

**GLOBE  
KONNECT**

# **SMS FIREFWALL**

**(WHITE PAPER)**



**CONNECT | COMMUNICATE**  
**A GTS Brand**

**[www.globe-konnect.com](http://www.globe-konnect.com)**

# GLOBE KONECT

## Table of Contents

## Page No.

1. Introduction .....	3
2. SMS firewall Facts and Figures .....	3
3. Why Firewall is needed? .....	4
4. Why does every mobile operator needs a SMS firewall? .....	5
5. How SMS firewall can benefit operators, enterprises and customers? .....	6
6. How does SMS firewall work? .....	8
7. Globe Konnect SMS Firewall system features .....	8
8. How firewall can protect the mobile network from spams, fraudulent and unbilled messages. ....	9
9. What are the various routes of grey traffic? .....	10
10. Various types of threats that require SMS firewall protection: ..	11
11. How are SMS threats detected and resolved? .....	12

## Introduction

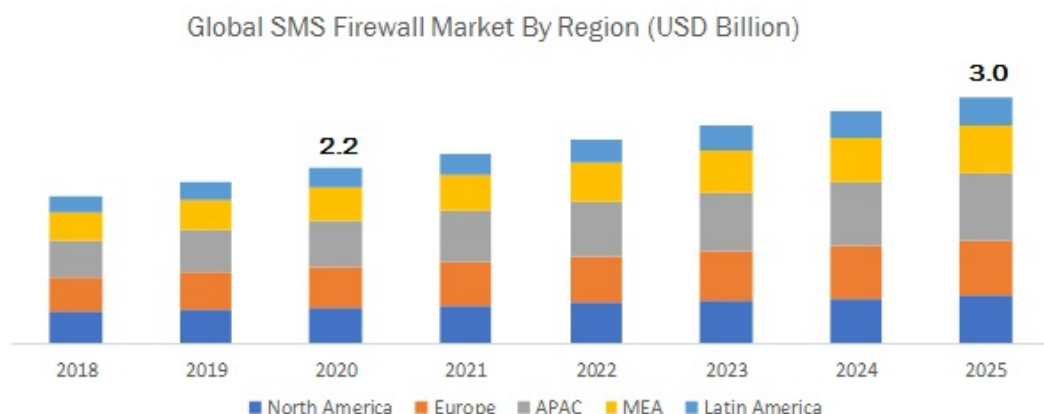
The global mobile messaging market has become vulnerable to cyber-attacks, spams, spoofing SMS scams.

Mobile network operators often face the challenge of detecting multiple messages. Moreover, they have to make sure that their network is not subjected to fraud and spam. Spamming, grey routing, and fraud messages can cost revenue leakage and operators start losing the trust of their audience.

Mobile SMS spam, spoofing and SMS scams have created havoc for both operators and subscribers. Fraud operators gain unauthorized access to the SS7 networks of major service providers and send massive spam into the network. Spoofing is another mode of fraud; here personal information is retrieved from the user which often leads to financial loss.

## SMS Firewall Facts and Figures

- As per Communications Fraud Control Association Telecom fraud, Voice frauds and SMS frauds amounted to \$30 billion loss in revenue.
- Mobile operators are monetizing one-third of the revenue that they can actually get through A2P SMS traffic. This happens as the SMS traffic is divided into white, black and grey routes. Well, there is no price agreement between the black and grey route so suppliers can set their own cost per SMS rate.



Source: MarketsandMarkets Analysis

<https://SMSmarketingreviews.org/SMS-firewall-market-8-billion-industry-2026/>

- According to Reports and Data, the SMS market is said to grow from \$2.77 billion in 2018 to 8.78 billion by 2026 at an annual rate of 22%.
- Global SMS Firewall Market is expected to grow by USD\$2.2 Billion in 2020 to USD 3.0 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 7.0% during the forecast period.
- The APAC and Europe region have the highest market shares in the SMS firewall market .They together contribute approx 45-50% to the global SMS firewall market in 2020.

## Why is Firewall needed?

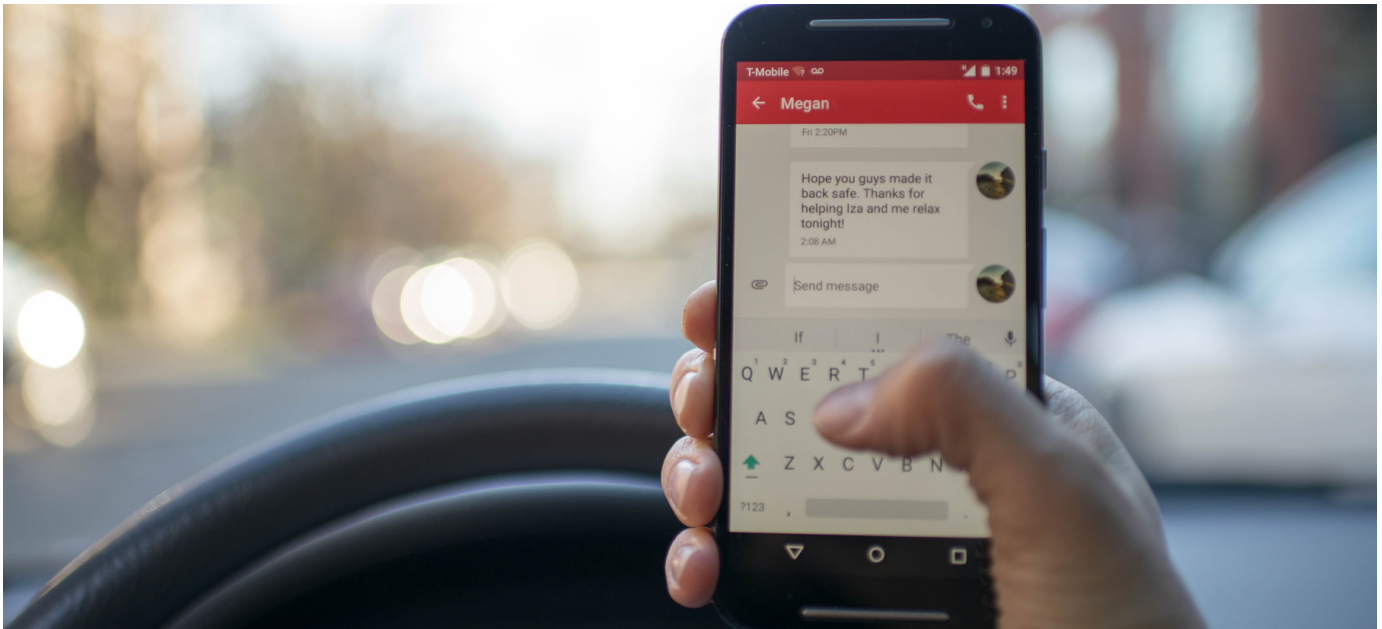


- With an SMS firewall, they can get a clear picture like who is sending traffic and in what amount. Furthermore, will be able to control the type of messages and can identify among A2P messages and P2P messages.
- A firewall safeguards the mobile network against all SMS frauds, attacks, and revenue leakage from unauthorized sources. All the messages are routed through the firewall.
- Globe Konnect Firewall system stops spoofing and scans each message sender, source, and route. Our cost-effective service guards your subscriber against any fraud and spam. We ensure high-quality SMS termination from messaging originators, including over the top (OTT), business enterprises, and A2P aggregators, directly to the MNO.



## Why does every mobile operator need an SMS firewall?

- Filtering and then blocking the fraud and spam messages, this improves customer retention.
- SMS Sim box: It prevents SIM Box fraudsters from exploiting 'unlimited' consumer text packages.
- To prevent loss of revenue -by blocking grey routes and make way for more monetization opportunities.
- To build trust among the customers and safeguard their bank account.



## What advantages does SMS firewall have for businesses, customers, and mobile operators?

SMS is considered as a safe and cost-effective medium for communication.

Hackers or fraudsters can break the trust you built with your customers within a fraction of seconds. This in return can damage your revenue.

SMS firewall is based on a holistic approach that combines software and hardware features to ensure monetization.

**"SMS is considered as a safe and cost-effective medium for communication."**

## How it can benefit operators?

- SMS Firewall is an ideal SMS anti-fraud solution for mobile operators. It protects the network and subscribers against unauthorized SMS traffic like SMPP traffic or transit mobile-originated traffic.
- It protects against anti-spoofing and detects manipulated addresses.
- The SMS Firewall uses several metrics that can be used to detect whether the message is spam or not.
- With an SMS firewall, the operator gets full control of the SMS messages in the network. Operators can monitor and accordingly implement certain restrictions to increase their revenue. This can reduce spam messages and deliver the best to the customers.
- The firewall protects your subscribers against smishing. Smishing is a cyber-security attack in which SMS is used to steal personal credentials.
- Sometimes people tend to click on harmful links and even respond to fraudsters.
- SMS algorithms classify messages based on the malicious keywords, URL, email ids and phone numbers. This protects the customer from sharing confidential information with the wrong source.



## Some of the advantages of SMS firewall for customers?

- SMS firewall saves the customers against unauthorised SMS traffic. The firewall has detection capacity and it identifies spam and fraud messages.
- Globe Konekt SMS firewall provides high performance and scalable solutions to meet the safety requirements.
- It blocks malicious signaling attacks.

## Benefits for businesses

With an SMS firewall businesses can secure their business and unlock new ways of revenue.

### **Unified or Independent:**

SMS firewall includes both analysis and home router. It is an answer to both SMS security and monetization. It can be deployed standalone along with additional protocols for security. The firewall also can be executed on customized servers, which large conglomerates use for their data. Moreover, the firewall is independent of the device used.

### **Fast and Flexible:**

From the first day of deployment, it blocks all kinds of threats. The firewall is quite flexible. Users can modify their requirements on the go. Furthermore, it detects potential revenue leakage but also provides valuable intelligence in real-time. SMS firewall can also implement new policies without any software updates.

### **Security:**

SMS firewall defends mobile networks against all kinds of attacks. It ensures that no fraudulent messages go through and blocks all 'grey routes.' It means that it even analyzes outbound messages. After it blocks a suspicious or fraudulent message, the message sender is informed that they delivered their message, when in fact, the firewall blocked the message beforehand. The firewall also features a home router, which protects subscriber privacy.

### **A2P:**

The firewall provides a complete A2P monetization solution by classifying messages into A2P or P2P. Additionally, they block the grey routes appearing, which also provides safety to the user. It enforces A2P termination over official routes and prevents any revenue leak. SMS firewall blocks messages by bulk SMS providers until a favorable business agreement is in place.

**Accessible Reporting:** The SMS firewall has a robust reporting feature. It means that it alerts the users in the case of a spam or fraud message received/blocked. Moreover, you can also have more accurate information about network traffic and security.



## How does SMS firewall work?

- Whenever an SMS reaches you, SMS firewall starts detecting the source, address, a destination address, and route of that message.
- It also checks the traffic spikes, repeated traffic and identifies grey routes and blocks it.
- SMS blocks traffic based on different parameters and triggers like malicious addresses, phone numbers, and email ids.
- A2P SMS traffic can identify various routes of monetization. With this mobile operators can charge for traffic.
- Usually, operators want to offer A2P SMS via the said interface, but if there is no agreement then marketers get access to some other routes which are less priced. The traffic flows through this channel and on the other hand operators lose revenue. So it becomes necessary for operators to safeguard their revenue via SMS firewall and let traffic take the mandate routes.

## Globe Konnect SMS Firewall system key features

- **Eradicate Grey routes:** Different spams can reduce the speed of your business. A2P SMS A firewall can help you get rid of grey or undesired routes.
- **Prohibit message overflow:** Restrict huge amounts of messages to one or more destinations.
- It detects the manipulated addresses and prohibits them.
- **Achieve Complete Control of SMS Traffic in Your Network:** SMS Firewall removes the unnecessary messages that are blocking your way and let the relevant SMS traffic drive towards your business.
- **Protect the Transparency of Your Network:** Our Firewall system makes your SMS more secure. A2P firewall helps you differentiate between targeted clients and spam.
- **SMS monetization:** SMS Firewall identifies and unleashes the sources of revenue
- **Drive enterprise traffic to approved channels**
- **Control SMS traffic in your area**
- **Protects against viruses**
- **AI and ML-based protection –** Identify unknown patterns for protection.
- **Anti-spamming:** it blocks traffic from the unauthorized source
- Blocks large amount of messages to one or more destinations
- Stop messages from the fake addresses



## How Globe Konect SMS firewall guards against spam and fraud?

### Globe Konect Security solutions:

Globe Konect's SMS Firewall let operators identify the threats and protect their network from malicious attacks.

#### Network visibility:

It collects network signaling traffic such as SS7 and SIP, as well as MAP, ISDN, HTTP, FTP and more. Operators get visibility to their network and now they can easily identify unauthorized access. Furthermore, operators get the data usage in the form of reports and customized dashboards which can be accessed by standard browsers.



#### Stopping scams:

SMS Firewall detects the spoofing and SMS scam and blocks them. It has two main components: basic and advanced firewall filters. The basic filter Blocks incoming and outgoing scam by screening at SSCP and MAP levels.

Advanced filters protect the service provider by analysing various parameters such as content filtering, address analysis.

When a message is rejected based as per the filters. The error message is sent back to the originator SMSC or a faked success status is sent to the sender SMSC.

- Our firewall is compliant with industry standards which include IR.70 and IR.71. It protects against unauthorised and spam messages to subscribers and this prevents unwanted SMS traffic.
- Also helps in detecting faking, spoofing, and GT scanning for illegal subscriber address and MNO SMSC representation or usage.

- SMS firewall detects, alarms, and removes threats and protects MNO networks and their subscribers.
- Our SMS filter captures all threats that lead to revenue leakage and free/low-cost routes in your network. Moreover, the grey route gets eliminated.
- It safeguards the subscribers against the fraudulent activities like exposing their bank details.

## What is grey traffic?

- It comes in the middle of white and black routes. Moreover, a combination of legal SMS and illegal SMS. Here one connection is legal for one country or the party at one end and another is illegal. It reduces the cost of sending messages by bypassing international SMS laws and fees.
- It does work like a usual SMS sending process. Here, via grey routing message will be sent to another country with fewer regulations, and then will be sent back to the person you were sending.
- In grey routing, only destination MNOs with a termination agreement will generate revenue others will experience revenue leakage.



### Cons

- It's not secure and reliable mode of sending messages
- Delay in messages could be experienced
- It doesn't provide delivery routes and caller ID.

## Routes of grey traffic:

Way to terminate traffic without reimbursing a mobile operator: Some operators can disguise the international A2P traffic as P2P traffic, which is a lot cheaper.

This way, operator that doesn't follow these practices can lose profit as they won't be getting the full price of international A2P traffic termination.

## **Blending:**

Here the partner can fake the delivery reports by not sending non-sensitive traffic to users. This is merely done to receive all the profits at lower costs.

## **Termination through national aggregators**

In this international partner approaches a local aggregator and asks to deliver its international A2P traffic using the Sender ID of the local service. And the operator is not able to detect and sees it as "local delivery service messages" instead of international service traffic and then loses the profit.

## **SIM box fraud:**

A SIM box is a hardware containing many sims that are owned by a third party but determined by MNO as normal mobile numbers.

The partner collaborates with the owner of the SIM box and leaves the operator out of the process. This way, partners and the SIM box owners can earn profit on traffic termination.

## **Various types of threats that require SMS firewall protection:**

### **Mobile security threats:**

One way to hamper the security is to send simple viruses such as Trojan via SMS.

### **SMS frauds:**

It involves the illegal use of an operator's SMSC network by a third-party.

### **PRS related scam tricks:**

Here fraudsters send subscribers unsolicited messages and hence trick them by charging them high amounts.

### **Flooding and Denial of Service (DoS) Attacks:**

It is an attack in which the network shuts down and becomes inaccessible to the intended users. Flood attacks happen when the system starts receiving too much traffic.



### **Handset viruses:**

Smartphones have become more connected and even offer full web access. They have become more vulnerable to the malicious virus attacks. Viruses can easily enter our smartphones via website, Bluetooth and SMS. Earlier in 2005, the Cabir virus, which was the first handset virus infected phones in over 30 countries.

### **Artificial Inflation of Traffic (AIT):**

In this type of fraud, a fraudster sends a message to itself via a SIM Farm. Look out for commercial loopholes to make money from a transaction.

## **How are SMS threats detected and resolved?**

Operators have now become more aware of their network security. To ward off the fraudsters they need to track the traffic coming and going out of their networks in real-time. With SMS Firewall, operators can protect their SMS network from hostile spam attacks. SMS Firewall filter enables the operator to react to the new threats quickly.

## **How does SMS firewall protect against spoofing?**

As soon as the SMS Firewall detects the MO-spoofed message it blocks a foreign SMSC or a device pretending to be an SMSC to send a message to the network.

### **Spamming:**

SMS Firewall intercepts the message, generated by a foreign SMSC for inconsistencies in headers and message content. If it detects any inconsistency, then the message may be blocked.

### **Anti Flooding:**

The SMS Firewall filter detects the sudden spike in traffic from the same originator. It continuously monitors short and long term traffic. If a short term traffic average is more than long term traffic by a certain margin for a long period of time, flooding is detected.

### **Pattern detection:**

Here the duplicate filter detects messages which are similar to a large number of recent messages. Once such a group is detected, a duplicates filter starts to track them closely.

### **Content Filtering:**

The content filter detects the messages that contain a word or phrase from the setlist. If any match is found then the message is blocked.



## About Globe Kconnect

Globe Kconnect provides Automated SMS Marketing Services to send Bulk SMS online globally. Our various SMS products are A2P Messaging, SMS Firewall, International Bulk SMS, SMSC, VOIP, Reseller Panel & more. The Globe Kconnect multicultural, multiracial, and the multilingual global team is spread across all major time zones to address the needs of our clients as quickly and as efficiently as possible.

Globe Kconnect provides Automated SMS Marketing Services to send Bulk SMS online globally. Our various SMS products are A2P Messaging, SMS Firewall, International Bulk SMS, SMSC, VOIP, Reseller Panel & more.

SMS Firewall offers mobile operators a secure spam-free roaming & messaging environment

## Conclusion:

As soon as SMS Firewall detects the MO-spoofed message it blocks a foreign SMSC or a device pretending to be a SMSC to send a message to the network.

### **Spamming:**

SMS Firewall intercepts the message, generated by a foreign SMSC for inconsistencies in headers and message content. If it detects any inconsistency, then the message may be blocked.

### **Anti Flooding:**

The SMS Firewall filter detects the sudden spike in traffic from the same originator. It continuously monitors short and long term traffic. If a short term traffic average is more than long term traffic by a certain margin for a long period of time, flooding is detected.

### **Pattern detection:**

Here the duplicate filter detects messages which are similar to a large number of recent messages. Once such a group is detected, a duplicates filter starts to track them closely.

### **Content Filtering:**

The content filter detects the messages that contain a word or phrase from the setlist. If any match is found then the message is blocked.