PRESS RELEASE

CLARIFICATION ON ISSUES RAISED IN THE "STORY PANIC AS NATIONAL ID DATA IS STOLEN"

Reference is made to the lead story in the **Sunday Vision of June 25, 2017 titled Panic as National ID Data is Stolen**, which further says that confidential data submitted to and in possession of the National Identification and registration Authority (NIRA) could have landed into wrong hands.

The article is premised on a case currently under investigation by the Criminal Investigation Directorate (CID) of the Police in which a city businessman is alleged to have lost 51m shillings through a fraudulent payment to a one Norbert Kamwebaze.

Whereas the article refers to an on-going investigation, NIRA notes that the headline to the story is not only incorrect, but is misleading and has serious implications for national security if not immediately corrected. In addition we note that the most of the adduced supporting information in the article is not only inaccurate, but also a serious misrepresentation and reflects lack of understanding of how the national ID data is gathered, stored, shared and managed. We believe the authors of the article could have obtained the right information and informed the public better if they had good intentions.

NIRA therefore wishes to clarify on some of the issues raised in the article as follows:

1. The National Identification Number (NIN) **CM8605210PADGW** mentioned in the story does not exist at all in the National ID Register (NIR). This is therefore a clear case of forgery and does not amount to identity theft as is suggested in the article.

2. A search of the National ID Register has been done to establish the right NIN of the mentioned Norbert Kamwebaze. Whereas the name indeed exists, his right NIN is different from the one quoted in the article.

3. NIRA also wishes to make it clear that access to data in the National ID Register is strictly regulated and guided by procedures laid down in the Registration of Persons Act 2015 contrary to what is alleged in the article. The established

procedures restrict access to data to specific offices at NIRA and no persons other than those stated in the law can access data. The process of establishment of the national ID register envisaged risk to data security, hence the establishment of stringent technical and legal controls on data access.

"No NIRA staff other than those designated by internal control procedures and policies can access data in the NIR. It is therefore erroneous to suggest that the information could have been leaked by a NIRA official"

4. On allegations that next of kin are required to sign NIRA documents, we wish to state categorically that there is no provision for next of kin to sign anywhere on any NIRA documents. NIRA does not use next of kin or anybody other than the applicants for national IDs to obtain information on identities of persons.

5. We also wish to re-state that no data from the National ID Register has been shared with the telecom companies during the on-going SIM Card validation exercise as alleged in the article.

   "The procedure for SIM card validation is such that the telecom companies submit their subscriber details to UCC which is later submitted to NIRA for verification. This information is then compared against the national ID data by NIRA and a simple YES/NO report is generated confirming whether a subscriber is registered and his or her NIN and names correspond to information in the NIR or not. The report is then sent to UCC for action."

   The information verified during the SIM card validation is strictly that which appears on the face of the ID card.

6. On allegations of people using others NINs to validate their SIM cards, we wish to inform the public that such cases existed a NO response will be sent to UCC and their SIM cards will be deactivated.

NIRA wishes to reassure the public that the national ID data is secure to the highest security levels and access to that data is strictly according to the Registration of Persons Act 2015 and regulations. Whereas this appears to be a clear case of forgery, Due diligence by ROKO could have established the authenticity of the identity card before making the payment. We wish to re-state our commitment to cooperate with and support the Police and other law enforcement agencies in investigating and prosecuting and cases of forgery or theft of identity documents and data

NIRA MANAGEMENT

FOR GOD AND MY COUNTRY