Enghouse Networks

An Enghouse Managed Service

for more information visit
www.enghousenetworks.com

International Grey Route Detection

The universal availability and reliability of SMS means that it is still the communications medium of choice for enterprises to reach their customers, both nationally and internationally.

Enterprises such as airlines, social networks, financial institutions, and technology companies use application to person (A2P) SMS to reliably send security confirmations, updates, and other information to subscribers. A complex ecosystem of intermediaries has grown up around the delivery of such messages between enterprises and their customers worldwide. Some of these intermediaries exploit loopholes to the disadvantage of mobile operators, which end up losing revenue as a result.

If every enterprise needing to send A2P SMS were to connect directly to each mobile operator, the complexity of contracts and network connections would be impossible to manage. For this reason, an entire ecosystem of intermediaries (aggregators, hubbing providers, and termination providers) has evolved to ensure that enterprises and operators have a manageable number of connections and contracts.

Enterprises pay aggregators to deliver their messages, and aggregators pay other intermediaries and eventually mobile operators to deliver these messages to their subscribers. Each intermediary makes margin by minimizing the cost that they pay for downstream delivery of messages.

The highest costs and therefore margins are applied to international A2P SMS messages. International brands pay a premium for rapid, reliable delivery to their international customer base. Most international messages are sent using IP-based protocols (SMPP, UCP, HTTP) to the destination network, but messages can also be sent via SS7 provided that the proper agreements are in place.

In order to legally send international SMS to another network, intermediaries must have signed an AA.19 agreement with the destination network, which specifies the routes that may be used, the traffic types allowed, and the delivery rates that apply.

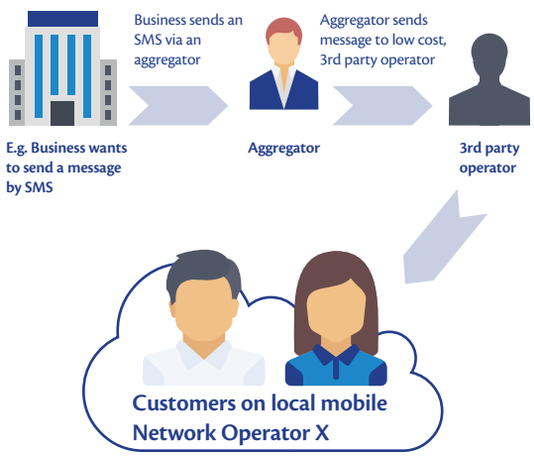
However, intermediaries do not always follow the terms of AA.19 agreements. For some, the temptation to maximize their margins is so strong that they send international A2P SMS into networks with whom they have no AA.19 agreement, or whose agreement does not cover the traffic being delivered. In this way, the intermediary avoids paying the contracted termination fee for international traffic, and may pay a much smaller amount or indeed nothing for delivery.

SS7 routes that are used for the delivery of unauthorized international A2P traffic into mobile networks are known as, 'grey routes.' Their status is 'grey' because the routes themselves are legal, but the parties using them or the traffic type sent across them are not authorised by AA.19 agreements.

The MNO receives the proper revenue only for messages that are delivered via the contractual SMPP and SS7 routes. Whenever grey routes are used to deliver international A2P traffic into a mobile network, the mobile operator loses revenue.

Operators lose legitimate revenue

Unauthorized messages arrive from external intermediaries who do not pay termination fees, or pay less than the AA.19 agreement rate to the terminating operator. As a result, the operator receives less compensation per message than is due, and hence loses significant revenue.



Intermediary uses an unauthorized SS7 route to deliver the message to into Network X

SMS content marketing campaigns are not billed accurately

Revenue loss for operators from global grey routes will amount to $62 billion by 2021, as reported by Juniper Research[1]. Operators that implement a solution to filter the SMS grey routes and shift this traffic to the appropriate chargeable channel can recuperate substantial amounts of revenue per annum.

1. https://www.juniperresearch.com/press/press-releases/operators-to-face-$62bn-revenue-leakage-from-grey

Enghouse Networks

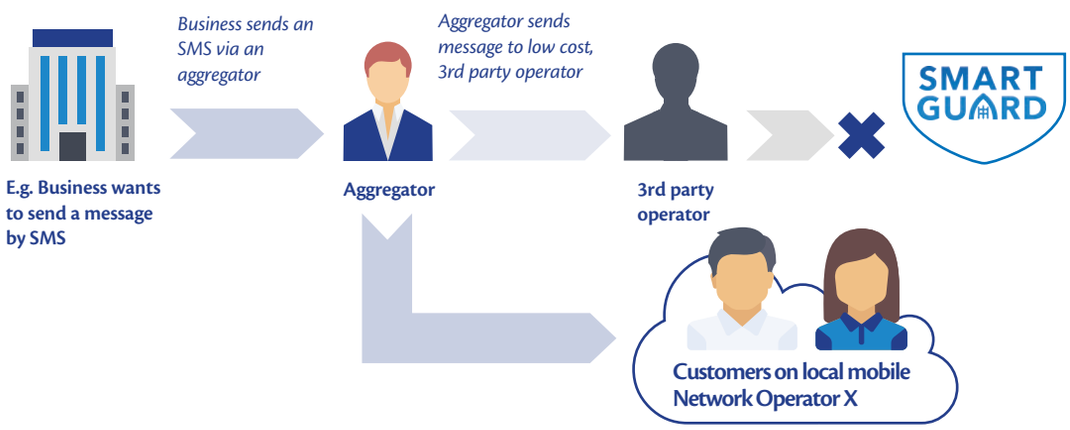
for more information visit
www.enghousenetworks.com

How to detect grey route traffic, and what to do about it?

Several techniques are available to identify and eliminate grey routes. Technology such as advanced SS7 and IP filtering detects grey route SMS through special algorithms and real-time analysis of messages that are delivered into the network.

The Enghouse managed service for grey route detection combines the real-time filtering features of the SmartGuard SMS Firewall together with ongoing analysis and reporting to identify long-term trends in A2P traffic.

The managed services team works with mobile operators and their chosen aggregators to eliminate A2P revenue leakage. Enghouse is open to collaborating with all parties who are seeking to protect legitimate revenue streams.



When grey route deliveries are detected, there is no point in contacting the originating enterprises, which are typically unaware of the message routing. Instead, the intermediaries must be encouraged to return to using legitimate routes.

Since unscrupulous intermediaries continuously try to exploit new grey routes whenever a known one is blocked, a managed service with ongoing analysis is critical to maintaining revenue protection. The Enghouse Networks managed service enables operators to block grey route traffic, and eventually force it back onto legitimate routes. There is no silver bullet that eliminates the problem permanently. It is a constant battle to protect MNO revenues.

The Enghouse managed service team configures the rules on the SMS Firewall to ensure that only authorized parties use SS7 routes for A2P traffic. With constant analysis of data from the network, the team revises and updates these rules to close off each new attack point and safeguard revenues.

For more information please contact us at
networksinfo@enghouse.com

Enghouse Networks SMS and security managed services experts continuously filter our operators' traffic through daily monitoring. The team generates reports that are shared with the operator to inform them about current risks and blocked senders.

Reports include defined keywords that SmartGuard applies to block grey route A2P messages, and permit legitimate, monetized A2P traffic.

In addition to grey route filtering, the Enghouse SmartGuard solution can also provide MO anti-spoofing, MT anti-faking, and home routing.

These additional filters are used to further identify and stop revenue leakage by preventing other forms of fraud and grey route usage, enhancing and protecting revenue streams.