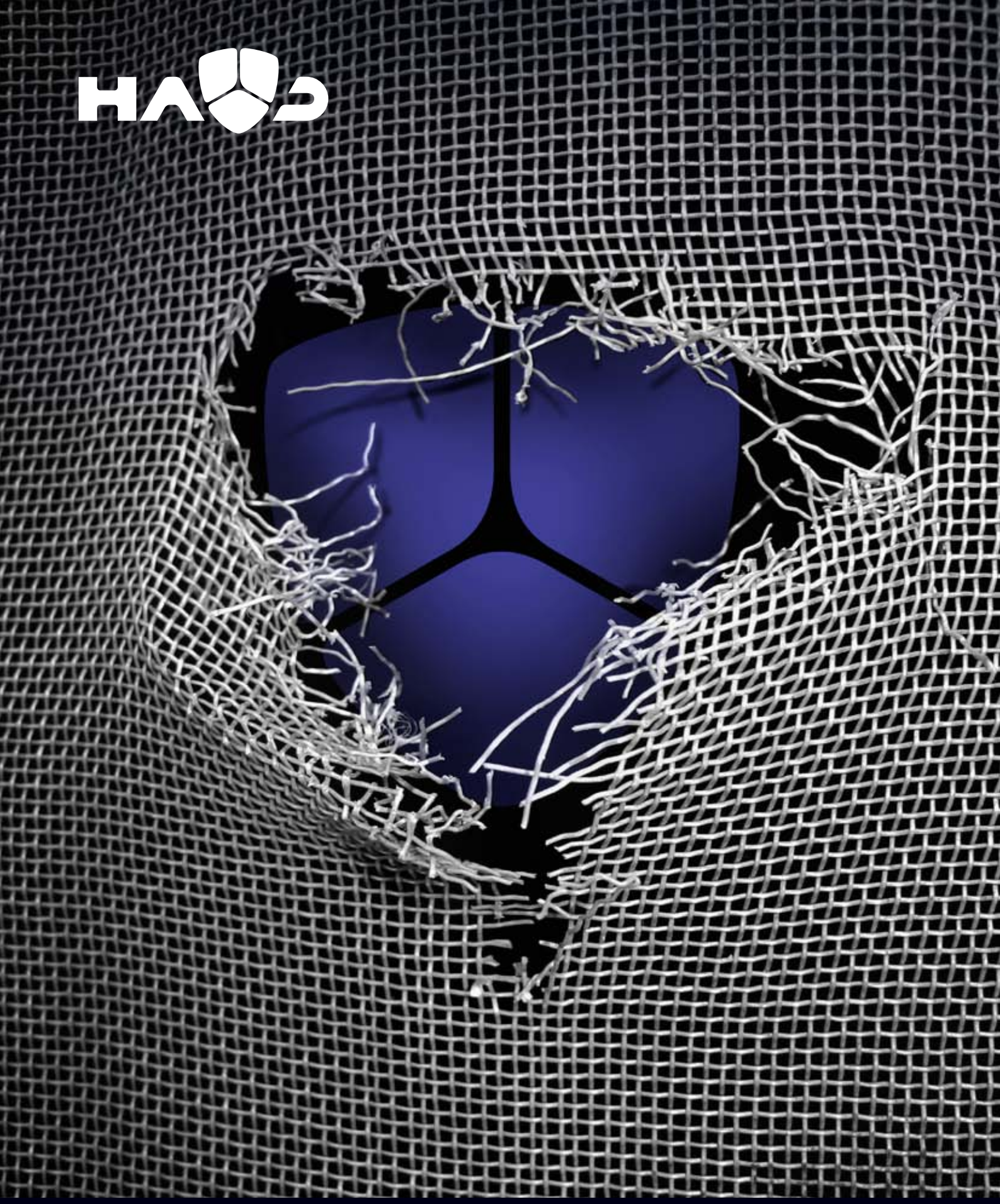

Grey Routes and Revenue Leakages
Are you protected?

HAUD Systems - White Paper

November 2012

Contents

White, Black & Grey Routes

For traffic to flow between operators within the same country or internationally, international traffic routes are used. These routes fall into three distinct categories known as **white routes, black routes** and **grey routes** respectively.

A white route is a route where both source and destination are deemed to be legal. This generally means that the sender and receiver are both authorised to convey SMS over their network to the other. Moreover in such cases operators usually enter into an agreement, which outlines the charges and the manner in which SMS will be conveyed. The most common of these are the established GSMA roaming agreements such as the AA.12, AA.19 and AA.60 as well as AA.63.

This is opposed to a **black route**, a route that is deemed to be illegal at both ends. On one hand it is considered as illegal due to there being no contractual agreement in place between the parties, but more importantly is deemed unlawful in view of the fact that both parties would not be authorised by the relevant regulatory authority to provide the service. This results in such parties not following required standards or paying the relevant charges for conveying SMS. Generally, they would be flying under the radar of scrutiny, security and charges thus making an unfair gain over other players who would be adhering to the requirements and legal obligations imposed for providing such services.

By undertaking **black route** business, one can easily undercut prices, ignore data privacy policies in the country of termination and spam and defraud subscribers. Moreover one would also be in insensitive to any regulatory requirements imposed by the country where the message is terminated.

The last type of route is generally known as **grey route**. This in particular will be our focus for discussion. As the name implies it is the most difficult to assess and the one which gives rise to legal, regulatory and revenue assurance concerns. A **grey** route is generally defined as a route that is legal for one country or the party on one end, such as the sender or the receiver, but deemed to be prohibited at the other end i.e. origination or termination.

Spectrum of SMS Traffic Routes

"A grey route is generally defined as a route that is legal for one country or the party on one end, such as the sender or the receiver, but deemed to be prohibited at the other end i.e. origination or termination"

SMS Revenue Leakages

Revenue assurance is a common term used in the telecommunications industry the world over, which essentially seeks to curb revenue leakages and ensure that all the products and services provided by operators are adequately billed for and revenues are collected in a timely manner from subscribers and wholesale partners alike.

Unfortunately however, we know that there is still a considerable gap between ensuring an adequate level of revenue assurance and the current state of affairs. Our main purpose here is to highlight the manner in which a basic (but essential) service like SMS that has been around for decades is still subject to revenue leakages. In particular, we shall narrow our discussion to the international scenario and wholesale SMS in the realm of bulk SMS.

In a press release issued by KPMG on the 28th March 2012, they quote figures from their second Global Revenue Assurance (RA) Survey entitled 'Entering a new era for revenue assurance. The key highlights are the following:

"20% percent of telecom operators currently reporting revenue leakages of up to 10%"

"41% of RA functions fail to identify more than half of total leakage"

- 20% percent of telecom operators currently reporting revenue leakages of up to 10%.
- 4% of operators expect revenue leakage to increase and half believe it will be significant.
- 36% of respondents say their company leakage is more than 1% of total revenue.
- 41% of RA functions fail to identify more than half of total leakage.
- New transformational projects (new technology, network, billing system migration, for example), poor system integration and fraud are the top 3 sources of revenue leakage.
- 78% use some kind of RA/fraud management tool.

One of the main issues which effect the success of revenue assurance we find, is the fact that most operators focus on the identification part mainly but are not sufficiently prompt to take pre-emptive or consequent action. Sometimes this is due to the fact that prevailing systems are diagnostic tools which do not offer the facility to take action. Moreover, most of these systems, believe it or not, are managed manually by several people working within operators solely on revenue assurance and hence without the help of alarms and pre-emptive tools to alert the user. Sometimes precious time goes by before an actual leakage is identified and addressed. This is confirmed by the fact that many operators we speak to seem very well equipped in identifying the problem, but few are effective in actually recovering significant revenue leakage.

This could be due to many factors, but the most prominent we encounter are:

- Timeliness in addressing the issue.
- Taking effective measures.
- Efficiency and ease of use of the tools at hand.
- Experience in dealing with a specific area of RA.

RA is a very vast area that deals with all of the functions within a telecommunications operator. However, many times the people working in the RA function do not have the luxury of becoming specialists in a specific area, but are constrained to operate as generalists and deal with matters ranging from subscriber fraud to unlawful bulk SMS aggregators using black or grey routes to terminate wholesale SMS onto an operator's network.

Grey Routes and Revenue Leakage

Let us start off buy outlining the food chain for bulk SMS delivery first.

First and foremost at one end of the food chain you have the content provider who would like to push content to the mobile subscriber. These content providers can be service providers such as banks, insurance companies or software providers who would like to send the subscriber notifications in relation to that subscriber's business with them. Content providers could also be marketers or retailers wanting to notify subscribers and potential customers of their latest offers.

Secondly, we generally find the bulk SMS providers whose main activity is to seek out least cost routing for the content providers to deliver their messages to the subscriber. It is usually these providers who adopt white, grey or black routes to deliver SMS depending on where they stand in terms of their legitimacy and being subject to regulation.

Thirdly, we find the mobile network operator who receives the text message via the SCCP carrier, and who in turn ensures the delivery of the messages.

Finally, we find the subscriber who is the receiver of the messages.

The food chain is such that the content provider pays the SMS provider to terminate the text message to the subscriber. The SMS aggregator finds the least expensive way in which to terminate this message. In many cases this means that the SMS provider may at times try to avoid paying the mobile network for terminating the message.

There are various ways in which such avoidance is done. At times SMS providers piggyback over operators who would have a connection to the mobile network operator to whom they want to send the messages wherein the amount of messages transacted between operator A and operator B would be so small in terms of volume that they do not charge each other for such termination. Hence the SMS provider exploits this situation and uses that route to terminate the SMS. In other cases SMS providers may even attempt to spoof the operator and change their identity when terminating the message so as not to incur any termination charges.

In all such cases the party which is the victim in this situation is primarily the mobile operator, and generally for more than one reason. The first reason is that the content provider, the SMS provider and the subscriber all attained a benefit. The first is satisfied for having its content delivered, the second for making money from such conveyance and the third from receiving the content. So the only one to lose out here is the operator for not having detected the grey route conveyance and adequately charged for the SMS termination in such case.

In a worse case, the second reason would be such that the content is spam and unwanted by the subscriber. In such case the mobile operator would end up sandwiched between a revenue leakage on the one hand and a vexed customer on the other. Hence here the situation could lead to both loss of revenues as well as customer churn.

"...SMS providers piggyback over operators who would have a connection to the mobile network operator to whom they want to send the messages..."

Ways to control Grey Routes

From the onset we need to state that so long as there is money to be made from bulk SMS, unlawful providers or ones of a dubious nature will continue to seek new ways in which to avoid paying operators.

This is precisely the reason why we advise our customers that there is a clear strategic way in which to tackle this matter. The strategy involves the adoption of the right tools, the right resources as well as roping in expert help from the sector. All these factors combined will ensure that revenue leakages are abated significantly and your network becomes more secure and less exposed. The operator must try to remain one step ahead of the fraudsters abusing its network.

Our suite of modules ensures a holistic approach to this problem ranging from analytics to standard functionality in the form of blacklisting and whitelisting solutions for Sender IDs and global titles (GTs) to more sophisticated modules which block text messages based on preconfigured phrases you want to stop by the system. The list goes on and finally we find pattern builders which detect new patterns of activity and alert the operator that a possible leakage could be occurring. All this happens in real time to ensure that immediate action may be taken to stop the revenue leakage.

From our research to date and from test cases we have done with operators it is safe to say that 5 to 10% of all SMS traffic going through the network is not going through white routes but is using grey routes. Hence all this is tantamount to revenue leakage.

Furthermore, a feature we have seen repeat itself in the market is that once a network operator is deemed penetrable by SMS providers, the market price for terminating SMS to that network quickly shrinks, hence, with a solution like HAUD Systems one could combat this leakage as well as ensure that satisfactory market prices are being paid for termination of all SMS to a mobile network.

''Our suite of modules ensures a holistic approach to this problem ranging from analytics to standard functionality in the form of blacklisting and whitelisting solutions for Sender IDs and global titles (GTs) to more sophisticated modules which block text messages based on preconfigured phrases you want to stop by the system''

About HAUD Systems

HAUD Systems is a subsidiary company of FORTYYTWO Group. At HAUD Systems we have developed a proprietary solution that focuses on advanced software and technological solutions in the SS7 arena.

Our primary customers are mobile network operators and SCCP carriers that require SMS analytics and filtering tools for originating and/or terminating SMS on their networks.

At HAUD Systems, we pride ourselves on our company values in creating solutions, which provide reliable ease of use and control over communications networks.

Our business practice is to partner with our clients and assist them in achieving results through using our solutions. For this reason we like to hand-hold our clients throughout the business life-cycle, from initial discussions through to prompt and efficient customer support and maintenance.

"...5 to 10% of all SMS traffic going through the network is not going through white routes but is using grey routes. Hence all this is tantamount to revenue leakage"

Disclaimer

The opinions expressed in this white paper are those of HAUD Systems and do not reflect the opinions of the companies or organizations referenced in this paper. All research was conducted exclusively and independently by Haud Systems.

Contact

For further information about HAUD Systems, please contact our sales team:

Email:	sales@haudsystems.com	Singapore:	+65 68 36 69 95
Malta:	+356 9994 2342	UK:	+44 (0) 203 411 0483
Sweden:	+46 (0)13 32 92 101	Americas:	+1 (212) 4191 320

HAUD Systems is a proprietary solution that is fully owned by FORTYTWO Group.

HAUD Systems