DATA BREACHES AND NIGERIA'S DIGITAL INFRASTRUCTURE: AN ANALYSIS OF RESILIENCE, RESPONSIBILITY, AND REGULATORY RESPONSES

Chukwuyere Ebere Izuogu
&
Favour Osayuwamen

Image credit: https://www.idagent.com/blog/data-breach-duplicate/

Introduction

Digital infrastructure has evolved into critical national infrastructure, forming the backbone of modern governance, financial services, and the broader architecture of national economic coordination. As Nigeria continues to digitise public services and our economy increasingly depend on interconnected platforms for transactions, communication, and data exchange, the reliability, resilience, and security of these systems have assumed heightened national significance. Protecting digital infrastructure is therefore no longer solely a technical or operational matter; it is a strategic national priority essential to sustaining institutional continuity, safeguarding sensitive information, and maintaining the stability of vital public and private sector services.

Within this ecosystem, payment platforms, banking networks, and government revenue systems rely extensively on interconnected digital environments that process vast volumes of sensitive information each day. These systems have enabled greater efficiency, transparency, and scale in both public administration and commercial activity. At the same time, their growing interdependence introduces complex cybersecurity risks. Vulnerabilities within a single institution can propagate across interconnected systems, potentially disrupting critical services and exposing the personal information of millions of individuals. As a result, strengthening the security and resilience of digital infrastructure has become an essential component of contemporary governance and economic policy.

Recent reports of a cybersecurity incident involving Sterling Bank Plc, the government payment infrastructure operated through Remita, and data connected to corporate records held by the Corporate Affairs Commission (CAC), Nigeria' company registry have raised serious questions about cybersecurity governance and data protection compliance in Nigeria. Available reports suggest that the incident may have been triggered by an unpatched vulnerability in a bank server, which enabled a malicious actor to gain unauthorised access and subsequently use that access as a staging point for further intrusions into interconnected systems.

The significance of the incident lies not only in the technical compromise itself but also in the nature of the data potentially affected. The systems involved contain information connected to financial transactions, government payments, and corporate registration records. Such datasets frequently contain personally identifiable information and therefore fall within the regulatory scope of the Nigeria Data Protection Act 2023 (NDPA) and the subsidiary regulatory instrument issued by the Nigeria Data Protection Commission (NDPC) through the General Application and Implementation Directive (GAID).

Against this background, we examine the reported cybersecurity incident and the associated data breaches. We assess whether the compromised

information constitutes personal data under Nigerian law, evaluate whether the applicable legal framework triggers data breach notification obligations, and propose regulatory steps that may be necessary to safeguard individuals and strengthen the resilience of Nigeria's digital infrastructure.

Description of the Cybersecurity Incidents and Data Breaches

The Initial Compromise

The cybersecurity incident appears to have originated on 18 March 2026, when a publicly exposed server associated with Sterling Bank responded to a malicious request exploiting a known vulnerability identified as CVE-2025-55182.[1] This vulnerability reportedly allowed remote command execution on a server running a web application framework. Because the flaw permitted unauthenticated access, a threat actor could execute commands on the server without requiring valid credentials.[2]

Security researchers had previously documented this vulnerability, and a software patch had already been issued.[3] However, the affected server had reportedly not been updated.[4] The compromised system was believed to form part of a pilot or testing environment within the bank's infrastructure.[5] While testing environments are sometimes considered less critical than production systems, they can nonetheless provide attackers with entry points into broader internal networks. Once the vulnerability was exploited, the attacker obtained command-level access to the server. This access enabled exploration of the system environment, the deployment of tools, and the possibility of lateral movement across connected infrastructure.

Establishment of Command Infrastructure

Following the initial intrusion, the attacker reportedly established a command-and-control (C2) channel using a remote server address. A C2 channel is a hidden communication pathway that enables a threat actor to remotely interact with and direct a compromised device or system inside a target network.[6] Such infrastructure enables attackers to maintain persistent access to compromised systems while concealing operational activities.

C2 systems are commonly used in sophisticated cyber intrusions. They allow attackers to issue instructions, retrieve data, and manage compromised systems remotely. By maintaining control of the affected server environment, the attacker could conduct further reconnaissance and identify connections between the bank's internal systems and external platforms.

Pivot into Payment Infrastructure

Evidence suggests that the compromised Sterling Bank server was subsequently used as an operational corridor to conduct further attacks on payment infrastructure connected to Remita.[7] Remita functions as a central platform for processing government payments and financial instructions associated with Nigeria's Treasury Single Account (TSA) framework.[8] The platform facilitates salary payments for public sector workers and processes revenue

[1] David Odes, 'Sterling Bank & Remita: How a Global Hacker Walked Through Nigeria's Banking Sector and Took Everything' (8 April 2026) < https://securityintelligence.substack.com/p/sterling-bank-and-remita-how-a-global-f9c > accessed 25 April 2026.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Paloatonetworks, 'What is a Command and Control Attack?' (n.d) < https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained#:~:text=Malicious%20network%20attacks%20have%20been,Ingress%20Tool%20Transfer > accessed 25 April 2026.
[7] Odes (n 1).
[8] Musa Oladipupo, 'Remita, the TSA, and Nigeria's Most

collections across ministries, departments, and agencies.

The attacker later claimed to possess approximately three terabytes of data extracted from the Remita ecosystem.[9] If accurate, this dataset could include financial transaction records, payment instructions, institutional accounts, and other operational data processed through the platform. The potential scale of the breach is therefore significant. Because Remita serves as a central payment gateway for government financial operations, any compromise could affect multiple public institutions and potentially millions of transactions.

Exposure of Employee and Corporate Data

Additional data samples allegedly published by the attacker included detailed information relating to thousands of Sterling Bank employees.[10] The information reportedly contained employee names, emails, phone numbers, staff IDs, job roles, branch assignments, supervisor chains and other contact information.[11]

Separate references within the breach also suggested the presence of corporate registration information associated with the CAC. The CAC database contains records relating to companies operating in Nigeria, including information about directors, shareholders, addresses, and contact details. The CAC breach appears to have occurred around 10 April 2026 and involved weaknesses in the authentication and document management infrastructure supporting the company registry's internal administrative systems.[12] Technical evidence released by the attacker suggests that the breach of the company registry occurred after weaknesses were identified in CAC's login system.[13] By exploiting a flaw that allowed user accounts to be identified through predictable numbers, the attacker was reportedly able to obtain a valid login token linked to a staff account.[14] This access allowed entry into the internal administrative portal used to manage company registrations and corporate records. The attacker then created a new administrative account and assigned it extensive privileges, enabling broad access to internal systems and operational records.[15]

With this level of access, the attacker claims to have viewed and extracted large volumes of information containing personal identifiable data.[16] This reportedly included the names of company directors and shareholders, residential addresses, dates of birth, passport numbers, National Identification Numbers, email addresses, telephone numbers, and supporting identity documents submitted during company registration processes.[17] Although the full scope of the incident has not yet been independently verified, available evidence suggests that several categories of personal data may have been exposed, including employee records, government issued identification numbers, corporate registration information and other administrative datasets.[18] Given the role of the CAC as Nigeria's central company registry, the incident raises important legal and governance concerns about the protection of personal data, cybersecurity oversight and institutional accountability.

Successful Government Technology Project' (9 March 2026) < https://www.thecable.ng/remita-the-tsa-and-nigerias-most-successful-government-technology-project/ > accessed 26 April 2026.

[9] Odes (n 1).

[10] Ibid.

[11] Ibid.

[12] David Odes, 'I Spoke With ByteToBreach: The CAC Breach, Sterling Bank's €250,000 Ransom, and Why Nigeria' (16 April 2026) < https://securityintelligence.substack.com/p/i-spoke-with-bytetobreach-the-cac > accessed 26 April 2026.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

Legal Analysis of Data Breach Notification and Security Obligations

Whether the Breach Involved Personal Data

The NDPA in Section 65 defines personal data as

> any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

An individual is identified when he is capable of being 'distinguished' or 'singled out' from among a group of persons, and identifiable when, 'although the person has not been identified yet, it is possible to do' so.[19] Applying the statutory definition of personal data under Section 65 of the NDPA, the central inquiry is whether the information in question can identify an individual, either directly or indirectly, through reference to an identifier. On this basis, the categories of data reportedly exposed in the present incident clearly meet the legal threshold. The information includes direct identifiers such as names, telephone numbers, and email addresses, as well as indirect or quasi-identifiers such as passport numbers, national identification numbers, and residential addresses. When combined, these data points significantly increase the likelihood that individuals can be singled out, profiled, or otherwise distinguished within a broader dataset, thereby satisfying the statutory requirement of identifiability.

When assessed against the factual context of the incident, several distinct categories of information fall within this legal definition. Data reportedly associated with employees of Sterling Bank includes names, job roles, branch assignments, and contact details, all of which are inherently linked to identifiable individuals. Similarly, corporate registration records maintained by CAC routinely contain personal information relating to company directors, shareholders, and secretaries, including names, residential addresses, and identification details connected to natural persons involved in corporate governance structures. In addition, payment infrastructure systems such as those operated through Remita may process financial and transactional data linked to individuals, including account identifiers and payment records that can be traced back to identifiable persons.

The NDPA in Section 65 further characterises a personal data breach as any security compromise involving personal data that results in, or is likely to result in, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such data. On the basis of the categories of information reportedly affected, the incident therefore constitutes, at minimum, a likely unauthorised access to personal data within the meaning of the statute. It consequently falls within the regulatory scope of the NDPC, triggering the full application of the NDPA's compliance, supervisory, and enforcement framework.

Statutory Obligations to Secure Personal Data

Beyond breach notification obligations, the NDPA establishes a broader regulatory framework governing the security and protection of personal data. Section 24(1)(f) of the NDPA requires every data controller and data processor to ensure that personal data is processed in a manner that provides an appropriate level of security. This obligation encompasses safeguards against unauthorised or unlawful

[19] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> accessed 23 April 2021, pp. 12 - 13.

processing, unauthorised access, accidental or deliberate loss, destruction, damage, and other forms of compromise that may result in a personal data breach.

Within this framework, institutions that determine the purposes and means of processing personal data are classified as data controllers and are therefore subject to these statutory duties. In the context of the incidents under discussion, Sterling Bank, Remita and CAC each operate as data controllers in relation to the categories of personal data they collect, store and process. As such, they are required under the NDPA to implement appropriate technical and organisational measures to safeguard that data and to ensure that their systems, processes and service providers maintain adequate levels of security.

Complementing this obligation, Section 39(1) of the NDPA requires data controllers and data processors to implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data in their possession or under their control. These measures must take into account several factors, including:

- the amount and sensitivity of the personal data involved;
- the nature, degree, and likelihood of harm that could result from misuse or disclosure;
- the extent of the processing activities undertaken;
- the period for which the data is retained; and
- the availability and cost of security technologies relative to the size and capabilities of the organisation.

The NDPA further provides illustrative examples of the types of measures that may be required. These include encryption, pseudonymisation or other forms of de-identification, processes to ensure the resilience and availability of processing systems, mechanisms to restore access to personal data following technical incidents, and regular risk assessments and testing of security measures.

Equally important is the requirement that organisations periodically review and update security measures to ensure that they remain effective against evolving technological and cybersecurity risks.

The Three Domains of Data Security

The statutory framework established by the NDPA reflects a broader policy understanding that data security operates across three interconnected domains.[20]

The first is preventive security, which imposes an obligation on data controllers and processors to implement safeguards designed to reduce the likelihood of security failures.[21] These safeguards may include vulnerability management, patching protocols, system hardening, and access control measures.

The second domain is incident detection and response.[22] Even well-designed systems may experience security breaches.[23] Organisations must therefore implement mechanisms capable of detecting potential intrusions and responding promptly to contain and mitigate harm.[24]

The third domain is remedial security, which requires

[20] Stewart Room, 'Security of Personal Data' in Eduardo Ustaran (ed), *European Data Protection Law and Practice* (2nd edn, IAPP 2019), pp. 184 - 186.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.

organisations to take corrective steps after incidents occur.[25] These steps may include improving system architecture, strengthening monitoring capabilities, and updating security policies to prevent similar incidents in the future.

The policy foundation for the obligation to process data in a secure manner is grounded in the realities of an increasingly digital economy. As organisations collect, process and store ever larger volumes of information, the value of that data and the systems that hold it has grown significantly. At the same time, cyber threats have become more frequent and more sophisticated. In this environment, the critical issue is no longer whether organisations may face a data breach, but when such incidents may occur and how effectively they are managed.

Recognising the potential harm that data breaches can cause, including risks of identity theft, financial fraud and reputational damage, the NDPA and the General Application and Implementation Directive (GAID) issued by NDPC establish a framework of layered obligations for organisations that control or process personal data. These obligations are intended both to strengthen preventive safeguards against unauthorised access and to ensure that prompt and effective measures are taken to contain harm, notify affected parties and support regulatory oversight when breaches occur.

Legal Requirements for Data Breach Notification

The NDPA establishes clear obligations for data controllers and data processors when a personal data breach occurs. The breach notification framework established under Section 40 of the NDPA creates a structured chain of responsibility designed to ensure that personal data breaches are detected, reported and managed in a timely and transparent manner. The provisions recognise that personal data processing often involves multiple actors, particularly where a data controller engages a third-party service provider to process information on its behalf. In such circumstances, the NDPA places an immediate obligation on the data processor to notify the data controller or the entity that engaged it once the processor becomes aware that a breach affecting personal data has occurred. This notification must include a description of the nature of the breach and, where possible, an indication of the categories and approximate number of data subjects affected as well as the volume of personal data records involved. The processor is also required to cooperate fully with the engaging controller or processor by responding to information requests that may be necessary for the latter to meet its own regulatory obligations.

The NDPA then imposes a direct regulatory reporting duty on the data controller. Where the controller becomes aware of a personal data breach that is likely to pose a risk to the rights and freedoms of individuals, the controller must notify the supervisory authority, the NDPC, within seventy-two hours. The notification must provide sufficient information to allow the NDPC to understand the nature and scale of the incident, including the categories and approximate number of individuals whose data may have been affected and the corresponding volume of personal data records involved. This requirement reflects a broader policy objective of enabling early regulatory oversight so that systemic risks can be assessed promptly and, where necessary, corrective measures or guidance can be issued to limit the spread or impact of the breach.

Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals, the NDPA introduces an additional obligation of direct

[25] Ibid.

communication with the data subjects themselves. In such situations, the data controller must inform affected individuals without undue delay using clear and plain language. The purpose of this communication is not merely to disclose that a breach has occurred, but also to provide practical information that allows individuals to understand the potential consequences and take steps to protect themselves from possible harm. These steps may include monitoring accounts, updating credentials or taking other precautionary measures depending on the nature of the compromised data. The law recognises that in some circumstances direct individual communication may be impracticable, particularly where the number of affected individuals is extremely large or where reliable contact details are unavailable. In such cases, the controller may fulfil the obligation through public communication using widely accessible media channels in order to ensure that affected individuals are reasonably likely to become aware of the incident.

Across all forms of notification and communication required by the NDPA, certain minimum information must be provided to ensure clarity and accountability. The controller must identify a contact point through which additional information may be obtained, describe the likely consequences of the breach, and explain the measures already taken or proposed to address the incident and mitigate its adverse effects. Taken together, these provisions reflect a policy framework that emphasises transparency, timely reporting and coordinated response. By requiring cooperation between processors and controllers, rapid regulatory notification, and meaningful communication with affected individuals, the NDPA seeks to limit the potential harm arising from personal data breaches while strengthening institutional accountability for the protection of personal information.

Whether Notification is Required in This Case

The circumstances surrounding the reported breach strongly suggest that notification obligations would arise. The alleged compromise involves unauthorised access to systems containing personal information relating to employees, corporate officers, and potentially individuals whose financial transactions are processed through government payment infrastructure. Such access creates risks of identity theft, financial fraud, phishing attacks, and reputational harm. Because the breach appears to involve large-scale datasets and sensitive operational systems, it would likely be characterised as presenting a high risk to the rights and freedoms of affected individuals.

Under these conditions, the legal framework would require both regulatory notification to the NDPC and direct notification to affected data subjects.

Adverse Effects of Failing to Notify Data Subjects

Failure to notify affected individuals may generate several adverse consequences.

First, individuals whose contact information has been exposed may become targets for social engineering attacks. Cybercriminals frequently exploit leaked datasets to craft convincing phishing messages designed to extract further information from victims.

Second, financial data exposures may enable fraudulent transactions or identity theft. Early notification allows individuals to monitor their accounts, change credentials, and take preventive measures to protect their financial assets.

Third, delayed or absent notification erodes public trust in digital infrastructure. Citizens expect that institutions entrusted with sensitive information will respond transparently and responsibly when security

incidents occur.

Finally, non-compliance with notification obligations may expose data controllers and processors to regulatory sanctions. The NDPC possesses statutory authority to investigate violations and impose penalties where organisations fail to comply with their legal obligations. Failure to notify affected individuals may generate several adverse consequences.

First, individuals whose contact information has been exposed may become targets for social engineering attacks. Cybercriminals frequently exploit leaked datasets to craft convincing phishing messages designed to extract further information from victims.

Second, financial data exposures may enable fraudulent transactions or identity theft. Early notification allows individuals to monitor their accounts, change credentials, and take preventive measures to protect their financial assets.

Third, delayed or absent notification erodes public trust in digital infrastructure. Citizens expect that institutions entrusted with sensitive information will respond transparently and responsibly when security incidents occur.

Finally, non-compliance with notification obligations may expose data controllers and processors to regulatory sanctions. The NDPC possesses statutory authority to investigate violations and impose penalties where organisations fail to comply with their legal obligations.

Suggested Actions for the Nigeria Data Protection Commission

Given the systemic importance of the institutions involved, the NDPC may consider several regulatory responses.

First, the NDPC should initiate a formal investigation to determine the full scope of the breach. This investigation should assess the technical vulnerabilities that enabled the intrusion and evaluate whether the affected organisations implemented adequate security measures as required under the NDPA.

Second, NDPC should require comprehensive breach notifications from all relevant data controllers and processors involved in the incident. These notifications should clearly identify the categories of data affected, the number of individuals impacted, and the steps being taken to mitigate harm.

Third, NDPC should ensure that affected individuals receive timely and transparent communication regarding the breach, including guidance on protective actions such as password changes, account monitoring, and reporting suspicious activity.

Fourth, NDPC may consider issuing sector-specific cybersecurity guidance for financial institutions and digital payment platforms. Because these systems function as critical national infrastructure, their cybersecurity posture must reflect the highest standards of resilience and risk management.

Finally, NDPC should strengthen inter-agency coordination by working closely with financial regulators, cybersecurity agencies, and law enforcement authorities to enhance national incident response capabilities.

Conclusion

The reported cybersecurity incident involving Sterling Bank, Remita, and data associated with the CAC illustrates the cascading nature of modern cyber risks. A single unpatched vulnerability within one organisation created a pathway through which a threat

actor could access interconnected systems and potentially expose sensitive information relating to millions of individuals.

Available evidence strongly suggests that the compromised datasets contain personal data within the meaning of the NDPA. As a result, the affected organisations are likely subject to clear legal obligations to notify both regulators and affected individuals.

Timely notification is not merely a procedural requirement. It serves as a critical safeguard that enables individuals to protect themselves from the downstream consequences of data exposure. The regulatory response to this incident will therefore serve as an important test of Nigeria's evolving data protection regime. Effective oversight, transparent communication, and strengthened cybersecurity governance will be essential to restoring public confidence in the digital systems that underpin modern governance and financial operations.

Ultimately, this episode underscores a broader policy lesson. Digital infrastructure must increasingly be treated as a strategic critical national asset requiring continuous vigilance, sustained investment, and institutional accountability. In a world where public services, financial systems, and corporate records depend on interconnected technologies, resilience is not optional. It is the foundation upon which trust in the digital economy must be built.

Strengthening that resilience will remain essential if societies are to safeguard their digital lifelines and secure the future of an increasingly connected world.

Chukwuyere Izuogu, LL.M (Hannover), CIPP/E
Partner

chukwuyere@sskohn.com

Favour Osayuwamen
Associate

favour@sskohn.com

STREAMSOWERS & KÖHN is a leading commercial law firm providing legal advisory and advocacy services from its offices in Lagos, Abuja, and Port Harcourt. The firm has extensive experience in acting for Nigerian and international companies, government, and industry regulators in the firm's various areas of practice.

Contact us at:
852b Bishop Aboyade Cole St,
Victoria Island,
Lagos
Tel: +234 1 271 2276; **Fax:** +234 1 271 2277
Email: info@sskohn.com; **Website:** www.sskohn.com