FINTECH COMPANIES IN NIGERIA: DECIPHERING THE ROLES OF DATA CONTROLLERS.

Yunus Adelodun Esq. [317] and O. M. Oyabambi Esq.[318]

ABSTRACT

Undoubtedly, the acceptance of FinTech in Nigeria has served as a catalyst for economic transformation, and a boost to commercial participation and partisanship. Businesses are now seen from a different perspective, inherently paving way for creativity and young entrepreneurship. Statistics show that the Fintech industry raked in $293.2m in the first quarter of 2021, with over 70% percent realized from foreign direct investment, these numbers have even doubled since 2021. The growth of Fintech in Nigeria is capable of placing the Nigerian economy and market at the forefront among other economies in the world. However, in other to achieve this feat, the Fintech industry needs to be appreciated and addressed closely, especially in terms of regulation and roles identification. Data control, processing, and exchange are highlights of the Nigerian fintech industry, there is a need to address the underlying legal issues and caution key players to act 'ex abundanticautela'. The nature of services rendered by these FinTech companies requires access to highly confidential information of customers and effectively triggers data protection regulations. Mismanagement or negligence of this confidential information (including personal data) by the companies is highly detrimental and may result in huge fines or sanctions. This work examines the role of Data Controllers in Fintech companies, especially in terms of regulatory compliance and security. In addressing this, we among others, consider how the breach of personal data could be handled vis-a-vis various relevant applicable extant laws.

[317] LLB, BL Associate, Babalakin& Co. Adelodunyunus@gmail.com
[318] LLB, BL, ACIS, ACIarb Associate, FolashadeAlli& Associates
oyabambioladamola@gmail.com

INTRODUCTION

The Nigerian Fintech market is one of the fastest-growing sub-sectors globally. In 2021, Nigerian Fintech companies and/or startups attracted over US$800 million in funding. This is higher than the entire funding attracted by Nigerian Fintech companies and/or startups in 2018, 2019, and 2020 combined.[319] Also in 2021, three out of the five African new Unicorns[320] are Nigeria companies. Two out of the three are Fintech companies.

The proliferation of Fintech companies and Fintech products is a step in the right direction in attaining financial inclusion and the growth of the Nigerian economy. However, in order for this growth not to falter or result in more harm than good, players in the industry must ensure that regulations are not only in place, but that the regulations are effective and complied with. There are different legal concerns that come to mind when a deep reflection is had on the Fintech industry. For instance, the reputability and volatility of Fintech, platform regulations, multi-jurisdictional nature of Fintech transactions, cybersecurity, and multiple personal data issues- including protection, accessibility, and transfer among others.

The control, processing, use, accessibility, exploration, surveillance and even exchange of personal data by Fintech operators is huge. Fintech operates on the heavy processing of personal and financial data of individuals and corporate entities alike. These data primarily include confidential financial information,

---

[319]EbunoluwaLadipo 'Nigeria's Fintech Landscape in 2021' (*Bussiness Day,* 4 January 2022) https://businessday.ng/technology/article/nigerias-fintech-landscape-in-2021/ accessed 20 October 2022.

[320]

personal choices and other personal and sensitive data of individuals and entities. The legal issues of cybersecurity may arise in event of loss, compromises and cyber-hacking, right breaches issues may also arise in cases of personal data exploration and surveillances. For instance, if a Fintech company gets hacked and its customers' data are compromised or lost, automatically, the customers' finances or even the customers themselves are exposed to danger. The importance of having proper all-round measures in place for the security of user data in a fintech company cannot be overemphasized. The possible and/or necessary discussions around these issues or this field are numerous, however, this article focuses on and emphasizes the duties placed on the data controllers in the event of a personal data breach in Fintech-related transactions.

The common term "Data controller" and "Data Processor", although severally defined is still being confused in the context of Fintech Companies. Hence, the article opens by conceptually clarifying the term 'Data Controller' as differentiated from a 'Data Processor' under the extant data protection regime, particularly within the compass of Fintech. This is followed by an in-depth explanation of what can be termed a personal data breach. Thereafter, the article explains the duties of a data controller in the event of a personal data breach and the consequences therein. What then follows is a discussion of the security requirements stipulated by law to prevent personal data breaches. Finally, the work concludes by delving into the specific data breach and prevention obligations for Fintech companies in Nigeria.

WHO IS A DATA CONTROLLER?

Data controller is simply the individual or company (Corporate person) primarily in charge of personal data. The Data controller determines the collection of personal data and the reason for collection. The data controller also directs the data processor and/or any other person encountering or dealing with the data. Fintech companies and/or startups are data controllers of any personal data that are submitted them or they have direct access to whether in order to process fintech transactions for the data subject or otherwise.

The primary law regulating personal data in Nigeria is the Nigeria Data Protection Regulation, 2019 ("**NDPR**"). By the NDPR, a Data Controller is "*a person who, either alone, jointly with other persons, or in common with other persons or as a statutory body, determines the purposes for and how personal data is processed or is to be processed*". Section 1.3(x) of the NDPR.[321] This definition is *in pari material* with the definition of data controller under the EU General Data Protection Regulation (GDPR).

According to Article 4 (7) of the GDPR[322], a data controller is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State Law, the controller or the specific criteria for its nomination may be provided for by the Union or Member State Law*".

[321] Nigeria Data Protection Regulations 2019, s 1.3 (x)
[322] The GDPR is the legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

There is a fine line between a data controller and a data processor. While a Data Controller determines the purposes and means of processing personal data, a Data Processor engages in personal data processing on behalf of the controller by carrying out operations such as collection, structuring, storage, use, etc. Hence, in the Fintech setting, the Company and/or startup is usually the data controller, while the officer in charge of processing, transferring or using the data can be designated as the Data Processor. The term “Data Processor” is often used interchangeably with “Data Administrator”. The Fintech company may in some cases qualify as both the data controller and data processor. According to Article 1.3(ix) NDPR " 'Data Administrator' means *a person or an organisation that processes data*". In any event, what determines the designation of an individual or entity as either a Data Controller or Data Processor are factual accounts underlying such designation.

Thus, the significant difference between a data controller and a data processor is that the data controller gives instructions to the data processor to process personal data. Therefore, the processor cannot process personal data unless acting on the controller’s instructions, otherwise, the processor will become the controller.

Hence, as shown above, in FinTech companies, the company itself is usually the data controller (for third parties, commercial counterparties, customers and employees)). In unusual events, the fintech companies may be a data processor. For instance, if the personal data is submitted to Fintech company by a third party who specifies the purpose for which the data is used and the Fintech Company is only responsible for processing the data.

WHAT IS A PERSONAL DATA BREACH?

The only form of data protected from breaches by the NDPR is personal data. There are different kinds of data that cannot be breached by disclosure, such as public information or other information that the Nigerian populace is entitled to under the Freedom of Information Act.

Article 1.3 (xix) of the NDPR defines personal data as any information relating to an identified or identifiable natural person. It further defines an "identifiable natural person" as one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Subsequently, Article 1.3 (xxii) of the NDPR defines a personal data breach as "*a security breach, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed*". This security breach includes breaches that are a result of both accidental and deliberate causes. It also implies that a personal breach is more than just losing personal data; it could involve the access of personal data by an unauthorized third party or sending personal data to an incorrect recipient and other similar acts.

Broadly speaking, a personal data breach is a security incident that has affected personal data confidentiality, integrity, or availability. Some of the laws that may regulate personal data breach in the Nigerian Fintech industry include; the Constitution of the Federal Republic of Nigeria, the NDPR, the Cybercrime

(Prohibition, Prevention, etc) Act 2015, Advanced Fee Fraud and Other Fraud Related Offences Act 2006, CBN's Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Policy and Procedure Manual, CBN's Consumer Protection Framework, The Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018 and the Consumer Code of Practice Regulations, 2007.

Nigeria Information Technology Development Agency (NITDA) was established by the NITDA Act 2007 to oversee and regulate information technology development- this includes data protection- as accentuated by the NDPR. In recent times, the Nigeria Data Protection Bureau (NDPB) was also established to be responsible for enforcing the NDPR in Nigeria. Although no legislation yet exists to delineate the regulatory contours of the NDPB. Before 2022, NITDA was the only existing data protection enforcement authority. However, on February 4, 2022, President Muhammadu Buhari announced the establishment of the NDPB, a dedicated data protection agency for Nigeria. The Bureau will be in charge of consolidating the NDPR's gains and assisting in the development of primary legislation for data protection and privacy.

It can be said that the NDPB, and not the NITDA, will be in charge of the enforcement of data protection laws and the administration of all related data protection matters in Nigeria, even though the scope of the Bureau's regulatory powers and responsibilities within the sphere of data privacy and protection in Nigeria is still unclear. The NDPB will therefore operate within the current legislative framework, which consists of the NDPR and the Institutional

Framework of the NDPR until the substantive data protection regulation is passed.[323]

SECURITY REQUIREMENTS TO PREVENT PERSONAL DATA BREACH

The best way to begin the prevention of the nightmare and cost of personal data breaches is by understanding them. According to the 2022 cost of data breach report by International Business Machines Corporation (IBM), the consolidated average global cost of a data breach reached $4.35 million, amounting to a 12.7% increase from the preceding year, and also the highest ever noted across the history of IBM reports.[324] This is in addition to incalculable damage to the organization's reputation.

The NDPR, in furtherance of its objective to mitigate data breaches, has provided some security requirements for avoiding personal data breaches. These security requirements apply to all the data controllers and data processors within the scope of the regulation.

Article 3.2 (v) of the NDPR provides that data controllers must continuously improve their information security architecture to prevent possible data breaches. In the same light, Article 2.6 of the NDPR provides that anyone involved in data processing or personal data control must develop security measures to protect it.

---

[323]Jumoke Lambo, ChisomOkolie 'Data Protection Laws and Regulations Nigeria 2022' (*ICLG,* 8 July 2022) https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria accessed 20 October 2022.

[324]DilkiRathnayake 'Key Points from the IBM Cost of a Data Breach Report 2022' (*Tripwire,* 28 August 2022) https://www.tripwire.com/state-of-security/key-points-ibm-cost-data-breach-report#:~:text=The%202022%20report%20records%20the,the%20history%20of%20IBM%20reports. accessed 20 October 2022.

These measures include protecting systems from hackers, setting up firewalls, storing data securely with access to specifically authorized individuals, employing data encryption technologies, developing organizational policy for handling Personal Data (and other sensitive or confidential data), protecting emailing systems, and continuous capacity building for staff.

The audit template provided in the NDPR-IF also indicates that a data controller must also have the following:

i. An adequate information security system that includes physical, logical, technical, and operational measures that ensure the security of the processing of personal data;[325]
ii. A register of data breaches and security incidents;[326]
iii. An information security standard and implement the same;[327]
iv. Methods for data pseudonymization, anonymization, and encryption which are applied to reduce exposure of personal data.[328]

As well, in compliance with Article 12.3 of the NDPR-IF, organizations who are third-party data processors must process data only based on authorization expressly granted by the data controller through a written agreement that specifies the roles and obligations of each party concerning data protection and also ensures that there are adequate information security measures to protect the personal data being processed.

[325] Nigeria Data Protection Regulations 2019; Implementation Framework, Item 4.23 Annexure A
[326] Nigeria Data Protection Regulations 2019; Implementation Framework, Item 3.5 Annexure A
[327] Nigeria Data Protection Regulations 2019; Implementation Framework, Item 1.3 Annexure A
[328] Nigeria Data Protection Regulations 2019; Implementation Framework,Item 4.3 Annexure A

Other measures that are germane for Fintech companies for the protection of personal data breach include; (a) development and display of privacy policy, (b) design of a data protection compliance system, (c) appointment of a data protection officer, (c) development of continuous capacity check of the data protection officer, (d) conduct of data protection impact assessment and (e) airtight agreement with third party processors, among others.

THE DUTIES OF A DATA CONTROLLER IN THE EVENT OF A PERSONAL DATA BREACH

Generally, a data controller is obligated to implement the appropriate data protection policies and suitable technical and organizational measures to ensure and be able to demonstrate that the processing is done by the NDPR. Controllers are also expected to keep records of their processing activities. Therefore, when preparing a new processing activity, they must consider the appropriate legal grounds for its lawful processing.

However, in the event of a data breach, the two most important duties of a data controller are notification. The required notification here is to be made firstly to the regulator and subsequently, communicated to the affected individual or data subject. By Regulations 3.2(ix) and 9.2 of the NDPR-IF, data controllers and processors are duty-bound to notify the National Information Technology Development Agency ("NITDA") of personal data breaches within 72 (seventy-two) hours of becoming aware of the breach.

Data controllers are also mandated to notify the data subject immediately of any breach which poses a high risk to the freedom or rights of the data subject.

However, the authors of this work note that the criteria for assessing what amounts to high risks to the freedoms and rights of the data subjects are not stated in the NDPR-IF. Both the NDPR-IF and the GDPR provide that a data controller must notify the data subject and the supervisory authority of a personal data breach that will likely result in high risks to the freedoms and rights of the data subject.

We have thus considered below, the Nigerian notification provisions against that of the GDPR which is the global benchmark for data protection. The critical differences between the NDPR-IF and GDPR regarding personal data breach notification are hereby highlighted as follows:

1. While Article 9.4 of the NDPR-IF provides that the notification must be "immediately" made to the data subject, Article 34 (1) of GDPR provides that the notification should be made "without undue delay". This allows data controllers under the GDPR to fetter some discretion in interpreting what qualifies as "undue delay". In Nigeria, the notification must be immediate.
2. Article 34(3) (a) of the GDPR provides for circumstances under which a data controller would not be mandated to notify a data subject of a personal data breach.[329] However, the NDPR-IF provides that data

[329] Such as (a) where the data controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize; (c) it would involve disproportionate effort.

controllers should make the notification to the data subject without providing for any case exceptions.

3. Article 33(1) of the GDPR provides that where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This allows data controllers to report personal data breaches outside 72 hours where it can provide justifiable reasons for the delay. However, the NDPR does not provide a justifiable basis for data controllers who report personal data breaches after 72 hours of becoming aware of such a breach.

Article 9.2 of the NDPR-IF also provides that notification of personal data breach made to NITDA must include the following information:

i. A description of the circumstances of the loss or unauthorized access or disclosure.
ii. The date or period during which the loss or unauthorized access or disclosure occurred.
iii. A description of the personal information involved in the loss or unauthorized access or disclosure.
iv. An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure.
v. An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure.
vi. A description of steps the organization has taken to reduce the risk of harm to individuals.

vii. A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure and lastly;

viii. The name and contact information of a person who can answer, on behalf of the organization, NITDA's questions about the loss of unauthorized access or disclosure.

Lastly, it is important to note that Article 10.1.2 of the NDPR-IF also provides that any person who believes a party is not complying with any of the provisions of the NDPR may file a complaint with NITDA in writing and describe the acts or omissions believed to violate the applicable provision.

THE CONSEQUENCES OF THE FAILURE TO REPORT A BREACH OF PERSONAL DATA

Where a data controller fails to make the required notification of a personal data breach under the relevant laws, such a failure would expose the controller to the general responsibilities and penalties as provided below.

Section 18 of the NITDA Act provides that where a person or body corporate fails to comply with the regulations, standards, guidelines, frameworks, circulars, directives, or any subsidiary legislation issued by the NITDA in the discharge of its duties, such person or body corporate commits an offense and is liable on conviction (in the case of a body corporate) to a fine of not less than N200, 000.00 (for a first offense) or N500, 000 (for subsequent offenses). As an alternative to a fine, offending entities upon conviction are liable to

imprisonment for the principal officers[330] for a term of not less than 2 years or both.

Therefore, failing to notify a personal data breach to NITDA and/or individuals as prescribed by the NDPR-IF is a breach of the NDPR-IF which is a NITDA regulation and will expose a contravening corporate entity to the penalty provisions contained in the NITDA Act.

Furthermore, Article 10.1.4 of the NDPR-IF provides that as an administrative sanction, NITDA may issue an order for compliance with relevant provisions to curtail further breach where it finds an entity in contravention of the provisions of the NDPR. It further states that NITDA or a court of competent jurisdiction may prescribe additional sanctions in liquidated monetary sum.

SPECIFIC DATA BREACH OBLIGATIONS FOR FINTECH COMPANIES

It must be noted that the provisions of the NDPR-IF and the other laws espoused above apply to all companies, including Fintech companies in Nigeria. However, for Fintech companies, there are additional specific data breach obligations given the sensitivity of data shared with the companies and the delicacy of fintech companies that must comply with and they are contained in various laws and regulations outlined below:

[330] Principal Officers may only escape liability if they can demonstrate that the act or omission constituting the offence took place without their knowledge, consent or connivance.

1. Section 19 (3) of the Cyber-crimes (Prohibition, Prevention, etc.) Act (CCPPA) provides those financial institutions[331]re expected to implement effective counter-fraud measures to safeguard customers-sensitive information. Customer-sensitive information referred to in the CCPPA is majorly made of the personal data of customers.
2. Article 5.4 of the Central Bank of Nigeria ("CBN") Consumer Protection Regulations mandate institutions licensed with the CBN to protect the privacy and confidentiality of consumer information and assets against unauthorized access. It also provides that institutions will be held accountable for acts or omissions concerning the privacy of consumer information.
3. Article 6 c (i) of the CBN Risk-Based Cyber-security Framework and Guidelines for Deposit Money Banks and Payment Service Providers (Cyber-security framework) mandates designated money banks and payment service providers to ensure that no vendor has unfettered access to its systems, database, network, and applications.
4. Article 3.14 of the Guidelines on Card Issuance and Usage in Nigeria ("Card Issuance Guidelines") recommends that CBN-licensed issuers of payment cards should continuously educate cardholders on security tips

[331] The definition of financial institutions can be derived from Section 131 of the Bank and Other Financial Institution Act, 2020 to mean "any individual, body, association or group of persons; whether corporate or unincorporated, other than the banks licensed under this Act which carries on the business of a discount house finance company and money brokerage and whose principal object include factoring, project financing, equipment leasing, debt administration, fund management, private ledger services, investment management, local purchases order financing, export finance, project consultancy, financial consultancy, pension fund management and such other business as the Bank may from time to time designate."

for safeguarding cardholder information. In addition, Article 3.21 of that same guidelines provides that the security of the payment card shall be the responsibility of the issuer and the losses incurred on account of a breach of security or failure of the security mechanism shall be borne by the issuer unless the cardholder is found liable.

With regards to notification requirements in the event of a personal data breach, Fintech companies must take note of the following;

1. Under the Cybercrime Act, the company must immediately (but no less than 7 days) inform the National Computer Emergency Response Team (CERT) Coordination Center of any attacks, intrusions, and other disruptions liable to hinder the functioning of another computer system or network. The notification must contain the details of any attacks, intrusions, and other disruptions liable to hinder the functioning of another computer system or network.
2. Under the Cyber-security Framework, the company must report all cyber-incidents (whether successful or unsuccessful) not later than 24 hours after the such incident is detected to the director of banking supervision, CBN.
3. Under the Card Issuance Guidelines,[332] where the company is a licensed issuer of payment cards, the company must make statutory returns at the end of every month, and not later than the 10th day of the following month. This report must include any incidents of fraud, theft, or robbery

[332] Central Bank of Nigeria, "Guidelines for Card Issuance and Usage in Nigeria": https://www.cbn.gov.ng/out/2014/bpsd/approved%20guidelines%20for%20card%20issuance%20and%20usage%20in%20nigeria%20.pdf.

on cards, card data, and reports of foreign exchange remitted to international card schemes and international acquirers.

Finally, it is also essential to understand that notification should be made in all instances where the law requires notification. Regardless of the volume or risk, once an event satisfies the requirement for notification, the relevant authorities must be notified.

CONCLUSION

There are several nuances around the regulation of both Fintech and personal data, however this research has been able to effectively discuss the regulation of Fintech companies and especially the obligations of data controllers towards preventing personal data breaches in the course of Fintech transactions. It was discovered that the most important obligation, after curbing the breach is that of notifying the regulatory authority and the affected individuals and that failure to make this notification could attract serious sanctions that may extend to terms of imprisonment for the principal officers of the company. To prevent occurrences of personal data breaches of data subjects, Fintech companies should conform with the regulation of the NDPR[333] and the NDPB[334] that mandates Data Controllers to appoint a Data Protection Officer (DPO) to ensure adherence to the NDPR and other relevant data privacy and protection legislation.

[333] Nigeria Data Protection Regulations 2019, s 4.1
[334] Nigeria Data Protection Regulations 2019; Implementation Framework, s 3.4.1