

## Transparent SMS Spam and Fraud Control

SMS Defence covers SMS Anti Virus Requirements including

SMS Spam

SMS Faking

SMS Spoofing

SMS Flooding

Smishing

SMS Home Routing

SMS Spam

Unwanted messages are delivered to subscribers

Irritated subscribers, degraded network performance, blamed for spam relay

SMS Flooding

Remote system sends massive numbers of messages targeting subscribers and nodes

Overload in the signalling network, home operator incurs relay operator costs

SMS Faking

Foreign system uses identity of a legal SMSC (i.e. MT faking)

Home operator cannot collect termination fees

SMS Spoofing

Messages sent illegally by simulating subscribers who are in a roaming situation (i.e. MO spoofing)

Subscribers wrongfully billed for unsent messages and perhaps unwanted content

Smishing

Messages that appear to be from a valid company attempt to acquire subscriber information

Subscriber annoyance, billing issues, potential to spread viruses which in turn can result in more spam

SMS Viruses

Hacker engine launches messages luring subscribers to a download site with viruses

Compromised handsets cause customer service problems and may send unwanted messages

The main concerns that the impact SMS Spam and Fraud can have on a provider's customers, network and financial performance is:

Results in lost revenue for inter-carrier messages. With SMS fraud, the sender assumes the identity of a valid subscriber or SMSC, so the operator receives no termination fee.

Increases operational costs because of the large volumes of unauthorised messages. SMS spam and fraud can degrade network and SMSC performance and at times severely impact them (in some instances acting as a Denial of Service network attack).

Irritates subscribers and in turn increases churn, raises support costs and casts a negative light on the carrier's brand. Subscribers find spam annoying and many regard it as an invasion of privacy. It also results in unwarranted charges leading to customer frustration.

Damages the adoption of revenue-producing services. Spam can destroy trust in an operator, leading subscribers to opt-out of emerging mobile advertising opportunities.

While Point Code Based solutions may differ among themselves with respect to these capabilities and features, they all share the same distinct disadvantages because of their Point Code Based nature, disadvantages that include:

All Off-Net mobile-to-mobile SMS spam and fraud is allowed to enter a carrier's signalling network unchecked and consume STP/Gateway resources.

Every Off-Net and On-Net SMS message must first be routed to the Point Code Based node (or nodes) before being sent to an SMSC, increasing the amount of SMS traffic in a carrier's SS7 core and consuming additional network resources.

Because this approach requires an SS7 point code, carriers must reengineer their SS7 network and in some cases deploy intelligent routing mechanisms and additional STP resources to enable the redirection of the flow of SMS traffic.

SMS Defence also comes with the capability to create whitelist rules to ensure that trusted entities are always allowed to pass so service agreements are maintained.