FEBRUARY 2013 | WHITE PAPER

Assuring the future of SMS

SPONSORED BY

PUBLISHED BY

telecoms.com INTELLIGENCE
Getting the industry thinking

ABSTRACT/SUMMARY

SMS may be said by some to be at the start of a long-term decline, but its importance to operators is still vital, both in terms of brand value and revenue. The competitive landscape means that it is now more vital than ever that operators take steps to protect their assets by investing in two key areas - revenue assurance on SMS interconnect, and spam analysis and prevention. By doing this they will protect their own revenue streams, as well as ensure that their subscribers benefit from the best user experience.

INTRODUCTION

On 3 December 2012 the mobile industry marked the twentieth anniversary of what is widely regarded as the birth of SMS - the sending of a message from a PC to a mobile phone on the Vodafone network by engineer Neil Papworth. Two years after that milestone, Nokia released the first phone that allowed users to write and send SMS in an easy manner. What had started out as an interesting technical quirk - using the SS7 signalling network to carry text messages between devices - was on the path to becoming the key communication medium of the past twenty years.

SMS soon became a core part of mobile operators' revenues, and an even more important component of their profit line. One analyst estimated that in 2011 SMS had grown to account for 16% of the total mobile revenue generated by Western European operators.

NOT DEAD, STILL GROWING

Yet SMS' 20th anniversary was also marked with a series of articles hailing the "death of SMS". SMS, the argument went, itself once the usurper of the dominance of voice telephony was now in turn being usurped - this time by internet and social media-based messaging apps. Volumes were peaking in several major Western markets, including the USA for the first time. In Western Europe, revenues have been in slow decline since 4Q 2011. Vodafone UK reported a decline in messaging revenues of 1.2% in its Q1 results for 2012/2013. (Voice revenues declined by nearly 4.5%). In some countries, such as Spain and The Netherlands, there was a more marked decline in messaging revenues and volumes, driven by economic reasons in the case of Spain, and high level adoption of alternative technologies in The Netherlands. Informa Telecoms and Media's World Cellular Data Metrics found that the number of texts sent per month per user was in decline in the majority of the top 20 ranking operators for that metric. There were even one or two major declines: for example, between 2Q 2011 and 2Q 2012 Vietnam's S-Fone experienced a substantial decline in SMS sent per user per month of 81.9%, followed by Telemobil Romania (down 74%) and France's Bouygues Telecom (down 19.1%).

Although there are signs of a post-peak decline, there is also plenty to suggest that the "Death of SMS" narrative is one that struggles to carry the whole truth of SMS right now.

Informa Telecoms & Media's World Cellular Data Metrics estimated that in 2Q12 global SMS traffic actually increased 8.3%, to 2.2 trillion messages, up from 2.1 trillion messages in 2Q11. Another analyst estimated that SMS revenues will grow every year from 2012 to 2016, delivering a cumulative $1 trillion in operator revenue during those five years.

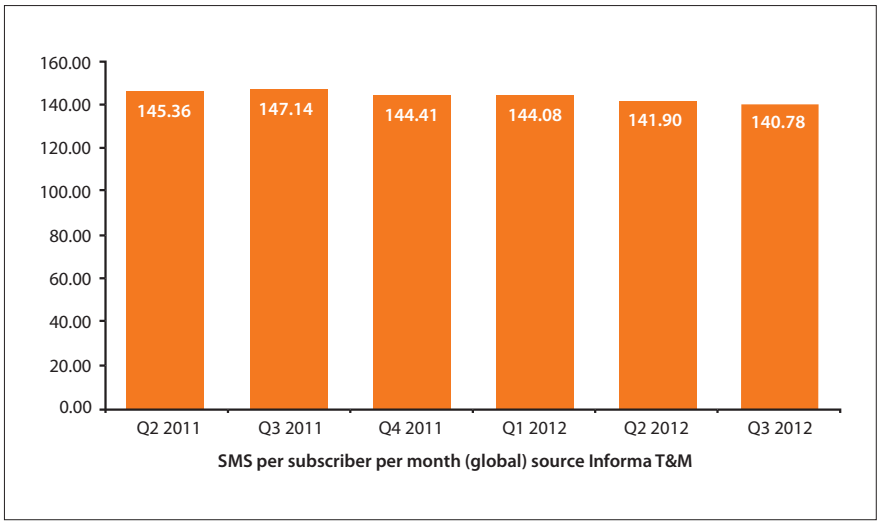
Even where there is evidence of an end to growth, the peak is relatively flat. 77% of the 266 operators tracked by Informa saw a year-on-year rise in their SMS-traffic volumes between 2Q11 and 2Q12. That's a strong number, although it represents a slight fall from Informa's SMS-traffic data for the year previously, when 83.1% of the 272 operators tracked experienced year-on-year growth. The French regulator, ARCEP, estimated that growth in overall volumes of SMS, and in the amount of SMS sent per user per month, only just levelled off in mid-2012, at which point users were sending, on average, 224 text messages per month, nearly three times the number per subscriber being sent just three years before.

What we are seeing, then, is still overall market growth, with a topping off of peak volume (not drastic decline) in some mature markets, and some statistical outliers seeing a steeper decline caused by specific market conditions.

CONTINUING RELEVANCE

Whatever the trends, the overall picture only illustrates the continuing strategic importance of SMS to operators, even as alternative technologies may threaten to erode volumes and, in combination with regulatory action and competition, revenues. It is also worth noting the continued importance of SMS to users. The technology, or rather the service, has shown the ability to adapt itself to a whole host of use cases, with the market seeing a great expansion in the application of SMS. SMS is now utilised by brands for marketing, advertising, vouchers, promotions and competitions; by transport and other organisations for customer messaging and ticketing; by banks and financial services companies for transactions, notification and security; by TV and media bodies for voting and viewer or listener interaction; by messaging companies to transcode emails to SMS, and vice versa, so that users in emerging markets or without internet connections can receive and respond to emails. Finally, SMS is a key bearer for much of the M2M market, delivering notifications and messages between enterprise platforms and endpoints across the globe.

In all of these cases the attractions of SMS are its cost effectiveness, its reliability and its



SMS per subscriber per month (global) source Informa T&M

availability. That ubiquity across devices and markets can still not be matched by the OTT or rival messaging applications. Of course, not every application benefits from ubiquity, but many - such as those listed above - do, and SMS looks set to remain the medium of choice for customer communication for a whole host of businesses. And it is where that ubiquity exists that carriers still have opportunity to extend revenues and their brand reputation.

Having established that SMS will continue to be strategically important to operators, it is also worth pointing out the very attractions of SMS as a communications channel also bring with it dangers for operators. Other parties, some of them not so welcome, also want to take advantage of SMS' ubiquity and cost-effectiveness.

Top-4 alternative messging services among users of these services, by country, October 2012

	France	Germany	Spain	UK
1	Skype (36%)	WhatsApp Messenger (76%)	WhatsApp Messenger (87%)	Skype (52%)
2	Facebook(34%)	Facebook(49%)	Facebook(31%)	Facebook (43%)
3	WhatsApp Messenger (14%)	Skype (43%)	Skype (30%)	WhatsApp Messenger (39%)
4	Google Talk (14%)	ICQ (17%)	Google Talk (15%)	BlackBerry Messenger (23 %)

Source: Analysis Mason

WHOLESALE ASSURANCE

Operators are alive to fraud and revenue assurance within their retail base, but many do not have the systems in place to make sure that they are also receiving their fair share from other service providers that are terminating messages on their networks.

One danger is that operators risk missing out on revenues due from messages that are terminated on their network but are sent by an originating party that does not have a wholesale commercial agreement with the terminating operator. This is the problem known as the grey route, where a service provider or SMS aggregator in another country delivers messages to end users in another without paying the terminating operator for delivery of those messages. They may do this either by exploiting an intermediary that does have a terminating agreement with the end operator, or by disguising the origin of the message and making the message appear to be national where it is actually international.

The aggregators make their money by exploiting margins gains made from terminating messages for free, or by selling access to marketing companies and others who are attracted by very cheap rates for the delivery of bulk SMS. Detection is not always so easy. Often the aggregators take care to make sure that although they are sending a lot of messages, they are not sending so many as to draw attention to themselves. They may also shift their number ranges around, so that as soon as an operator may notice a suspect number range and close it down, the service provider starts injecting messages from a new number range.

Analysis and live market experience from leading SMS analysis company HAUD Systems suggests that many operators are suffering from hidden losses that may total as much as 10-20% of their interconnection revenues. Consider that a typical estimate is that around 20% of overall SMS revenue is derived from interconnect revenues (Analysys Mason for reference), with the other 80% being accounted for by retail sales. We can see, therefore, that by addressing leakage through missed interconnection fees, an operator could claw back at least 2-4% of their overall SMS revenues. That would have been enough, for example, for Vodafone to have more than offset their Q1 2012/13 SMS revenue decline. (This is a theoretical example, of course).

Operators are also losing money by missing out on direct partnership deals with major internet based messaging providers. For instance, one operator found that a great many messages coming into its network were SMS notifications from a major internet-based email platform provider. This provider had done a deal with an aggregator to send messages to end-users. By analysing that traffic, the mobile operator was able to approach the internet company directly, and do a deal that was of benefit to both parties, by cutting out the middle-man aggregator.

HAUD Systems CEO Claire Cassar says,"Our SMS profiling services have found that, typically, around 10-20% of messages are either entering a network from sources that have no connection with the home operator, or are coming through aggregators carrying content

from banks or from big internet companies. Having that knowledge means that operators can then address those parties directly to negotiate delivery, so stemming the associated revenue leakage."

SPAM THREAT

Allied to loss of revenue from grey routes, the termination of messages sent by parties that fall outside agreed commercial interconnect arrangements can have other impacts upon the operator business.

Unsolicited or "spam" messages can lead to users calling back or replying to premium rate numbers, often racking up large bills doing so. Or the spam message may pretend to be offering a prize or free coupon if a user enters some personal details. Those details are then often sold on to third parties to exploit for marketing or fraudulent purposes. According to Cloudmark, the company that runs the GSMA's Spam Reporting Service, the number of unique SMS spam campaigns quadrupled in the first half of 2012 and the overall rate of receipt grew by 300% from 2011 to 2012.

Spam impacts directly upon the brand equity of a mobile operator. First, the reputation of the host operator suffers, as subscribers object to being targeted on their mobile device by third parties to whom they have not given permission. Second, spam can also be a factor in reasons to churn - as customers lose trust in their operator to protect their user experience .Thirdly, operators are trying to build up opt-in databases so that they may legitimately sell access to third parties for mobile marketing and advertising activities. Users that do not trust a brand to prevent spam are less likely to opt in and then respond to legitimate campaigns.

Finally, there is the increased cost of customer support, as operators field calls from angry or disappointed customers, or make counter-offers to disgruntled customers threatening to churn. Operators may even make offers to compensate users for financial loss caused by responding to a spam message.

The ability to recognise spam messages as they enter the network, and to be able to take action to block messages that look similar to those messages, and originate from unknown parties, could give operators a boost to customer satisfaction and net promoter scores, reduce customer support costs at the call centre, and increase future revenue opportunities to be gained from exploiting SMS as a true trusted medium.

PROTECT AGAINST REVENUE LEAKAGE AND SPAM

So how can operators take steps to defray revenue leakage, and guard against external spam?

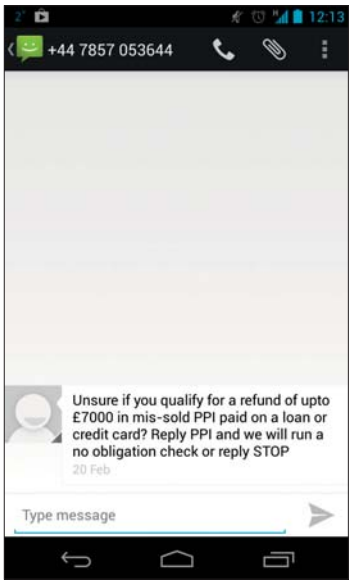
One thing operators can do to protect themselves against interconnection leakage is to make an attitudinal commitment not to let traffic enter their networks unless the sending party is identifiably on a white list. Spain, where all the operators have made just such an investment, is considered to be watertight and virtually impossible for aggregators using grey routes to terminate a message without paying the proper termination price. As a result, spam from external sources is virtually unknown in Spain, and wholesale SMS prices are among the highest in the world.

Similarly in Ukraine, their filtering systems are very timely and hence grey routes are quickly spotted. Hence the price for terminating messages to Ukraine are more stable and in fact most businesses wanting to terminate message in Ukraine need to avail of direct connections.

So why have not all operators gone down this route? One reason is that to date they have not seen the need to do so, having made a sufficient amount of revenue from their existing wholesale agreements. As overall SMS revenues come under pressure, then this may have to change.

A further barrier within operators has been that the fraud and revenue management teams who manage assurance are generally greatly overworked and under-resourced. Further, detecting wholesale leakage can look like something that requires a switch-level intervention or changes to core network elements and databases. Operating teams may not be aware that there are solutions that sit outside of the core switch architecture, and therefore don't require requests and changes from engineering teams.

HAUD Systems markets a software platform that can be installed at a neutral or operator-owned data centre, positioned on the SS7 Signaling Transfer Point (STP) gateway (STPG)



Spam SMS can cause revenue leakage for operators

for incoming or outgoing traffic. By sitting on the gateway, analysis and management can take place before the traffic enters the operators' core network. The system can be scaled up or down to need, and can easily process up to 10,000 messages per second through its filters simultaneously.

Reports can be generated on all traffic, both white-listed and black-listed, enabling operators to build a profile of all their incoming and outgoing messaging traffic. For instance, a responsible operator may want to make sure that it is not acting as the unwitting originating operator of spam messages being sent by an aggregator that has access to its sending network.

The system incorporates two features that give extra flexibility to the operator. PhraseBlock can recognise chunks of text that look like spam, and also similar text, and alert the operator to their presence, or act on a set policy and block the message. The operator can then enter those phrases into a database to enable future blocking of such messages. However, if such phrases are contained in messages originating with a whitelisted operator, then that would over-ride the block, and the message will be delivered. It can even recognise non-Roman script languages as graphics rather than text, so that messages in any language can be analysed with equal effectiveness.

Another module, BulkGuard, looks at every message coming through the system and detects patterns in the messages. If it finds 100 messages in a minute having semi-identical content, say 80 characters from 160 are the same, it will send an alarm and ask the operator to inspect the content of all messages from that global title or number range. Then the operator can enter into PhraseBlock, input the phrases in question and block messages coming with that phrase.

An approach like this can put control of incoming and outgoing messaging flows and revenue protection in the hands of a non-engineering function within an operator. Numbers can be blocked without changes being made to core network elements and databases.

For a fraud or revenue assurance team, the approach means they are not at the mercy of their operators' technology investment roadmap, which typically tends to operate 18 months to two years ahead. The CFO's team therefore doesn't have to integrate into that roadmap, but instead can take action independently and be confident they cannot cause any disturbance or impedance to the mobile network itself.

CONCLUSION

SMS is still important to operators, both in terms of existing and future revenues, and in terms of their customers' perception of their brand. The right tools and commitment to analyse incoming and outgoing messaging flows can bring benefits in terms of increased revenues, reduced revenue leakage, and increased customer satisfaction. The technology exists to do this without entering lengthy and complex network upgrade roadmaps, and without requiring engineering changes to the core network. Operators that take this route could add 10-20% to their wholesale revenues, as well as seeing customer support costs decrease, and customer satisfaction and net promoter scores increase.

For more information contact: sales@haud.com or visit the website at: www.haud.com

Assuring the future of SMS

telecoms.com INTELLIGENCE
Getting the industry thinking

ABOUT TELECOMS.COM INTELLIGENCE

Telecoms.com Intelligence is the industry research offering from the leading news and analysis portal for the global telecoms industry.

With over 80,000 unique monthly visitors and more than 70,000 registrations to our webinar platform, Telecoms.com has access to executive opinion of unrivalled breadth and depth. That opinion needs context and our editorial team excels at transforming raw data into insight and analysis. And with a variety of print and digital channels, including Mobile Communications International magazine, we can drive unbeatable awareness of our findings.

HAUD

ABOUT HAUD SYSTEMS

HAUD Systems is an international organization which provides solutions for revenue assurance in the SS7 area for both SMS and voice. It provides tools to mobile operators and SCCP carriers to stop leakages and increase revenues through enhance security in their networks. These solutions are intended to detect fraud occurring on incoming and outgoing traffic on the network.

HAUD System's business philosophy is to partner with their clients and assist then in achieving results through the use of their solutions by supporting them throughout the business life-cycle.