MOROOM AFRICA

Data Protection by Famsville Series

Passwords, Privacy & Penalties: Lessons from the Largest Credential Leak in History

As technology and intelligence continue to evolve at an accelerated pace, the risks associated with personal data usage and security breaches have become a growing point of focus.

Cybernews[1] has recently confirmed what is now considered the largest credential leak in history, over 16 billion passwords have been exposed online, potentially granting access to numerous digital platforms, including Google, Facebook, Apple, and enterprise systems worldwide.

For Nigerian Data Controllers[2] and Data Processors[3], this is more than an Information Technology (IT) problem, it is a legal issue that calls for urgent action under the extant data protection laws and regulations in Nigeria.[4]

This series explores the lessons to be learned and the compliance steps to be taken.

Why This Matters to Data Controllers and Data Processors

Given that Nigeria's data protection laws now extend to data controllers and data processors who do not have any physical presence or are not domiciled in Nigeria but process or target the personal data of data subjects[5], the implications of this breach are far-reaching and potentially global in scope.

Data controllers and processors are required to implement appropriate technical and organisational measures to ensure data security, integrity and confidentiality.[6] Such measures include: pseudonymisation or other methods of de-identification of personal data; encryption of personal data, amongst others. Failure to do this, especially in the case of a global breach as this could expose the data controller or data processor to heightened risks, from reputational damage to regulatory penalties from the Nigeria Data Protection Commission (NDPC).

Why This Matters to Data Subjects

The exposure of billions of passwords and the scale of this data breach underscore the vulnerabilities that everyday users face in today's digital landscape. While the risk of security breaches can be mitigated, they remain an unfortunate reality. When a breach of this nature occurs, data subjects[7] may face a range of adverse consequences, including identity theft, financial loss, reputational harm, and

1 https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/ (last accessed 24/06/2025)
2 A Data Controller means an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data – see section 65 of the Nigeria Data Protection Act, 2023.
3 A Data Processor means an individual, private entity, public authority, or any other body that processes personal data on behalf of or at the direction of a data controller or another data processor.
4 Extant Data protection laws in Nigeria include: the Nigeria Data Protection Act (NDP Act), 2023, the NDP Act, General Application and Implementation Directive, 2025, amongst others.
5 Article 2 of the NDP Act GAID 2025.
6 Section 39 of the NDP Act, 2023.
7 A Data Subject means an individual to whom personal data relates– see section 65 of the Nigeria Data Protection Act, 2023

unauthorised access to private accounts. Even where an individual is not directly affected, the global scale of the leak increases the risk of exploitation by malicious actors for all internet users.

Under the NDP Act, individuals have the right to be informed of personal data breaches that present a high risk to their rights and freedoms.[8] This gives data subjects the opportunity to take timely and necessary steps, such as:

- creating stronger, unique passwords;
- enabling multi-factor authentication (MFA);
- and monitoring for suspicious activity, to reduce potential harm and safeguard their personal information.

Legal & Compliance Lessons

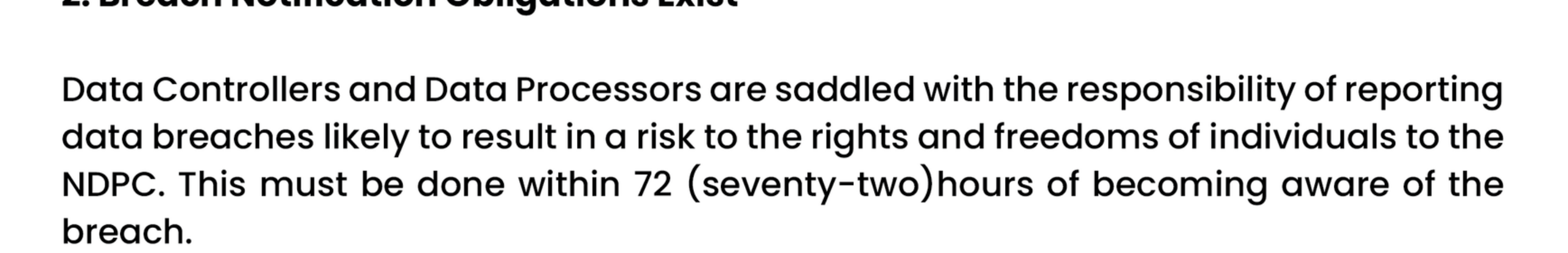
1. Violation of Data Security Obligations

Storing or encouraging the use of weak or unencrypted passwords without layered security controls (e.g., MFA) could be deemed a violation of data security obligations under the NDP Act.

2. Breach Notification Obligations Exist

Data Controllers and Data Processors are saddled with the responsibility of reporting data breaches likely to result in a risk to the rights and freedoms of individuals to the NDPC. This must be done within 72 (seventy-two)hours of becoming aware of the breach.

Where the data breach will constitute a high risk to the rights and freedom of the individuals, the data controller must immediately communicate the personal data breach to the data subject in plain and clear language or communicate through the public using widely used media sources such that the data subject is likely to be informed.



8 See section 40(3) of the Nigeria Data Protection Act, 2023.

What Data Controllers and Processors Should Do — Now

- Assessment/ audit of systems and services to identify risks of exposure to data breaches.
- Implement multi-factor authentication (MFA) and prohibit the reuse of passwords across various platforms.
- Implement the necessary technical and organisational measures to ensure data security.
- Train your team on data privacy and security, especially phishing and password hygiene.
- Update your data privacy documentation and incident response plan to reflect the NDP Act-compliant standards
- Engage a Data Protection Compliance Organisation (DPCO) to ensure readiness for NDP Compliance audits.

Conclusion

The largest credential leak in history is a wake-up call for organisations to move beyond checkbox compliance and adopt a truly proactive approach to data protection. In Nigeria, where the NDP Act has strengthened regulatory expectations, ignoring the risks of poor password management and security practices is no longer an option.

Data controllers and processors must act swiftly to assess their vulnerabilities, enhance their cybersecurity frameworks, and ensure continuous compliance with legal obligations. The cost of inaction is high, both in terms of regulatory penalties and the erosion of public trust. Now is the time to tighten the bolts of privacy and security before the next breach strikes.

Authors

Dayo Adu
Managing Partner

Rachael Olayemi
Associate

Uzochukwu Kpaduwa
Associate