MEF FUTURE OF MESSAGING PROGRAMME

Mobilesquared Databooks

The impact of fraud on A2P SMS monetisation

A report for the Mobile Ecosystem Forum by Mobilesquared

Published December 2019

Key Messages

- Grey routes are expected to cost the mobile network operators almost US$50 billion between 2018-2023. It is a revenue assurance imperative for mobile network operators to fight A2P business messaging sent via unregulated channels for P2P traffic.
- Market education is required with 60% of mobile network operators having not yet sufficiently protected their network from grey-routes and other A2P fraud by investing in fraud prevention solutions such as firewalls.
- For those mobile network operators that have made the investment, increased messaging revenue not fraud prevention is the key success measure (70%).
- Mobile network operators need to keep the A2P SMS channel secure and clean from fraud to ensure prolonged consumer trust, and a safe environment for brands to communicate with their customers.
- A fraud-ridden channel will drive brands and enterprises to alternative OTT messaging platforms, such as WhatsApp. The list of potential fraud types attacking SMS is considerable and an ongoing challenge for all stakeholders in the business messaging ecosystem. The industry can still defend the long-term position of SMS as the cleanest and reliable communication mechanism, but this requires a collaborative approach across the ecosystem.

Introduction

The global A2P SMS messaging market was worth US$14.75 billion in 2018 and will increase to US$16.58 billion in 2023, but it could be significantly higher. Grey routes continue to blight the A2P SMS marketplace, Mobilesquared's annual A2P SMS market forecasts revealed that grey route traffic has increased over the last 18 months and continues to cost the A2P SMS ecosystem billions of dollars in revenue leakage every year.

At the same time, while not all traffic carried via a grey route is malicious, the majority of fraudulent traffic that traverses the world is carried over a grey route. In addition, SIM farms continue to disguise A2P traffic as P2P SMS and exploit the mobile network operators (MNOs). This resurgence in grey route traffic confirms that fraud remains as much as a threat to MNOs and their subscribers, as it ever has.

Mobilesquared has conducted a survey of 22 MNOs on behalf of the Mobile Ecosystem Forum (MEF) to explore the impact fraud has on the market. As part of its industry best practices, MEF's Future of Messaging Programme participants identified 13 fraud types in its Enterprise Messaging Fraud Framework. This paper sets out to better understand how MNOs are reacting to these threats to the A2P ecosystem.

Section 1: The evolution of firewalls

SMS Firewalls

The starting point for an MNO to block fraudulent traffic is the investment of a next-generation SMS firewall. First-generation SMS firewalls were deployed to block unwanted spam from reaching the subscriber's SMS inbox. Today, the threat to subscribers has multiplied; spam is just one of 13 fraud types identified by MEF. Given this abundance of fraudulent traffic, first-generation SMS firewalls have been rendered largely ineffective.

Fraud Types classification

Commercial Exploitation	Grey Routes, Bypass, Non-Interworked Off-Net Routes	SIM Farms	Artificial Inflation of Traffic (AIT)
Data Theft	SIM Swap Fraud	SMS Roaming Intercept Fraud	SMS Malware - SMS Hacking
Identity Theft	SMS Originator Spoofing	SMS Phishing	
Network Manipulation	SMSC Compromise Fraud	MAP Global Title Faking	

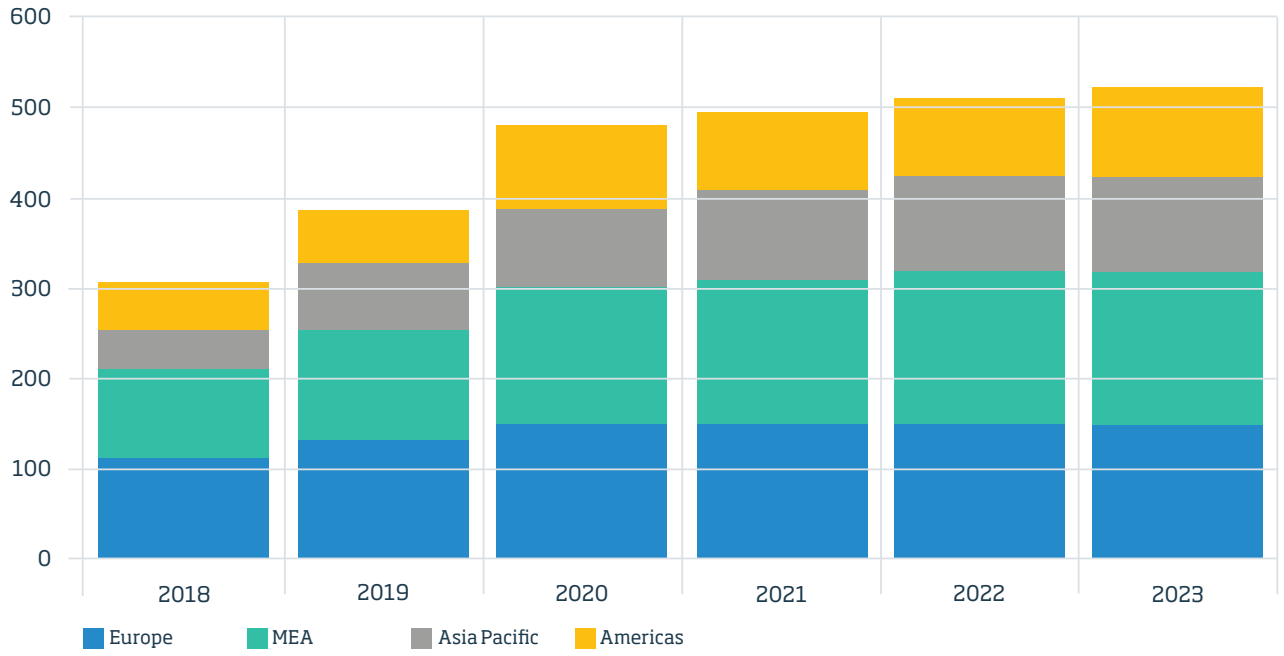
MNOs are central to nullifying the threat of all fraud types and unlocking the revenue potential of A2P SMS messaging. Investment in a next-generation SMS firewall provides greater visibility of traffic and enables MNOs to identify every message in order to detect and block the fraudulent SMS. In setting up monitoring alerts and rules on the SMS firewall to filter the traffic, MNOs will not only prevent network abuse and stop grey routes from terminating on their network, but it also only allows billable 'white' route traffic.

Mobilesquared published its updated A2P SMS global forecasts in October 2019, and as part of the research revealed that the number of MNOs that will invest in a next-generation SMS firewall will increase from 307 as of end 2018 to 517 by 2023. That means 40.9% of 750 MNOs have invested in an SMS firewall, and that will increase to 68.9% by 2023.

At the end of 2018, 48.3%[1] of mobile operators had effectively "locked down" their network having invested in a next-generation SMS firewall. Europe accounted for 38.8% of total deployments, ahead of Middle East & Africa (MEA) on 27.4%, the Americas on 17.6% and Asia Pacific on 16.3%. By 2023, 81.3% of MNOs will have invested in a next-generation SMS firewall.

[1] Mobilesquared global forecast universe covers the top 200 markets and includes 636 mobile operators.

Fig. 1: Mobile operator next-generation SMS firewall deployments (2018-23)



Mobile operator deployments

As an increasing number of MNOs are locked down and the number of grey routes is reduced, companies looking to exploit commercial loopholes will continue to probe networks with a view to uncovering new grey route opportunities.

This may include fraudulent activity, such as SMS intercept, which attacks the SS7 signalling network, and potentially exposes mobile customers to phishing activities, for example. As two-factor authentication (2FA) maintains its growth using SMS, security messages are particularly vulnerable to such fraud attacks.

MNOs risk their brand reputation, the loss of customer trust, increased churn and reduced revenues, were they to suffer an SS7 interception attack.

To ensure SMS is accepted as a long-term delivery mechanism MNOs can further protect their network with an SS7 firewall, which inspects signalling traffic in real time.

However, this is a difficult internal sell, because while an SMS firewall prevents fraudulent network activity it also delivers a direct return on investment from A2P SMS termination revenue. Whereas an SS7 firewall safeguards the A2P SMS revenue by protecting the traffic but does not generate direct revenues.

Based on our research, Mobilesquared estimates that less than 10% of MNOs had invested in an SS7 firewall as of end 2018. Mobilesquared expects slow growth in SS7 firewalls during the forecast period, with around one-third of MNOs using them by the end of 2023.

The research reveals that the MNOs driving the SS7 firewall deployments will be major mobile operating groups and mobile operators with scale (Tier 1s), as they look to protect their brand and subscription base. Deployments are expected to then filter down based on market size.

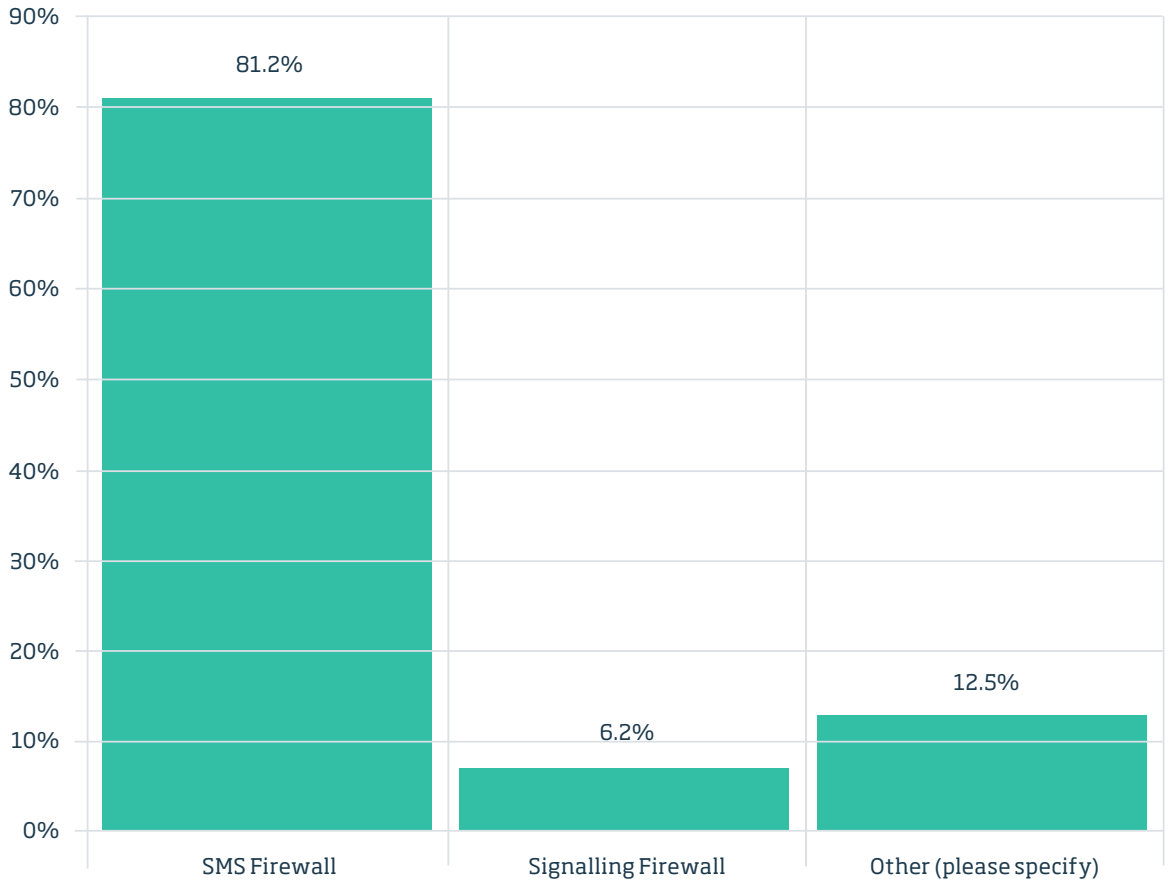
This indicates that SS7 firewalls are viewed as a secondary investment by the MNOs, with their primary focus on revenue generation via an SMS firewall.

Section 2: Survey Findings

So how is the threat of fraud dictating mobile network operator strategy?

Every MNO participating in the survey has protected their network with a revenue assurance platform. A breakdown of this figure reveals that 81% of respondents have invested in an SMS firewall, 12% had invested in both an SMS firewall and an SS7 firewall, and 6% invested in just an SS7 firewall.

Fig. 2: Which of these measures do you use to help protect against fraud?

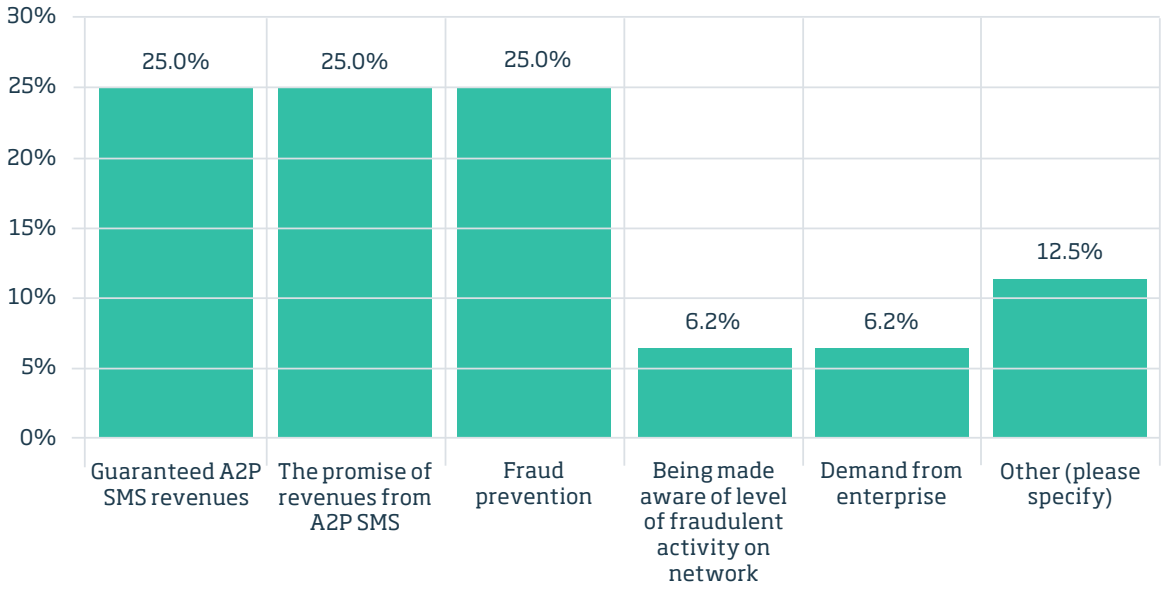


The overriding factor driving this investment in firewalls is monetisation of A2P SMS.

The survey revealed that protecting existing A2P SMS revenues and the promise of A2P SMS revenue growth, as well as fraud prevention, are central justifications for investing in an SMS revenue assurance platform.

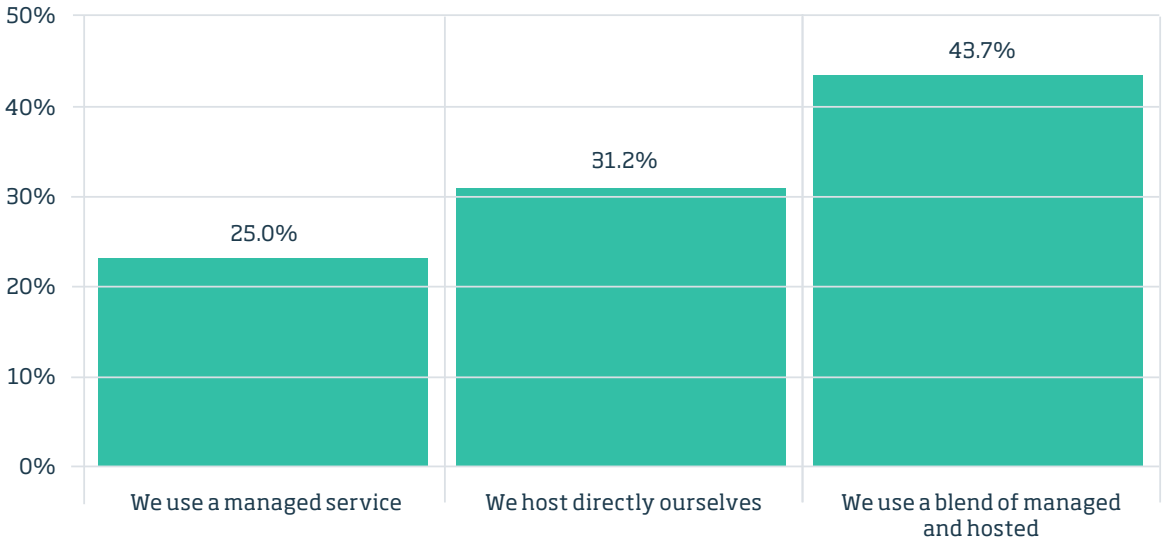
SMS firewalls are clearly viewed by MNOs as a monetisation platform, whereas an SS7 firewall is purely a fraud prevention service designed to protect A2P SMS revenue generation and a mobile network operator's brand.

Fig. 3: What was the main factor behind investing in an SMS revenue assurance platform?



When quizzed on the management of the firewall, the majority of MNOs (43.75%) said that they used a blend of managed and hosted services, almost one-third (31.25%) host the firewall themselves, leaving one-quarter to use a managed service.

Fig. 4: Do you use managed services solutions for A2P SMS or do you host and manage your services directly?



Mobilesquared research revealed that networks are likely to be more protected using a managed service as opposed to hosting directly in order to maintain and update the required filtering rules to ensure the firewall can identify grey traffic entering the network.

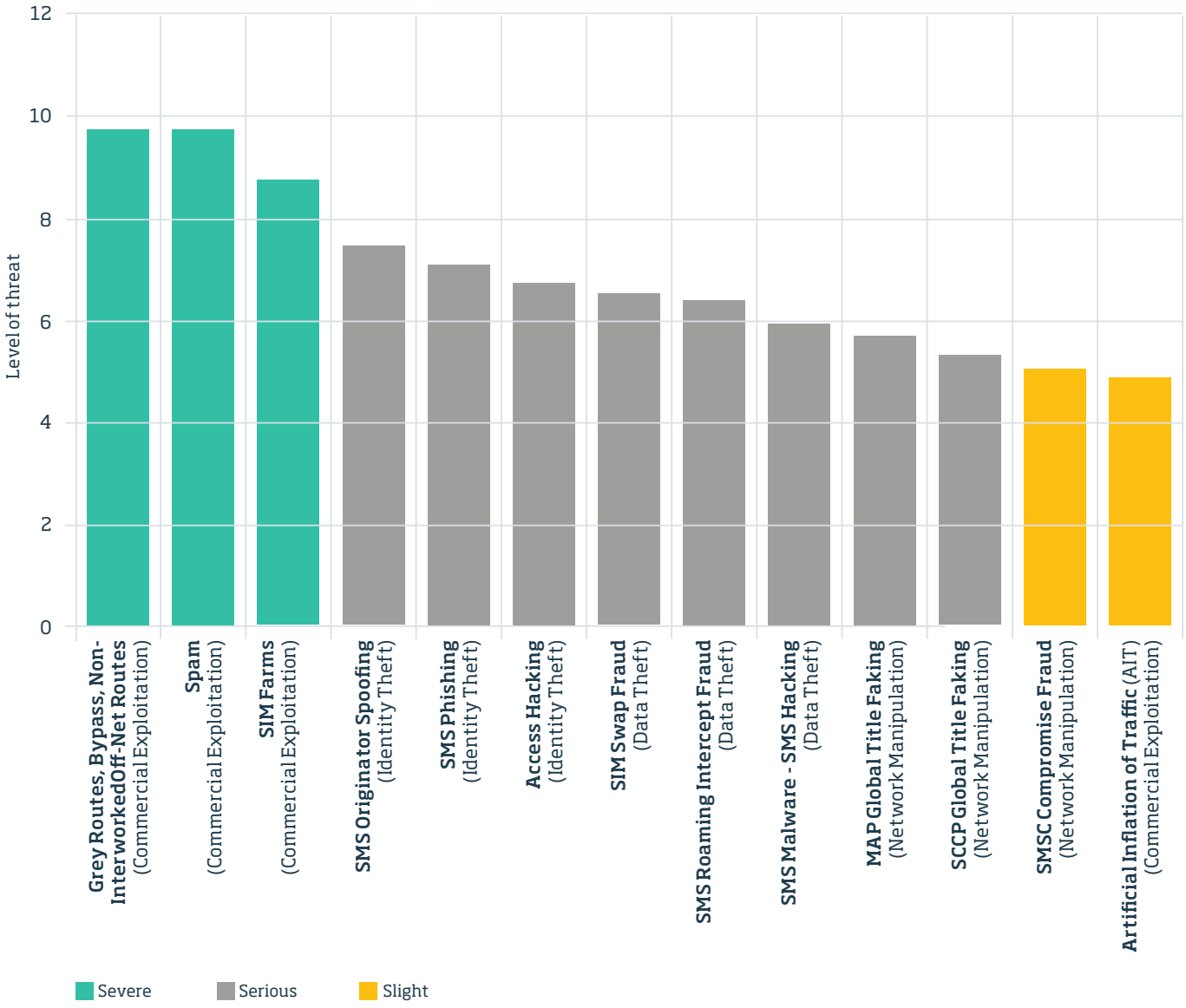
Grey-route traffic

Given the survey findings, monetisation will clearly drive more MNOs to invest in next-gen SMS firewalls. Subsequently, Mobilesquared expects the swing from grey-route to white-route A2P SMS traffic to drop from 599.25 billion in 2018 to 509.91 billion in 2023. Over this period the market share of grey routes will fall from 38.6% of total A2P SMS to 33.4%.

This of course still means fraudulent SMS traffic continues to have a massive distribution platform. Based on the survey responses, Mobilesquared has categorised these A2P SMS threats on monetisation as "Severe", "Serious" and "Slight".

The Severe threat to monetisation is linked purely to commercial exploitation, with grey routes and spam viewed as most damaging, followed by SIM farms. Serious threats cover a broader range of threats from identity theft, to data theft, and network manipulation, with SMS Phishing (Smishing) and Faking the leading categories. Slight threats are restricted to just two fraud types covering network manipulation and commercial exploitation.

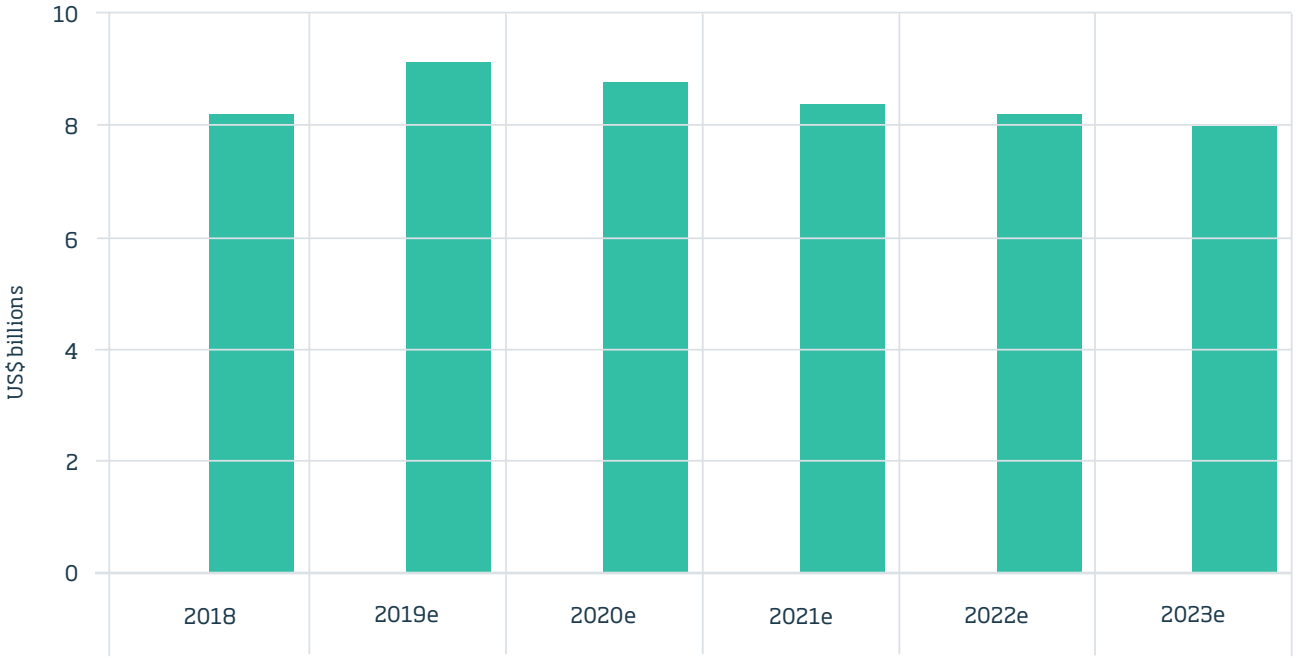
Fig. 5: Fraud types classification



Mobile network operators missing out on $50 billion

Mobilesquared estimates that if all grey-route A2P SMS messaging were instantaneously converted into white-route traffic starting in 2018, this would potentially generate an average of US$8.32 billion each year over the forecast period for a cumulative total of US$49.93 billion.

Fig. 6: Grey route traffic costing MNOs US$50 billion between 2018-2023



The impact of fraud in a grey world

Grey route traffic is having a negative impact on potential A2P SMS income. More alarmingly is the threat that this traffic can carry in terms of fraud, which can create lasting, and often irreparable brand damage to the MNO.

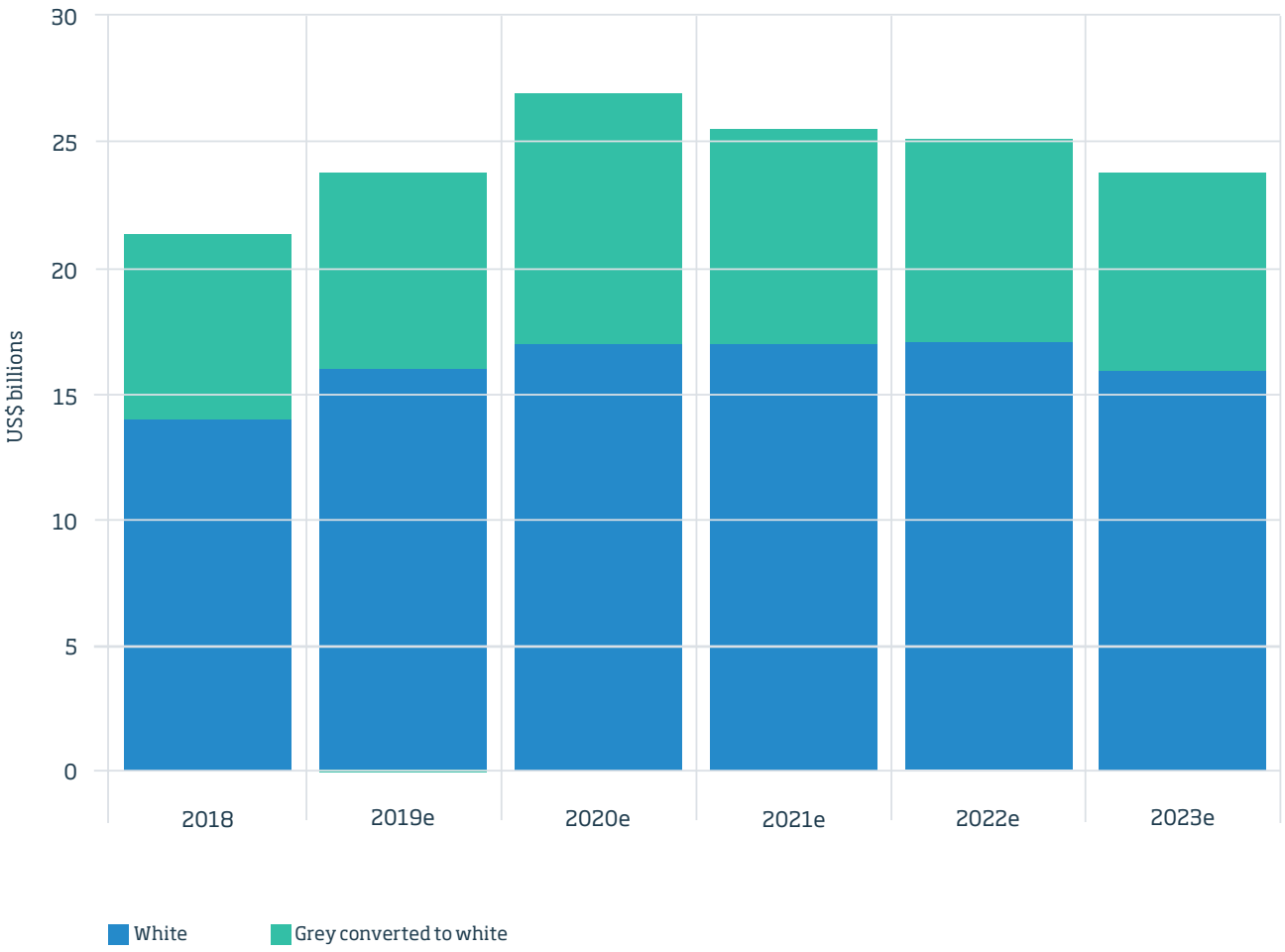
The sooner MNOs implement a next-generation SMS firewall, the sooner grey route traffic can be converted into white-route income, and MNOs can restrict the fraudulent threat to the A2P SMS marketplace.

By applying the converted "grey-to-white-route income" to white-route income projections, it reveals potential A2P SMS messaging income of US$22.89 billion in 2018 (compared to US$14.75 billion), peaking at US$26.49 billion in 2021, and ending 2023 with US$24.46 billion — currently projected to be worth US$16.58 billion in 2023.

These lost revenues from the 60% of MNOs yet to invest in an SMS firewall, indicates that education is still required as to the benefits of why networks need to be locked down.

What's more, MNOs need to keep the A2P SMS channel clean from fraud to ensure prolonged consumer trust, and a safe environment for brands and enterprises to communicate with their customers. A fraud-ridden channel will drive brands and enterprises to alternative OTT messaging platforms, such as WhatsApp.

Fig. 7: Total A2P SMS revenues (2018-2023)



MEF Comments

Mobilesquared's survey underlines the focus for mobile network operators is on revenue assurance. This is a logical first step: Closing down grey routes was already identified as key A2P industry priority when MEF's Future of Messaging Programme was first established in 2015.

While the findings highlight some encouraging progress, the research also identifies there is continued need to educate the market and enrol a larger number of MNOs.

Every MNO deploying an SMS Firewall is another step towards stopping unregulated enterprise messaging and mitigating the threat of fraud and every effort should be made to accelerate this important first phase towards the cleaning of the SMS enterprises messaging market. Revenue assurance benefits have made it an easier internal sell for MNOs: the ROI for a SMS firewall was generally easy to prove.

MEF is now calling for the industry to raise the bar further to protect the sustainability of business messaging. Greater attention needs to be placed for security and anti-fraud for the consumers. SMS is a premium delivery mechanism because of its efficiency and security. Email is free, but it cannot guarantee the response rate or security of SMS and the industry must maintain the features of this product.

As overall competition from other solutions intensifies (e.g. WhatsApp, Apple Business Communication, Line), SMS is under increasing scrutiny as an effective and secure communication mechanism. No communication channel is exempt from the attacks of fraudsters, none can claim to be a 100% 'secure channel'. However, proactive and consistent vigilance can make the difference. But how do we secure the ecosystem? It is unlikely that the MNOs are able to do this by themselves. Defending an investment in higher fraud security may be difficult to justify by an individual operator, which is why the future of the ecosystem needs to be tackled as an industry. Collaborative approaches to the issues of security should emerge and MEF is facilitating such discussions and ideas on how to bring the second phase of SMS security to life.

Dario Betti, CEO of MEF

Glossary

Acronym / Term	Explanation
2FA	A process which enables the confirmation of an individual's claimed identity by using a combination of two different components, namely: 1) something an individual possesses or is inseparable from them, 2) something the individual knows For example, a 2FA process for a mobile subscriber might require their being in possession of a mobile device, plus a PIN
A2P	Application-to-Person - Messages sent from an application to a device for a person to read
Firewall	A filtering system which enables MNOs to monitor, detect, block and report suspicious or unauthorised messages destined for delivery through their network and to their subscribers
Grey Route	The sending of business messages (A2P traffic) from a third country under the guise of person to person (P2P) messages in order to take advantage of lower (or no) interconnect charges between networks.
MNO	Mobile Network Operator
OTT	"Over the Top": Internet messaging solutions providing a service on mobile devices without going through the MNO billing system
P2P	Person-to-Person Messages sent between users for personal communication.
Phishing	Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication
SMS	Short Message Service
Spam	Messages sent for deliberate misrepresentation for fraudulent purposes by an illegitimate business OR aggressive marketing messages without consent by a legitimate business OR violation of acceptable use, poor communication and/or poor implementation of opt-out process by a legitimate business
SS7	Signalling System 7 A set of telephony signalling protocols that enable the sending of SMS messages as well as performing number translation, local number portability, prepaid billing and other mass market services.

About MEF

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.

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
- 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

Mobilesquared is #1 for business messaging intelligence.

Mobilesquared is the go-to partner for definitive business messaging intelligence, relied on by brands including Mastercard, LivePerson, Vodafone, and PricewaterhouseCoopers to inform messaging strategy. We own the most extensive in-house data forecasts in the industry, drawing on over 7 million dynamic data points across 200 markets and 650 mobile operators, to create our deep dive reports. We are also the only analysts invited to present our data at every major messaging conference internationally, in partnership with industry associations the MEF and the GSMA.

If you need accurate messaging market insight and future-proofed strategy, no one is better qualified to help.

Find out more about Mobilesquared at www.mobilesquared.co.uk

Disclaimer

Mobilesquared
Communicating data