anam

Fighting the threat of SIM boxes to A2P SMS revenues

telecoms.com INTELLIGENCE

INTRODUCTION

Mobile operators increasingly find themselves having to compensate for declines in revenue streams that were once reliable. No greater is this challenge than with SMS, which for consumers has become entirely commoditised thanks to a combination of aggressive pricing from operators and effectively 'free' OTT messaging platforms such as WhatsApp.

Application to person (A2P) messaging is an effective means for enterprise businesses to communicate directly with their customers, forming part of an omni-channel messaging strategy. Global A2P revenues have been steadily increasing over the past four years and are forecast to continue to grow.

Where there is legitimate revenue, however, fraud inevitably follows and A2P SMS is no exception. A well-established technique for extracting fraudulent revenues from mobile networks has been the exploitation of 'grey routes' which circumvent operators' own systems, subsequently leading to revenue leakage.

Over time mobile operators have become more efficient at closing these grey routes, forcing fraudsters to adopt more innovative approaches. One such innovative approach is the use of SIM boxes, which allow the distribution of bulk SMS through the exploitation of consumer-only 'unlimited' text packages.

This Telecoms.com Intelligence whitepaper, written in partnership with Anam Technologies, will examine the A2P SMS industry and drill down into the nature of the SIM box fraud threat. Finally it will explore the measures operators can put in place to protect their A2P SMS revenues against SIM-box grey-routes.

A GROWING MARKET

Application to person (A2P) messaging is an emerging revenue stream for operators looking to offset rapidly declining traditional person to person (P2P) SMS revenues with new business models.

Industry analysts Ovum forecasts global A2P messaging traffic will total around 2 trillion events in 2015, which will rise to 2.2 trillion by 2017, representing 31% of total messaging traffic - up from only 24% in 2014.

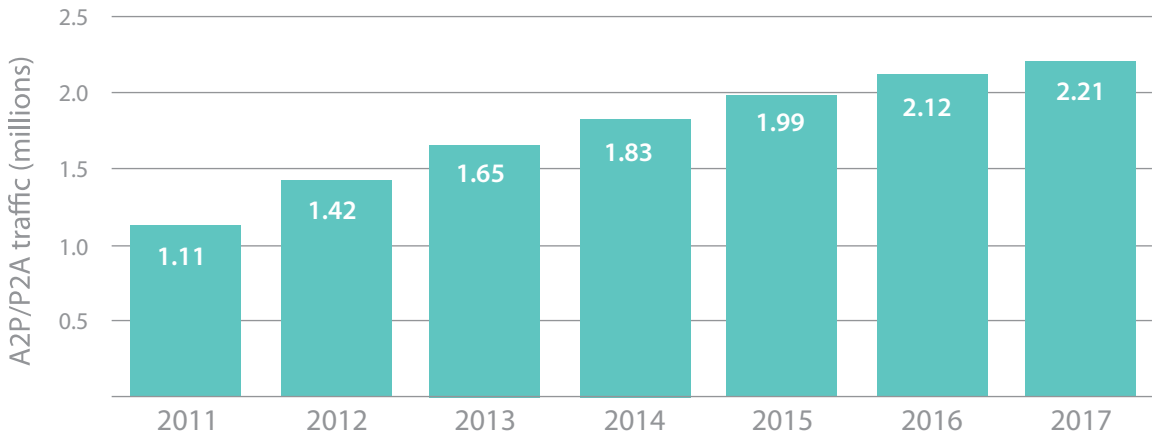
As mentioned above A2P is forecast to rise dramatically for at least the next two years, and there are sufficient reasons why that is the case. According the Direct Marketing Association, 44% of consumers would rather receive product details and marketing messages via text message; and texting as part of a multi-channel communications strategy is growing in popularity. Open and read rates of business-related text messages far outweigh those of e-mail, as text messaging offers a more personal interface with customers.

A wide variety of industries are making use of A2P messaging, appreciating it as a simple, inexpensive, efficient way to communicate with a large number of people – especially customers. A common use is two-factor authentication, which typically combines an online password with an SMS message to ensure that the customer needs separate devices operating over independent networks in order to gain access to secure services.

This facility is especially useful for the banking and finance industries, which have also called upon A2P messaging for things like account information, payments and alerts. Other consumer facing industries such as retail, FMCG and transport use A2P for direct marketing, coupons, loyalty and CRM in general.

Of course the substantial growth in A2P SMS volumes gives mobile operators an opportunity to offset the decline in P2P revenues resulting from the growth in use of competitive OTT messaging services. Ironically OTT services such as social media use A2P SMS for alerts, content delivery and two-factor authentication.

Global A2P SMS traffic, 2011-17



Source: Ovum

TRADING TEXTS

In principle the commercial dynamic governing enterprise procurement of A2P services should be straightforward, in which services are paid for on a metered/tariff basis much as with consumer subscriber contracts. Inevitably, however, an ecosystem has evolved specifically to cater for A2P messaging; aggregators and VARs enter into contractual agreements with operators in order to resell wholesale SMS to enterprise customers as part of value-added packages.

These middle-men serve a useful function to both operators and enterprise, considering they reduce the management overhead from a business arrangement that might otherwise be too small to justify it. It's not uncommon for there to be more than one layer of aggregator involved in the delivery of A2P SMS communications, and an inevitable consequence of any third party involvement is reduced control over the whole process.

A vulnerability often exploited by fraudsters looking to appropriate SMS revenues is large or even 'unlimited' SMS bundles. In an attempt to address the aforementioned threats to traditional SMS revenues the trend has been for operators to use generous SMS allowances to increase the appeal of tariff bundles, effectively using them as loss-leaders to attract more lucrative mobile data business.

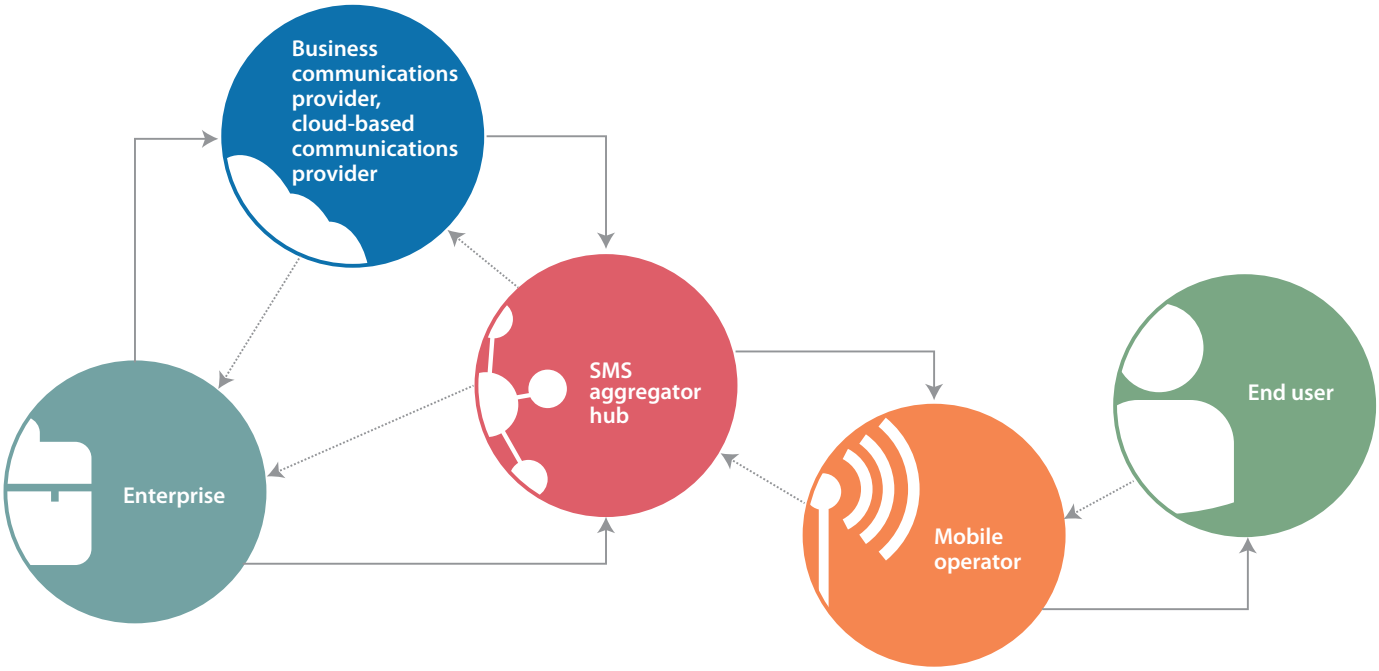
This trend has been underway in developed markets for some time, and is now rapidly increasing in emerging ones. The Asia Pacific region is by far the world's largest in terms of population and mobile subscribers, so the growth of generous SMS offers there provides especially fertile ground for anyone looking to repurpose those texts for other uses.

The world's largest mobile operator – China Mobile – offers 10,000 intra-network SMS per month as standard via its Hong Kong subsidiary. Vodafone India – the second largest Indian operator – bundles far fewer texts in its standard consumer tariffs, but for around US$2 you can buy a Bonus Pack of 3,000 texts for national use, seemingly over any domestic network.

In Malaysia, Maxis offers 'unlimited' SMS with its MaxisOne postpaid tariff, but attaches a fair use condition which clearly indicates that bulk messaging and A2P are not permitted. In the Philippines, even the cheapest postpaid tariff at Smart Communications has 'unlimited' intra-network texts, with no obvious mention of any fair use policy.

Telenor Pakistan offers micro-packages of hundreds of texts, which are unlikely to be attractive to fraudsters, but for US$2 offers daily 'unlimited' SMS packages. There is no reference to either a fair use policy or any notional ceiling to the 'unlimited package. Alternatively there is another bundle that offers a generous 10,000 SMS for use over the course of a month for around US$4. Both bundles can be activated merely by dialling a short code on a mobile phone.

These tariffs create billing loopholes that can be used by fraudsters to fulfil enterprise SMS services at minimal overhead. Not only does this deny operators significant revenue, but it also reduces their ability to manage the quality of the service. As a result, the entire A2P industry threatens to be undermined. The paradox for operators is that by offering generous consumer SMS tariffs they're also sowing the seeds for fraudsters to exploit their A2P business.



The A2P SMS ecosystem

Source: Ovum

CLOSING LOOPHOLES

A common form of fraud over mobile networks has been the use of 'grey routes', which utilise illegal interconnections to deliver a call or SMS, thus circumventing official delivery channels and avoiding termination fees. This is hardly a new concern for operators, who have been aware of the practise for some time. By effectively commercialising and protecting all interconnects, fraudsters exploiting grey routes have been forced to look for other technical vulnerabilities.

There are many other ways in which generous consumer SMS bundles can be used to deny operators revenue from enterprise deals, not all of which are necessarily illegal. In late 2013 mobile security specialist Lookout blogged about an app called Bazuc, which offered to pay consumers for their unused SMSs.

The thinking behind Bazuc was to take advantage of the fact that most people don't use even a fraction of the SMS bundle given to them by their mobile contracts. Therefore, an opportunity exists to repurpose that excess messaging capacity on to those that do need it, most notably large enterprise organisations. Of course this was a classic example of a loophole that results in significant revenue leakage, as well as helping to bypass spam and fraud detection systems by using otherwise normal accounts, so Lookout decided to investigate further.

Out of the 200 messages sent by Bazuc and analysed by Lookout; 90% involved some kind of A2P and only 1.5 % were peer-to-peer. Furthermore, while all the messages were delivered to US subscribers, they originated from countries all over the world. The investigation concluded that while Bazuc itself was not violating operator terms of service, it was inviting subscribers to do so.

The creator of Bazuc subsequently contacted the tech blog "AllThingsD" to address the claims in the Lookout report and conceded there are risks associated with the app for subscribers, but that these were clearly identified. He confirmed the business model was to target the A2P SMS market, but conceded the app has been pulled from the Google Play store for violating a clause that requires users to approve each text message sent on their behalf.

SIM BOXES

A SIM box (also known as a SIM farm, SIM bank or GSM gateway) is a device that can house a large number of SIM cards and be controlled via a computer. SIM boxes have been used for many years to bypass international voice tariffs. More recently, SIM boxes are used by fraudsters to originate large amounts of SMS from within a network by taking advantage of unlimited consumer SMS tariffs. This route could also be used to send spam, nuisance texts, etc. Despite how long it's been around, SIM box fraud is still considered a major threat to MNOs, costing them billions of dollars in revenue per year.

The use of SIM boxes as a channel for A2P SMS traffic is relatively recent but as is the case with the voice bypass, it is proving difficult for MNO's to detect and block. The capability and capacity of SIM boxes is growing ever more sophisticated whilst price points for SMS are coming down. Availability and accessibility is also no longer a barrier. Banks of SIM Boxes housed in mobile vehicles have also been detected and which further thwart location-based detection & blocking mechanisms. Fraudsters are also able to quickly switch out SIM cards from their boxes as and when individual routes become blocked by MNOs. Another recent development which complicates traffic detection from SIM boxes is support for IMEI (or device identity) re-configuration. Combine all these with the difficulty of tracing the owners of prepaid SIMs and the high churn environment that naturally exists in the market and you have a constant game of cat-and-mouse in which the MNO is frequently one step behind.

As a consequence, solutions to this problem require a significant degree of

Despite how long it's been around, SIM box fraud is still considered a major threat to MNOs, costing them billions of dollars in revenue per year

A computer linked to a SIM box device, often from a mobile location, can send multiple SMSs linking to local base stations

sophistication. A multi-layered approach involving successive levels of information analysis, decision making and action is considered best, often implemented in a phased manner to further complicate any counter-measures the fraudster might attempt.

FIGHTING THE FRAUDSTERS

Circumventing the use of SIM boxes for grey-route A2P purposes can be tackled on a number of levels.

When designing and launching price plans for the consumer and enterprise segments, MNO's need to attach clear fair usage terms to the availability of SMS volume bundles & unlimited packages. Restrictions limiting the usage of bundles toP2P communication and allowed volumes should be clearly stated and legally sound; if such clear T&Cs do not exist, MNO's should look to revise these especially for future price plans.

MNO's can also employ monitoring techniques to ensure that the defined fair usage policies are observed. This type of retrospective monitoring can be achieved though off-line analysis of billing system data. Whilst this approach can point to potential abuse of fair usage polices, it does not facilitate a differentiation between P2P and A2P traffic. It should be also noted that a billing data analysis approach only allows SIMs to be blocked "after the fact".

Another monitoring approach is the use of penetration test traffic systems to trace how A2P SMS is being routed to subscribers. Intelligent analysis of such results can detect the use of SIM boxes as the entry point onto the network to cause the A2P SMS termination bypass. While detection and identification capability related to these techniques is improving all the time, results will at most be "just near real-time". Given richer feature sets of increasingly cheap SIM box technology combined with rising levels of deployment and identity evasion ingenuity, the need for more sophisticated methods to safeguard against their usage for A2P SMS traffic is required.

SMS firewalls have been introduced into the MNO landscape over the past few years. The more sophisticated SMS firewall systems can represent a more effective approach to SIM box detection and blocking since they process SMS traffic in real-time and thus have the capacity for immediate grey route A2P SMS traffic identification and blocking. The challenge for existing SMS firewalls is that SMS traffic emanating from SIM boxes can be easily adjusted to defy the simple volumetric and pattern checks, especially if these are implemented as static configuration. SIM boxes operators also have the ability to dynamically re-program the IMEI (almost on a per-transaction basis), which evades any one-dimensional blocking technique based on IMEI detection. Thus a multi-faceted approach is needed, where a variety of techniques are applied in combination with SMS Firewall machine learning algorithms. This multi-faceted approach has led to extremely good results with the elimination of grey-route SMS via SIM boxes.

The nature of this fight against grey-route A2P SMS is that, once defended, the MNO's capability must be maintained. Continuous updating and sophistication of SMS Firewall detection techniques and filtering technology allied with latest threat intelligence and penetration testing services is the only truly effective means of blocking traffic and safeguarding A2P revenues.

CONCLUSION

A2P SMS is an important source of revenue for operators feeling the squeeze from declining ARPUs and OTT competition. It will remain a useful service for enterprises for some time, so it's worth protecting. Where there's revenue there is crime and A2P SMS is no exception. Fraudsters are constantly on the lookout for new ways to create revenue leakage from mobile networks and thus profit for themselves.

SIM boxes are a key tool in the fraudster arsenal as they allow both the routing of mobile calls via IP networks and the use of 'unlimited' SMS tariffs designed solely for consumer use. If operators are to maintain A2P SMS as a viable business they need to tackle this threat robustly.

Since SIM boxes also allow fraudsters to adapt rapidly when illegal use of a SIM is detected, a multi-layered approach is required. SMS firewalls can be configured not just to detect volume of traffic, but SMS signatures and IMEI information. A2P SMS is forecast to remain a significant source of operator revenue for some time, so it's worth protecting.

telecoms.com INTELLIGENCE

About Telecoms.com Intelligence

Telecoms.com Intelligence, the industry analysis arm of Telecoms.com, works closely with its partners to thoroughly research and create educational services for its readership. In 2014 alone we generated more than 25,000 leads for our clients across more than 50 campaigns.

A consultative and collaborative approach with our dedicated analysis team ensures the creation of truly unique content, highly regarded throughout the industry. Telecoms.com Intelligence services combine statistical analysis and broad industry knowledge to effectively deliver insight and analysis through the use of webinars, bespoke surveys, white papers and more. All campaigns are supported with extensive marketing campaigns, to guarantee quantifiable business leads for our clients.

Since its launch in 2001, Telecoms.com attracts more than 86,000 unique visitors and 173,000 page views on a monthly basis. The recently redesigned website also provides a newer and easier-to-navigate resource directory from which to access Intelligence content.

For more information, visit http://www.telecoms.com

anam

About Anam

SMS Assure, Anam's flagship product is a combined service and technology proposition which allows Mobile Networks to maximize revenue from A2P SMS traffic terminating on their network. Working closely with Mobile Network Operators to secure their infrastructure, SMS Assure involves business process structuring, effective SMS filtering and a managed operational and business service that generates new revenue for previously unbilled A2P SMS terminating on the network.

Anam's SMS Firewall (which forms the main technology element of our SMS Assure product) is based on industry leading and patented technology. Employing a multi-dimensional matrix-based approach to traffic analysis, the SMS Firewall runs a myriad of filtering techniques and correlations to identify SMS traffic attributable to SIM Boxes. Dynamic firewall rule management & continuous service monitoring by Anam's Managed Services Team ensures that SIM Box activity is kept under control in real time.

SMS Assure is extensively deployed in Mobile networks across Asia, Caribbean and Europe. The company's proven formula for monetizing A2P asserts that for every 1m subscribers, SMS Assure can deliver incremental annual revenue of $1m. Anam is headquartered in Dublin Ireland & has offices in Kuala Lumpur & London.