Guidelines on Reducing Fraudulent SMS

Issued by the

Telecommunications Regulatory Authority of the

Kingdom of Bahrain

27 August 2025

OSD/25/03/01/01

Purpose: To outline effective measures for reducing SMS fraud, assessing the risks, and recommending steps for MNOs to protect users.

Introduction

As the telecom industry continues to evolve and expand, the risk of fraud in SMS (Short Message Service) communication is also on the rise. Safeguarding SMS from these increasing fraud risks is crucial to maintaining the integrity and security of communication networks. This guideline explores the various strategies that can be implemented to protect SMS from fraud in the telecom industry.

The telecommunications industry has seen a significant increase in fraud risks in recent years, particularly when it comes to SMS communication. The rise of mobile banking, online shopping, and other digital services that rely on SMS for authentication has created new opportunities for fraudsters to exploit vulnerabilities in the system. As a result, it is increasingly important for MNOs to implement robust security measures to safeguard SMS transactions and protect their customers from potential fraud.

Given the rapid increase in SMS fraud, it is necessary to adopt robust, proactive measures aimed at protecting users. In response, the Telecommunications Regulatory Authority (the "**TRA**") has drafted these guidelines to outline effective measures for reducing SMS fraud, assessing the risks, and recommending steps for MNOs to protect users.

1 Purpose

1.1 Through this initiative, the TRA seeks to protect users from SMS fraud by requesting mobile network operators (**MNOs**) to:

a) adopt technical specifications for the detection and prevention of SMS fraud;
b) implement measures to mitigate the risk of users being exposed to SMS fraud;
c) publish guidelines for users and provide tools that will enable users to manage SMS fraud; and
d) provide users with a mechanism to report and block fraudulent SMS.

1.2 It is important that at all times MNOs ensure compliance with Bahrain's legal and regulatory frameworks, including the Telecommunications Law and Data Protection Law.

SMS fraud includes without limitation:

Identity Theft:

- **SMS Originator Spoofing:** Forging the sender's phone number or ID to make an SMS appear as though it is from a trusted source, often to deceive the recipient.
- **SMS Phishing:** Sending fraudulent SMS messages to deceive individuals into disclosing sensitive information.
- **Access Hacking:** Unauthorized intrusion into systems with the intent to gain control or access sensitive information.

Data Theft:

- **SMS Roaming Intercept Fraud:** Unauthorized interception of SMS messages sent to a victim's mobile device while roaming internationally.
- **SMS Malware:** Malicious software delivered via SMS designed to infect a mobile device, steal data, or perform unauthorized actions.
- **SMS Hacking:** Unauthorized interception of SMS communications to gain access to sensitive information.

Network Manipulation:

- **Mobile Application Part "MAP" Global Title Faking:** Manipulating the Global Title (GT) within the MAP signaling protocol to manipulate SMS or other network transactions.
- **Signaling Connection Control Part "SCCP" Global Title Faking:** Altering the Global Title in the signaling layer to misdirect messages and gain unauthorized access
- **Short Message Service Center "SMSC" Compromise Fraud:** Unauthorized access to an SMSC, enabling them to send fraudulent messages or exploit the service for malicious purposes.

Commercial Exploitation:

- **Grey Routes, Bypass, Non-interworked Off-Net routes:** Unauthorized or unofficial routes used to bypass traditional mobile networks. Used to reduce costs, evade regulation, fraud, spam, or illegal messaging which results in revenue loss for legitimate mobile carriers and potential security risks for end users.
- **SIM Farms:** Large-scale operations where multiple SIM cards are used to send fraudulent messages, often for the purpose of bypassing security measures or generating revenue through fraudulent traffic.
- **Spam:** Malicious messages sent in bulk, typically for advertising or fraudulent purposes.
- **Artificial Inflation of Traffic (AIT):** The manipulation of network traffic data to artificially increase the volume of messages, usually for fraudulent purposes, such as inflating revenue or exploiting telecom networks.
- **Message Trashing:** Intentionally discarding or blocking legitimate messages to disrupt communication services or exploit the network for fraudulent purposes.

2 Technical Specifications for SMS fraud

MNOs should implement robust technical solutions to detect and block SMS fraud effectively. These solutions should include the following key technical requirements:

2.1 **Layered and Near-Real-Time Detection:** Solutions should utilize a layered approach to identify and intercept potential SMS fraud in near-real-time, by analyzing message metadata such as sending patterns, frequency and origin.

2.2 **Adaptive Machine Learning Models:** MNOs should deploy adaptive machine learning models that continuously evolve to detect new fraud techniques, improving accuracy while minimizing false positives.

2.3 **Scalability and Integration:** Solutions should be scalable to handle high volumes of SMS traffic without compromising users' service quality and should integrate seamlessly with existing network infrastructure.

2.4 **International Standards:** Solutions should comply with international standards for privacy and data security, such as ISO/IEC 27001 for Information Security Management and ISO/IEC 200000 for Information Technology Service Management.

3 Measures to mitigate the risk of users being exposed to SMS fraud

3.1 **User Education and Awareness:**

One of the most effective ways to prevent SMS fraud is through education. MNOs should regularly educate their users about the dangers of SMS fraud, how to recognize suspicious messages, and what steps to take if they believe they have been targeted.

3.2 **Implement SMS Filtering Solutions:**

MNOs may deploy advanced SMS filtering solutions to monitor incoming text messages for signs of malicious content. These systems can identify fraudulent SMS messages based on known attack patterns, URLs, and keywords, helping to block them before they reach end-users.

3.3 **Multi-Factor Authentication ("MFA"):**

While MFA cannot directly prevent SMS fraud, it provides an extra layer of protection if a victim's credentials are compromised through an SMS fraud attack. By requiring a second factor, such as a code sent via email or an authentication app, MFA reduces the risk of unauthorized access to user accounts.

3.4 **Regular Penetration Testing and Security Audits:**

MNOs may conduct regular penetration testing to identify vulnerabilities within their networks and services that could be exploited in SMS fraud attacks and undergo regular security audits to ensure that any gaps in security are addressed promptly.

3.5 **Publish guidelines:**

MNOs are required to publish up-to-date guidelines on their website, detailing the various types of SMS-related fraud risks that subscribers may encounter. These guidelines should be clear, easily accessible, and regularly updated to reflect emerging threats.

3.6 **Provide SMS fraud mitigation services:**

MNOs must clearly communicate information regarding available products or services designed to help block suspicious SMS fraud. This includes explaining the functionalities of these products and services and providing user-friendly instructions on how to use them.

3.7 **Offer risk mitigation recommendations:**

MNOs should provide recommendations to users on how to mitigate the risks associated with SMS fraud.

3.8 **Define action steps for users:**

MNOs should inform users of the necessary actions to be taken when receiving a fraudulent SMS, including instructions on how the fraudulent SMS should be reported, steps to secure users' accounts, and how to prevent future occurrences.

4 Establish a mechanism for users to be able to report and block fraudulent SMS

4.1 MNOs may implement mechanisms that allow users to report suspicious SMS messages, with the reported messages being subject to further validation before any blocking action is taken.

4.2 MNOs must maintain and update blacklists of fraudulent numbers associated with SMS fraud campaigns;

4.3 MNOs must cooperate with the TRA to track and report fraudulent numbers, enhancing fraud prevention at the network level; and

4.4 MNOs must provide an accessible reporting mechanism that enables users to flag fraudulent messages.

4.5 Appropriate safeguards should be in place to prevent the blocking of legitimate SMS due to false or mistaken reports.

5 Consent and privacy requirements

In undertaking these SMS fraud prevention measures, MNOs should at all times act in accordance with the Data Protection Law of the Kingdom of Bahrain and the Data Protection Guidelines[1] published by the TRA and all other applicable statutory and regulatory requirements.

6 Transparency

MNOs should ensure transparency in their practices, specifically regarding data security and SMS fraud prevention through:

6.1 Informing users about data security

MNOs should inform users about the steps taken to secure their data, including measures taken to prevent unauthorized access or misuse. This information should be easy to understand and readily accessible.

6.2 Establishing a privacy complaints and breach resolution mechanism

MNOs should establish clear and effective mechanisms for handling privacy complaints and data breaches, ensuring timely investigations and resolutions.

6.3 Reviewing and updating practices

MNOs should periodically review and update fraudulent SMS prevention practices to keep up with evolving threats. Any significant changes should be communicated to users in a timely and transparent manner, ensuring they are informed of updates that may affect them.

7 Accuracy and Fairness

Where implemented, MNOs must ensure the highest level of accuracy in SMS fraud detection systems:

7.1 Detection Accuracy Rate:

[1] مجلس التنمية الاقتصادية البحرين | Personal Data Protection Law and https://tra-website-prod-01.s3-me-south-1.amazonaws.com/Media/Documents/Position_Papers_&_Guidelines/20240213131935547_r5djoxiq_cu5.pdf

SMS fraud detection systems should aim to achieve a minimum accuracy rate of 99%, blocking the vast majority of fraudulent SMS while ensuring minimal disruption to legitimate communication.

7.2 **Minimization of False Positives:**

MNOs must maintain a false positive rate below 1% and continuously monitor and refine detection algorithms, minimizing the impact on users' legitimate communications.

7.3 **Bias Minimization:**

Detection algorithms in SMS fraud should be regularly evaluated to ensure they are fair and unbiased across all users' demographics, ensuring the system does not discriminate based on factors such as language, region or users' behavior.

7.4 **Feedback Mechanism:**

MNOs should provide a feedback system for users allowing them to report false positives or undetected fraudulent SMS, this feedback will help improve system performance and enhance user protection.

8 Reporting Requirements

To ensure the effectiveness of fraudulent SMS mitigation efforts, MNOs must submit annual reports to the TRA by the 31st of January of every calendar year. These reports should adhere to the format specified in Appendix A.

Appendix A:

Annual Report

	Current Period *(month/year to month/year)*	**Previous Period** *(month/year to month/year)*	**Change (%)**
Total Number of SMS Blocked			
Number of SMS Blocked			*Increase, decrease, no change (%)*
System Accuracy			
Total False Positives			*Increase, decrease, no change (%)*
Subscriber Complaints			
Total Complaints Received Related to SMS Fraud			*Increase, decrease, no change (%)*
Type of complaints (Breakdown)			
False Positive			*Increase, decrease, no change (%)*
False Negative			*Increase, decrease, no change (%)*
Privacy Concern (data security, unwanted data collection)			*Increase, decrease, no change (%)*
Performance Issue (delayed SMS delivery)			*Increase, decrease, no change (%)*