# The Threat of SMS Spoofing: Prevent Revenue Loss by Securing The Network Against Fraudulent Attack

openmindnetworks
messaging experts

# The Threat of SMS Spoofing: Prevent Revenue Loss by Securing The Network Against Fraudulent Attack



## 1. SMS Spoofing

The GSM Association has identified a number of potential fraud attacks on mobile operators that are caused by abuse of SMS messaging services. The most serious of these threats is SMS Spoofing. SMS Spoofing occurs when a fraudster manipulates address information in order to impersonate a user that has roamed onto a foreign network and is submitting messages to the home network. Frequently, these messages are addressed to destinations outside the home network – with the home SMSC essentially being "hijacked" to send messages into other networks.

The impact of this fraud is threefold:

- The home network can incur termination charges caused by the delivery of these messages to interconnect partners. This is a quantifiable revenue leakage.
- These messages can be of concern to interconnect partners. Their customers may complain about being spammed, or the content of the messages may be politically sensitive. Interconnect partners may threaten to cut-off the home network unless a remedy is implemented. Home subscribers will be unable to send messages into these networks.
- While fraudsters normally used spoofed-identities to send messages, there is a risk that these identities may match those of real home subscribers. The risk therefore emerges, that genuine subscribers may be billed for roaming messages they did not send. If this situation occurs, the integrity of the home operator's billing process may be compromised, with potentially huge impact on the brand. This is a major churn risk.

An SMS Spoofing attack is often first detected by an increase in the number of SMS errors encountered during a bill-run. These errors are caused by the spoofed subscriber identities. Operators can respond by blocking different source addresses in their Gateway-MSCs, but fraudsters can change addresses easily to by-pass these measures. If fraudsters move to using source addresses at a major interconnect partner, it may become unfeasible to block these addresses, due to the potential impact on normal interconnect services.


Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**


openmindnetworks
messaging experts

## 2. How Spoofing is Stopped

The only 100%-sure way of detecting and blocking spoofed messages is to screen incoming mobile originated messages to verify that the sender is a valid subscriber and that the message is coming from a valid and correct location. This can be implemented by adding an intelligent routing function to the network that can query originating subscriber details from the HLR *before* the message is submitted for delivery.

This kind of intelligent routing function is beyond the capabilities of legacy messaging infrastructure.

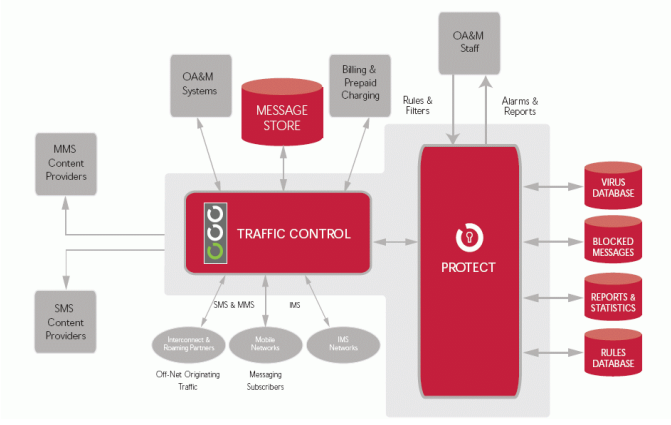
## 3. Openmind Networks' Solution

Openmind Networks' ***Traffic Control*** next generation message router gives mobile operators the intelligence, flexibility, scalability and reliability needed to cope with the uncertainties, capacity requirements and technological demands of current and emerging messaging services. The system supports the in-flight capture and control of protocol messages in order to provide intelligent message handling and routing applications. The ***Protect*** module augments Traffic Control with some specific anti-fraud features, including the ability to detect and block occurrences of SMS Spoofing. Protect is used to screen incoming messages by checking message contents and parameters against known fraud criteria. It can also perform external queries, such as HLR look-ups, to validate incoming messages.

Traffic Control can be used both as a replacement to legacy SMSCs and as an intelligent router that can add value to existing networks via the introduction of fraud screening and service enhancements. When used to block spoofing in a legacy network, messages from out-roamers are first routed to Traffic Control and Protect where they are screened before being relayed to existing SMSCs.

Traffic Control and Protect are software products from Openmind Networks that can be deployed on commodity, off-the-shelf hardware. They support SIGTRAN M3UA and SUA protocols, and can hence be deployed in the network without the need for expensive third party SS7 equipment.

The diagram below illustrates how the Protect module can be deployed with Traffic Control, to stop undesirable messaging traffic in a mobile network:

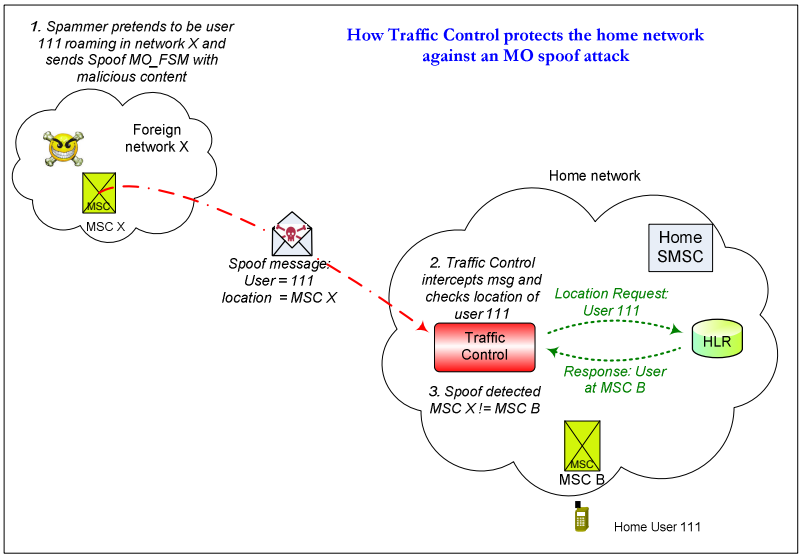



Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**

openmindnetworks
messaging experts

## 4. Network Details

The Traffic Control platform provides access to the GSM network and is used by the PROTECT module to intercept messages for screening prior to relaying them to the SMSC. The PROTECT system uses a sophisticated rules engine to screen incoming messages against a variety of pre-configured criteria. It is a powerful, rules based system that is highly configurable and which can target specific message types to remove known threats. PROTECT also uses intelligent heuristic algorithms to classify messages as fraudulent based on unusual patterns of submission or content.
The figure below illustrates how the Traffic Control PROTECT module checks against incoming Spoofed MO_FSM messages.




The diagram shows how a spammer attached to MSC X in a foreign network, pretending to be an out-roamer user 111 of the home network, sends a MO_FSM message destined for the home SMSC.

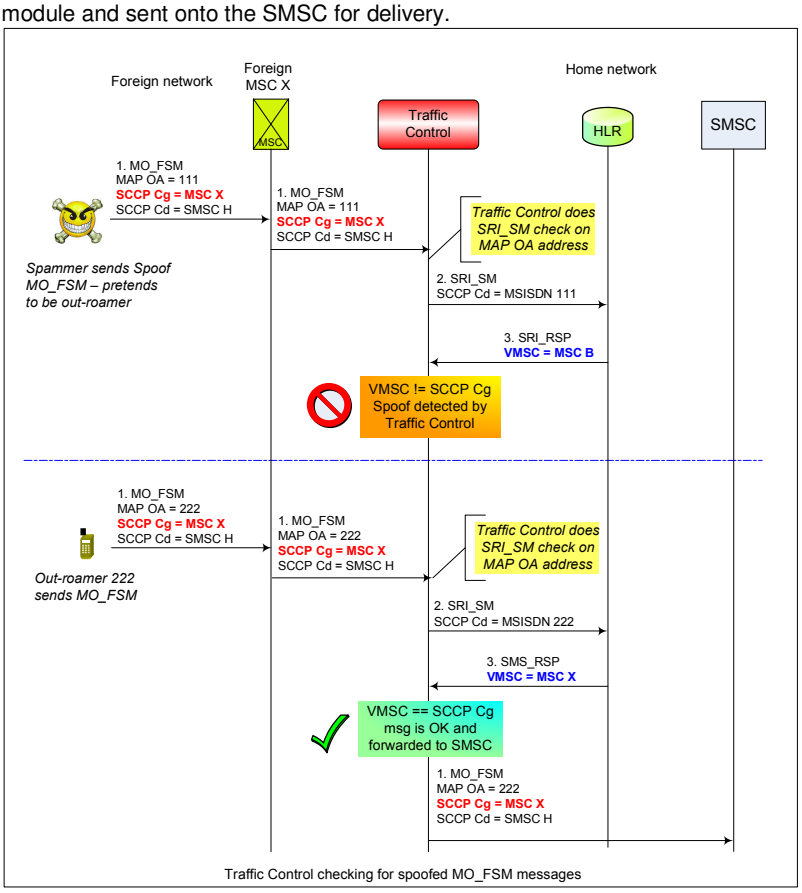
Traffic Control intercepts the message and queries the real location of user 111 with the HLR which replies with MSC B.

Traffic Control compares the location user 111 as given by the HLR i.e. MSC B against the location of the message i.e MSC X and indicates that a Spoofed message has been detected. The platform then handles the message based on the configured action plan.

Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**

**Network Details (continued)**

The same scenario is illustrated in a more detailed sequence diagram shown in the diagram below, which also shows a successful case of an MO_FSM from a genuine out-roamer being checked by Traffic Control with the PROTECT module and sent onto the SMSC for delivery.



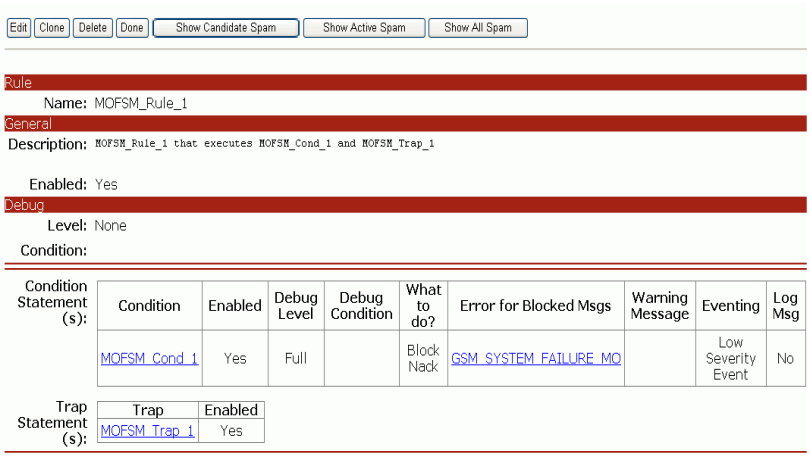

Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**

openmindnetworks
messaging experts

## 5. Conclusion

Fraudsters are becoming an increasing problem for mobile operators as attacks on messaging infrastructure become ever more sophisticated and ever more aggressive. Core messaging revenues are continuing to erode such that SMS Spoofing implies some specific commercial challenges. Firstly, messaging revenues will become increasingly sensitive to leakage. In addition, retaining subscription revenues will become more important than incremental revenues per message, such that the detrimental effects on customer loyalty due to over charging will be unacceptable.

The Protect module deployed with the Traffic Control platform represents the market-leading defense against this significant threat, based on the accumulated experience of real-world fraudulent behaviors that Openmind Networks has previously addressed. This experience has indicated that the nature of malicious activities can evolve rapidly, mandating a flexible approach to mitigate against the threat. The Protect module is highly configurable in this regard and the screen shot below describes how a rule can be defined using a web based interface to guard against emerging SMS Spoofing mechanisms as they are identified.




As malicious users become increasingly resourceful, and the commercial implications of SMS Spoofing become increasingly significant, mobile operators need to acquire the best possible protection of their messaging infrastructure, revenues and customers. Openmind Networks has the experience to provide best-in-class defensive processes and the Protect module coupled with the Traffic Control platform provides the best-of-breed SMS Spoofing product technology

Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**

openmindnetworks
messaging experts

Openmind Networks is the world's leading Next Generation Messaging Systems provider. Its product, Traffic Control, is a Next Generation Message Router that allows operators to consolidate legacy SMSC, first delivery router, and application delivery router platforms into a high performance, multi-purpose messaging engine.



**www.openmindnetworks.com**

Openmind Networks,
4 Westland Square,
Pearce Street,
Dublin 2,
Ireland
Tel: +353 1 633 0070
Fax:+353 1 670 8008
info@openmindnetworks.com
**www.openmindnetworks.com**

openmindnetworks
messaging experts