DATA BREACHES IN NIGERIA: THE CASE OF THE NATIONAL IDENTIFICATION NUMBER

There have been suspicions of a data breach on the database of the National Identity Management Commission (NIMC), the Commission responsible for establishing a National identity data base and issuing identity cards. These suspicions were fueled by reports from the Foundation for Investigative Journalism (FIJ) which reported that the data of Nigerians embodied in their National Identification Number(s) (NIN) had been publicly disclosed. NIMC has since debunked these reports by simply denying its occurrence. However, available evidence suggests otherwise as several websites publicly offered the NIN for sale before they were eventually taken down. If the breach did occur, as supported by available evidence, such breach has the potential to put the data of over a hundred million Nigerian citizens at risk.

A data breach is said to have occurred whenever there is a security incident which results in unlawful processing of personal data. In the case of NIMC, this breach might be an indication of weakness in the technical, organisational and other security measures that have been adopted in the protection of the National identity database. This, therefore, necessitates a possible reconsideration of the data privacy and security framework of the national identity database. It also calls to question, the need for a more robust and stricter monitoring and enforcement of (existing) (data protection) laws in Nigeria.

The NIMC Act prohibits access to information stored in the national identity database by 3rd parties, except with the authorization of NIMC and the individual(s) whose information is sought. The information deducible from, or collected as part of the NIN registration process includes demographic data, fingerprints, picture, other biometric data and digital signature. The NIMC Act further provides the disclosure of said information in the interest of National security, crime detection and prevention, or for any other purposes it might specify by way of regulations.

Furthermore, section 40(2) NDPA provides that a data controller shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the Commission of the breach and, where feasible, describe the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned. The essence of this notification includes helping data subjects anticipate the effects of such breach and take precautionary steps where possible. Following the denial of the breach by NIMC, it is necessary that appropriate investigations be conducted by the Nigeria Data Protection Commission (NDPC) to ensure risk mitigation and prevention. The identification and mitigation of data breaches requires subject matter expertise to control, mitigate, and prevent reoccurrence. NIMC has taken steps to ensure that a data breach of this nature does not reoccur by restricting the access of licensed agents to the NIN database. Although there is no evidence that other technical and organisational measures traceable to the root cause of the breach have been considered. We are also yet to see the outcome of the investigation instituted by the NDPC.

A security audit is another measure that ensures the systematic evaluation of an organization's information system against best practices. A thorough audit typically assesses the security of the system's physical environment, software, information handling processes and user practices. It is necessary to revisit and strengthen data protection and security as it pertains to the NIMC database. In the instant case, only NIMC ought to have access to its database. Any possible breach by bad faith actors can only emanate from the NIMC database which is completely in NIMC's custody. For breach mitigation and remediation to be effectively carried out, a thorough security audit that identifies the source and cause of the breach is necessary.

To reduce the (re)occurrence of critical data breaches, a holistic approach to data security which prioritizes state of the art technical and organisational measures must be established, to resolve data breaches right from discovery to mitigation and resolution. Organizations must be proactive to effectively safeguard sensitive information from potential threats, unlawful access, and bad faith actors.

Contributors


Emmanuel Salami, PhD


Ogunshola Ademola Francis