# Telecom fraud can be fought using technology and collaboration

**FAUSTINE NGILA**
THE EAST AFRICAN

The East African region has experienced tremendous growth in broadband connectivity, owing to the landing of the undersea fibre optic cables along the coast, with the result being a reduction in prices for higher internet speeds. That has been supported by the penetration of 4G LTE networks and greater smartphone penetration. Global technology research powerhouse, Ovum, forecasts that there will be 32 million LTE subscriptions in Kenya, Tanzania and Uganda by 2022, while smartphone connections will be 108 million.

The benefits for the region include growth of the digital services segment and mobile financial services, amongst others, but they have been accompanied by a spike in Cybercrime. Data revenue cannibalization for data service providers in the region is among the symptoms and Mobile National Operators (MNOs) and regulators have borne the heaviest brunt of this menace by losing millions of dollars in revenue through the fraudulent use of SIM boxes.

The more technical term for the concept is interconnection bypass fraud and is a process whereby person or group of people set up a device that can take up several SIM cards (a SIM box) and use it to complete international calls it receives from the Internet as voice over Internet Protocol (VoIP) and in turn serve them to the in-country mobile network subscribers as local traffic. This allows the *simboxer* to bypass international levys and claim the 'bypass profit'.

Telcos need to find a solution towards diminishing margins while being tasked to address the ever-increasing customer demands by investing in new technologies. The threat posed by SIM box fraud will therefore impede the growth of mobile telephony across the region, thereby slowing down the journey towards digital transformation. Experts are of the opinion that if adequate strategies through collaboration are not implemented, more revenue losses and security lapses become imminent.

**Telcos need to find a solution towards diminishing margins while being tasked to address the ever-increasing customer demands by investing in new technologies.**

According to the Uganda Communications Commission (UCC), the country continues to lose high tax revenues to SIM box fraud. Telecom revenue analysis by various experts estimates that in 2016, telecom companies in Uganda were losing about $60 million annually to SIM box fraud. Other than the direct impact on the operators' bottom line, it causes traffic disruption on networks, and the quality of service suffers due to network congestion. In a bid to avert rising cases of fraud, the UCC in July suspended SIM card registration for companies, non-governmental organisations and government agencies, ministries and agencies until further notice.

"The registration of SIM cards for companies, non-governmental organisations, ministries, departments and agencies or unnatural persons has been suspended to avert further risks pending completion of an ongoing investigation", Ms Irene Kaggwa Sewankambo, the UCC acting executive director, said in a statement.

According to a survey published in the January/February 2019 issue of the IOSR Journal of Mobile Computing and Application under the title, Grappling with the Challenges of Interconnect Bypass Fraud, regulators must task service providers and implementers to provide a location-aware system and enhanced bypassed traffic detection. Such a system has the capability of providing the global position system (GPS) coordinates for the exact location of the SIM box and also to identify fraudulent VoIP calls in real-time. Such proposed intelligent solutions could be software or hardware devices programmed to intelligently detect cases in real-time and then enforce immediate blocking of the SIMs detected.

Ultimately, the fight against fraud in the region benefits from an increase in joint collaboration strategies to identify, track and dismantle criminal networks, similar to what recently happened in Ghana during November 2020. In the first week of November, an operation between the National Communications Authority (NCA), Ghana Revenue Authority (GRA,) and the Accra Regional Police Command supported by Kelni GVG, led to a massive dismantling of a criminal network, that had in its possession more than 100 SIM cards, 90 recharge cards and 32 channel SIM box, among others. On 7th November a very similar illegal operation (SIM Box) at Anloga in the Kumasi Metropolis was uncovered by the Ashanti Regional Police Command together with the representatives from the NCA and Kelni GVG. In addition, on 26th November, Accra was the centre of yet another raid, which led to the further confiscation of equipment used in terminating international calls as local calls.

There is still a long road ahead to mitigate these criminal activities. But the time to act is now.