COMMUNICATIONS AUTHORITY OF KENYA

PRESS STATEMENT

FOR IMMEDIATE RELEASE

19th July 2018

ALERT ON DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) LEADING TO SIM CARD SWAP FRAUD

The Communications Authority of Kenya (CA), through the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC), has received reports of theft of Personally Identifiable Information (PII) through social engineering leading to SIM SWAP fraud.

Personally Identifiable Information (PII) refers to any information that can be used to distinguish or trace an individual's identity, such as mobile money PIN, national ID number, bank account PIN, password, date of birth, among others. PII is information that can be used to uniquely identify or authenticate a person.

In the case of SIM Card Swap Fraud, a fraudster usually makes a call pretending to be an employee of a mobile network operator. The fraudster further asks the unsuspecting mobile subscriber to share their Personally Identifiable Information (PII) such as their national ID number, mobile money PIN, or SIM card PIN, among others. After obtaining the Personally Identifiable Information, the fraudster then goes ahead to swap the SIM card thereby gaining access to all the SIM services including mobile money transfer, mobile and internet banking, voice calls, SMS, data services and any other service that can be accessed through the SIM.

In exercising its mandate of sensitizing and awareness creation on Cybersecurity related matters, CA is therefore advising the public to be vigilant and put in place the following preventive measures:

- **Be Cautious.** Do not respond to calls or emails asking for Personally Identifiable Information (PII) such as mobile money PIN, national ID number, bank account PIN, password, date of birth, unless you are sure of whom the person you are

corresponding with. Always verify the authenticity of the person through the official customer care contacts of the service provider.

- **Delete any request for financial information or passwords.** If you get asked to respond to a request with personal information, it's a scam.
- **Your PIN is Your Secret.** Never divulge any of your PINs to anyone, not even the mobile money service provider or agent.
- **Slow down.** Fraudsters want you to act first and think later. If the request conveys a sense of urgency, or uses high-pressure tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages or requests. If the request looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their official contacts.
- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' a scam.
- **Report Fraud Cases.** Immediately reports any such incidents to the Service Provider, the nearest Police Station, and to the National KE-CIRT/CC.

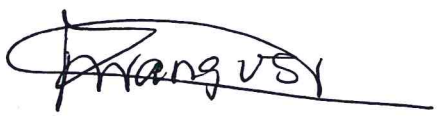
The Authority also wishes to take this opportunity to thank stakeholders, including members of public, for their continued support and further reiterates its commitment to enhancing the safety of Kenya's cyberspace.

About the National KE-CIRT/CC

The National KE-CIRT/CC is Kenya's national cyber-crime management trusted point of contact, and is globally recognized. Members of the public are therefore advised to contact the National KE-CIRT/CC via the email address incidents@ke-cirt.go.ke or through the dedicated 24/7 hotlines +254-703-042700/+254-730-172700, to report such incidences or seek advice on cybersecurity.

For further information, visit the National KE-CIRT/CC website at http://www.ke-cirt.go.ke or through the Authority's website at http://www.ca.go.ke.

Issued by:



Francis W. Wangusi, MBS
DIRECTOR-GENERAL