

SMS SafeGuard

Protecting your revenue,
your customers and your brand

Guard revenue by cutting out fraud

Ensure your customers' phones are safe to use

Protect the vulnerable from abuse



Protecting mobile phones is becoming increasingly important as they are no longer just being used to make calls or send text messages

Mobile phones have evolved from simple dumb terminals into feature-rich smartphones that are often more powerful than desktop computers were only a few years ago. Unfortunately, this increased power has attracted the same sort of malevolent and malicious activities, such as spam, phishing, denial of service and fraud, that infect the IT world.

In many cases, the carrier for such threats is SMS, and users, phones and networks are all affected. The damage caused can be beyond that of the apparent direct impact of the attack.

The three main areas which can be damaged are:

- **Direct Revenue**

The most apparent impact of SMS Fraud is on direct revenue – the operator incurs costs that it cannot recover either from its customers or from other operators.

- **Indirect Revenue**

The indirect impact on revenue is as a direct result of people losing confidence in using SMS.

Some people have moved away from using email for communications due to the number of spam and phishing emails they receive. With over 20% of an operator's service revenue typically coming from SMS, a reduction in consumer confidence could have a major impact on service revenues.

What is more, SMS typically has a greater profit margin than other services, so any reduction in SMS revenue has an even greater impact on profits.

- **Brand Value**

Damage to the brand occurs when users are spammed or defrauded and hence lose confidence in the operator. Media reports of incidents of spamming or fraud also have a negative impact.

With applications such as m-commerce and mobile money transfer becoming increasingly popular, on both smartphones and basic models, it is vital that confidence in the integrity of the phone and the network is maintained.



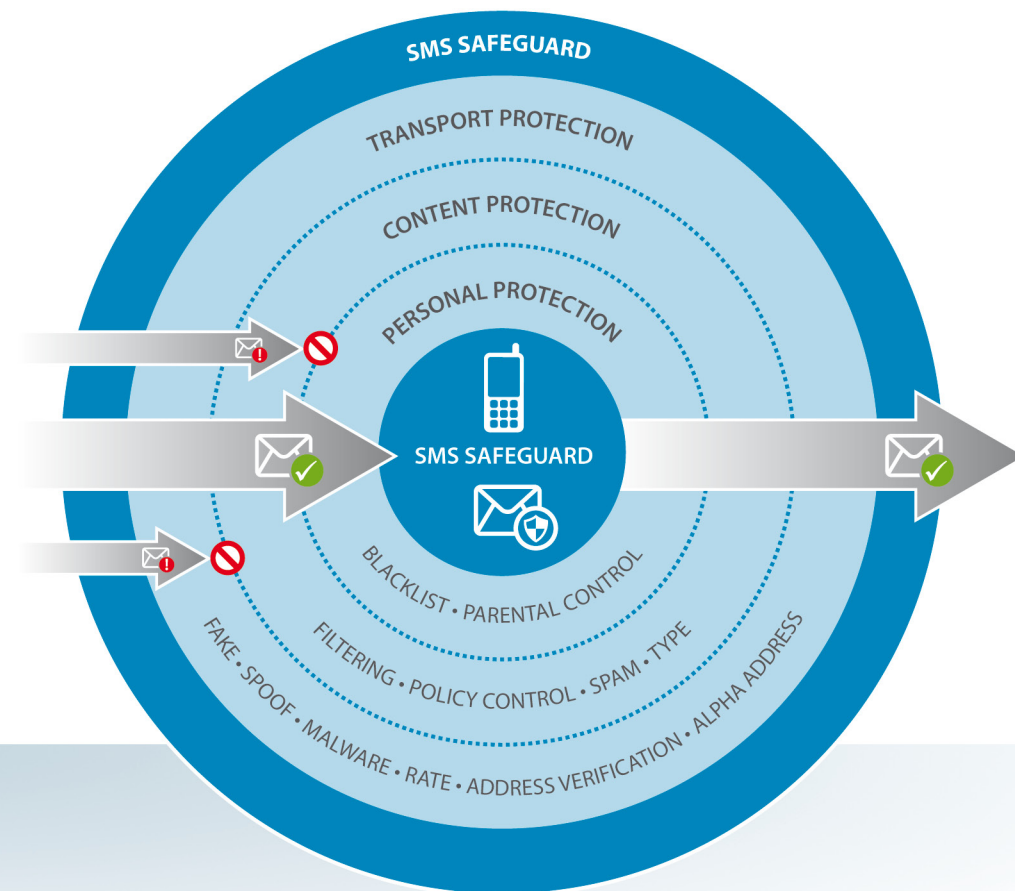
SMS SafeGuard

Telsis SMS SafeGuard addresses the many different types of threat to an operator's revenues, customers, and brand, by wrapping the network in three layers of protection.

Whether threats are malicious, fraudulent or just designed to inconvenience a network and its customers, SMS SafeGuard protects the network, handsets and users.

SMS SafeGuard sits alongside existing SMSC network infrastructure, leaving existing billing and CRM systems untouched, reducing integration effort and ensuring rapid service deployment. SMS SafeGuard also provides a foundation for Telsis SMS Smart Services – a set of simple and easy to use services that enhance the value of SMS, by giving customers the ability to control and manage their received messages.

SMS SafeGuard provides a layered approach to protecting against threats:



SMS SafeGuard is fast to put into service, sitting alongside existing SMSC infrastructure and usually requiring no integration with billing and CRM systems

Telsis understands just how important it is for mobile phone users to have trust in their network operator and the security of their handset.

SMS SafeGuard



Transport Protection

Transport Protection protects against transport level fraud, such as SMS Spoof and SMS Fake frauds, as well as messages that are malformed, or exploit weaknesses in handsets – such as the Nokia Curse of Silence or unauthorised OTA updates.

Transport Protection also offers protection against off-net Mobile Terminated messages that should not have originated off-net – such as messages with a false originating address or a short code that should have only been sent from an on-net Service Provider. Such messages are often sent for malicious purposes or to avoid payment charges.



Content Protection

Content Protection provides protection against Spam, Phishing and inappropriate content based on the content and categorisation of the message.

Content Protection examines the content of the message and the originator against keywords and message signatures which are contained in a policy control system, to classify the message and then either route or block the message based on the content and the user's preferences.



Personal Protection

Personal Protection offers a range of personalisation controls for which messages are received and how they are received.

Personal Protection allows the user to configure, for example, time windows for when they don't want to receive messages, personal blacklists and types of messages they want to receive.

Rapid System Integration – No risk to stability

Telsis SMS SafeGuard runs on industry-standard commercial platforms and is installed as an independent system that runs alongside existing SMSC or SMS Routing infrastructure. In many cases it requires no changes to billing systems, rating systems, provisioning or CRM systems. Deployment of SMS SafeGuard therefore involves minimal risk to existing SMS revenues.

Telsis SMS SafeGuard is in service with many leading network operators.

Contact: sales@telsis.com

Tel: +44 (0)1489 76 00 00

www.telsis.com