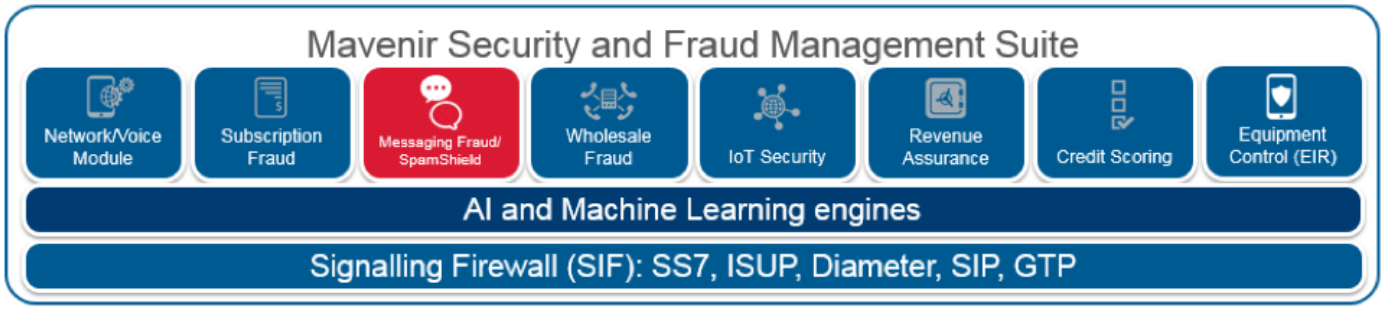
Messaging Fraud / SpamShield



The mobile messaging industry is rapidly evolving to resemble the Internet from a security and user behavior standpoint. Therefore, the mobile network operator faces an increasing, ever-changing flow of spam and fraud traffic that is difficult to detect and control. It's estimated between 5% -20% of all SMS messages are spam or fraud-related. (source: Mavenir and GSMA)

Providers of SMS based marketing explore every opportunity to 'optimize' costs and increase subscriber reach which sometimes results in business behaviors that blur the line between what is legitimate use and what is not. This means the mobile network operator faces an increasingly complex and dynamically evolving volume of spam and fraudulent attempts to subvert standard routes.

Spam and Fraud Overview

The increasing number of smartphones and the ever-dropping unit costs for one message (with free or unlimited SMS bundles) facilitates the spread of harmful SMS content (malware, viruses). At the same time, it encourages the use of the SMS for distribution of unsolicited messages, advertisements, and spam.

SMS messages are typically read and responded to, almost immediately. When exposed to fraudulent traffic this leads to a poor end-user experience but also causes significant revenue loss for the mobile network operator with missed opportunities for selling A2P value-added services, or through additional operating costs of increased traffic, capacity requirements and interconnection charges.

The following security breaches have already been observed in mobile networks:

- Originating subscriber spoofing avoid charging and identity theft
- Faked originating SMSC, used for free delivery (spam) or attacking the network
- SMS flooding - violating the fair use policies, DoS attacks
- SRI phishing - collecting subscriber base information for other types of fraud or for sale
- Spam and unsolicited advertisements
- Premium number scam requesting to call or text a premium charged number
- Phishing scams requesting sensitive information from the subscriber
- Homograph phishing attacks, mixing visually identical characters in the URL
- SMS malware such as viruses, worms or Trojans attacking mobile devices
- Botnets and SIM farms used for spam distribution or sending SMS to premium numbers
- Content violating cultural norms or local policies (pornography, profanity, etc.)

At the same time, attacks are becoming more sophisticated and evading basic traditional methods of detection, such as simple frequency analysis (anti-flood methods), limited pattern matching and offline analysis and

blacklisting. The following evasion techniques have been observed occurring in networks:

- Text variation changing some part of a campaign text content
- Homograph variation replacing visually similar characters from the same or different alphabet to complicate detection
- Using URI shortening technique to camouflage harmful links
- SIM farms spreading a large campaign across many originating addresses
- Rapid campaign switching
- SMS spam waves with high peak but very short duration
- Application farms and botnets
- SMS applications (ESMEs) and aggregators mixing spam into legitimate traffic
- SMS web portals being used for spam

Impacts to operator include:

- Lost A2P revenue
- Excessive traffic termination costs to other networks
- Lost termination revenue due to grey-routes
- Decreased QoS: Network congestions & Poor customer experience

Given current market pressure on operators messaging services, loss control on messaging spam would likely to impact conversational commerce monetization plans driven by RCS MaaP opportunities. Consumers would avoid using messengers that flood them with unsolicited content treated by the majority of people as Spam.

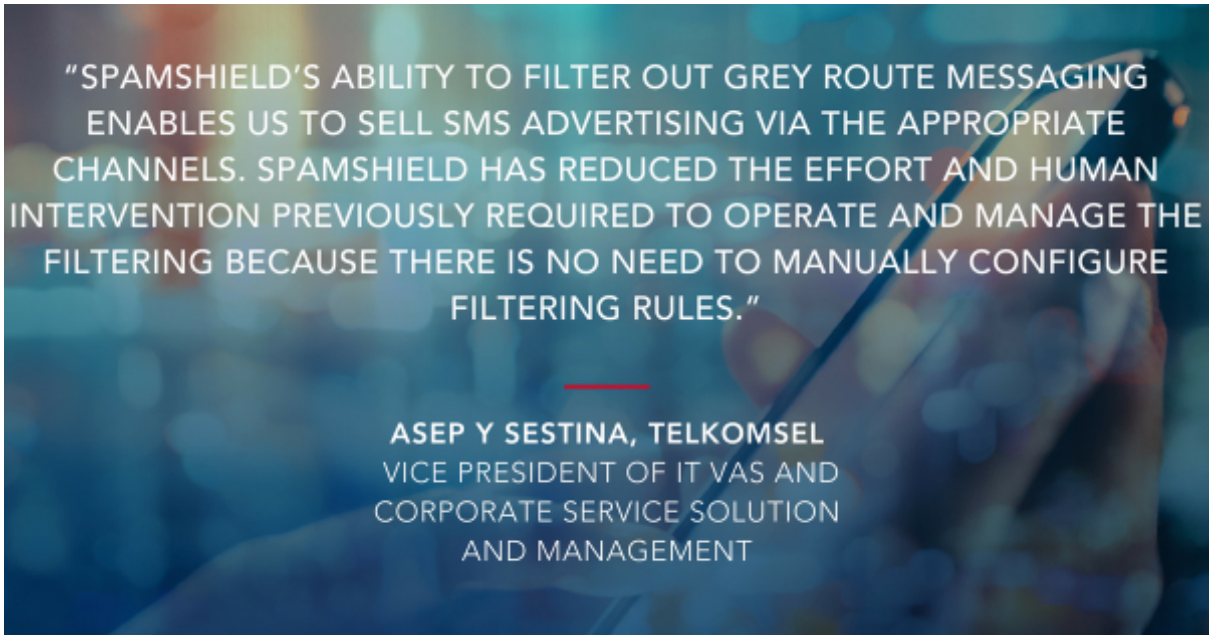
Mavenir's approach enables mobile operators to save between $0.5M and $3M USD monthly per network as well as ensuring projected revenue for commercial chatbots and rich messaging campaigns driven by new messaging technologies.

Spam and Fraud Prevention

Mavenir's comprehensive solution for controlling fraud, fakes, spoof, and spam provides the mobile network operators with 360-degree control to effectively address specific situations within their networks with a speed and flexibility unrivaled by other market solutions.

Mavenir's SpamShield addresses all major use-cases for mobile operator messaging channel control for SMS, MMS and RCS messaging protocols.

Core Spam detection technology used by Mavenir is based on Artificial Intelligence principles and Machine Learning which is developed with a detailed understanding of the subject area and specially tuned for real-time detection. Traditional detection and prevention techniques are based on deterministic rules and are easily detected and bypassed by spammers and fraudsters. Machine Learning detection algorithms are adapting to the current network and subscriber's behavior therefore still detecting spammers and fraudsters attempts.



The real-time nature of detection and advanced correlation techniques with external learning feeds including spam reporting service, centralized spam DB, hyperlink reputation statistics and call-back number reputation, enables real-time prevention of malicious campaigns invalidating spammers business case.

Machine Learning techniques implemented in Messaging Fraud module of Mavenir Anti-Fraud and Security suite are not only addressing traditional text-based messaging but also multimedia content used in RCS, as visual spam can represent much more powerful technique to fraudsters.

Some operators are still controlling their messaging traffic using traditional, rule-based approach. Mavenir's SpamShield solution protects the operator's revenue by relying on a very powerful real-time rule-engine which is integrated with Machine Learning modules enabling mobile operators to address any concern or business process established.

SpamShield also supports integration with 3rd party network components with the prerequisite that the interface specification is available for implementation.

SPAMSHIELD IS MAVENIR'S WORLD-LEADING MESSAGING FRAUD CONTROL SOLUTION:

- Employs advanced machine-learning techniques
- Maximize additional A2P revenues
- Rapidly identify and automatically control fraudulent traffic
- Without the cost of employing teams of analysts to sift through messages manually.