 85 countries for more than 700M subscribers.

Our global team of SMS & A2P consultants use firewall, routing, analytics, visualisation & reporting technologies to generate new revenues from A2P, protect subscribers against SPAM and fraud & deliver operational messaging efficiencies for global Mobile Operators. Our customer base spans 5 continents and includes many of the world's Tier 1 MNO's including MTN, Orange, Telenor, Maxis, Tele2, Etisalat & Digicel Group.

We are headquartered in Dublin, Ireland with regional sales offices in Malaysia & Kenya. The company has substantial worldwide support footprint incl Czech Republic, Egypt, El Salvador, France, Jamaica, Malta, Nigeria, Russia, Pakistan & Vietnam. Year on year since 2017, Anam has been rated No 1 SMS Firewall vendor in global industry research.

Visit www.anam.com for more details.

ABOUT TATA COMMUNICATIONS

Tata Communications is a digital ecosystem enabler that powers today's fast-growing digital economy. The company enables the digital transformation of enterprises globally, including 300 of the Fortune 500, unlocking opportunities for businesses by enabling borderless growth, boosting product innovation and customer experience, improving productivity and efficiency, building agility, and managing risk. With its solutions-oriented approach, proven managed service capabilities and cutting-edge infrastructure, Tata Communications drives the next level of intelligence powered by cloud, mobility, Internet of Things, unified communications, security, and network services. Tata Communications carries around 30% of the world's internet routes and connects businesses to 60% of the world's cloud giants and 4 out of 5 mobile subscribers.

The company's capabilities are underpinned by its global network, the world's largest wholly owned subsea fibre backbone and a Tier-1 IP network with connectivity to more than 200 countries and territories.

www.tatacommunications.com

MOBILE ECOSYSTEM FORUM

MOBILEECOSYSTEMFORUM.COM

Disclaimer

Mobile Ecosystem Forum makes no representation, warranty or undertaking with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this report. The document was developed by MEF in collaboration with its members in full compliance with the programme's antitrust compliance policy. The information contained in this document may be subject to change.

Please check for the latest versions online.