# Addressing the text scam scourge

https://opinion.inquirer.net/178622/addressing-the-text-scam-scourge

Receiving scam text messages is sadly becoming a part of life despite the implementation of the subscriber identity module card registration law and the efforts by the government and telecommunication companies (telcos) to weed out mobile numbers and SIM cards used in fraudulent activities.

During the Senate plenary budget deliberations last week, Sen. Sherwin Gatchalian, speaking on behalf of the Department of Information and Communications Technology (DICT) as sponsor of its P7.8-billion budget request for 2025, reported that some 10.8 million mobile numbers have been blacklisted and another 2.3 million SIM cards deactivated so far this year on suspicions that these were being used in scams. He added that the National Telecommunications Commission (NTC) also blocked more than 2.2 billion text messages that were sent by scammers involved in various fraudulent activities.

“The good thing is that the NTC managed to block a lot of SIM cards and prevented spamming and scamming from happening,” Gatchalian said.

However, consumer complaints abound in social media about being victimized by text scams in various forms. One plausible reason is that fraudsters seem to always be a step ahead of regulators and telcos. Proof of this is that text scams are now being sent through the legitimate numbers used by Globe Telecom, Smart Communications Inc., and their e-wallets GCash and Maya.

## ‘Fake cell towers’

How is this even possible? As early as May this year, Smart has warned the public that scammers were using what it calls “fake cell towers” to send text scams to mobile users, and were even using “Smart” as the sender name. It explained that these devices are able to lock on to mobile phones within a specified radius, enabling the scammers to push messages directly to subscribers’ devices without having to go through its network. The illegal “cell site simulators” can also spoof or mimic mobile numbers to deceive subscribers into thinking that they are receiving legitimate text messages, it warned.

These cell site simulators are typically used in disaster-stricken areas as temporary emergency communication platforms and their sale is regulated. How scammers gain access to these devices that are not made locally is easy to find out. The Bureau of Customs can start with the list of authorized importers, then the NTC or DICT can go over the list of their clients and check if these devices are being used for legitimate purposes. In short, it has to strictly regulate the importation and use of these types of equipment so these do not fall into the hands of scammers.

## Attractive baits

Another measure is to go back to what Gatchalian had suggested last June: Telcos should be made liable whenever their registered SIM cards are used in scamming activities, or answer for the SIM cards recovered by authorities in the course of their operations against cyber criminals. Sen. JV Ejercito also agreed that telcos should be held accountable for the continued spread of text scams and the use of SIM cards in scamming activities.

True, consumers need to take part of the blame. A penchant for things that are free is a problem that lies solely with the mobile users themselves. Imagine receiving a text from seemingly legitimate senders such as shopping sites and courier services with free vouchers or tracking codes for parcel deliveries you did not order. Or even a job or investment opportunity promising high salaries and returns that actually does not exist. These are very attractive baits that lure many potential victims.

However, the bigger responsibility in combating this text scam problem is with the telcos, not with the government agencies or the millions of mobile users nationwide. Globe has advised its subscribers to “think before clicking on links, verify the sender’s identity, (and) report scam or spam messages to Globe or to the NTC via their scam/spam report page.” However, changing mobile numbers, reporting scams to authorities, and blocking spam calls through various security apps in mobile phones do not all seem to work.

## Preventive measures

Blocking and deactivating suspicious texts and SIM cards are curative actions. What the consumers need are preventive measures on the part of the government and the telcos. One nagging question begging for an answer is: How have telcos not figured out until now how to prevent this text menace?

Regulators, for their part, can look into adopting a measure similar to Singapore’s Shared Responsibility Framework (SRF), which will take effect on Dec. 16 this year. Jointly developed by the Monetary Authority of Singapore and the Ministry of Communications and Information’s Infocomm Media Development Authority, the SRF introduces a structure that requires losses from certain types of phishing scams to be shared among the victims, financial institutions, and telcos. Locally, the structure should cover all digital fraud schemes, including text scams, to put everyone on high alert about this headache.