KENNA

Open Banking, Closed Courts?

Liability and Dispute Dynamics in Nigeria's API Ecosystem

Technology, Media & Telecommunications Insight

September 2026

Pioneer framework, lagging liability...

Open Banking refers to a framework that allows for the secure sharing of financial information through an Application Programming Interface (API), among authorised third-party developers.[1]

Nigeria can be credited as one of the earliest African countries to formally regulate open banking through a central bank-driven framework and API standards as opposed to relying solely on industry-led initiatives.[2] The regulatory journey formally commenced with the issuance of the Central Bank of Nigeria (CBN) Regulatory Framework for Open Banking in Nigeria in February 2021, which established the foundational principles, participant categorizations and API risk tiers.[3] This was subsequently operationalised through the CBN's Operational Guidelines for Open Banking in Nigeria 2023 (CBN Guidelines) which provide a firm foundation for participation, data governance and technical interoperability within an emerging ecosystem.[4]

This article examines emerging liability hotspots within Nigeria's open banking ecosystem, focusing on contractual privity in multi-party API relationships, responsibility for data breaches, and the adequacy of the existing dispute resolution mechanisms. It argues that while Nigeria has established a functional regulatory architecture for open banking, the liability and dispute resolution architecture remains underdeveloped, which leaves significant uncertainty and risks for banks, FinTech firms and end-users alike.

Regulatory Anchor

2021

CBN Regulatory Framework for Open Banking issued

Operational Spine

2023

CBN Operational Guidelines for Open Banking take effect

Article Scope

Three

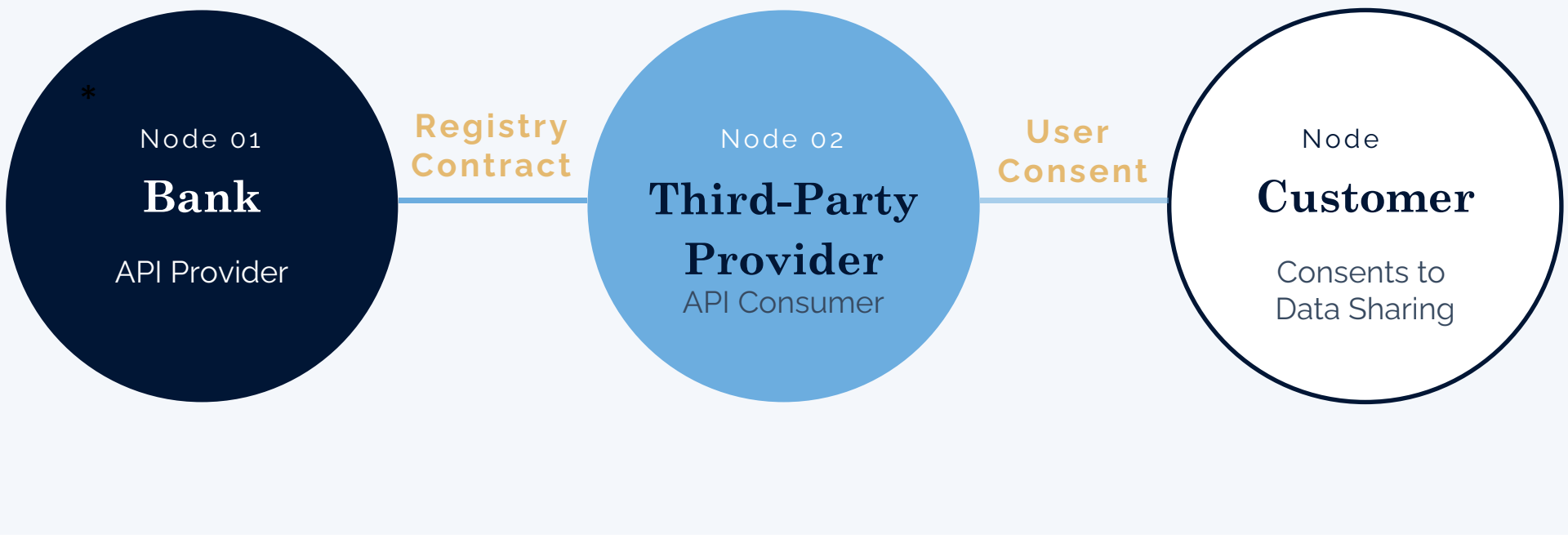
Liability hotspots examined across the API ecosystem

Contractual Privity in a Multi-Party API Ecosystem

In a multi-party API system in Open Banking, privity of contract works as a tripartite relationship between the bank (financial institution or API Provider), the third-party service provider (the API Consumer) and the user (the Customer).

The user must consent before any third-party data sharing can be done by the bank, and any third party data processing or control can be done by the third-party service provider. The bank and third-party service provider are limited to the extent of the consent given by the user and have a duty to process the user's data in accordance with the Nigeria Data Protection Act.[6]

For the bank and the third-party service provider, the contract is grounded in the ordinary principles of contract and contractual privity. The CBN Guidelines require both parties to be registered on the open banking Registry. They must also comply with defined responsibilities, including access rules, security standards, data ethics obligations, and consent management requirements.[7] The contract must clearly define each party's obligations, permitted data uses, liability for breach, and termination rights, ensuring enforceable accountability while upholding customer permissioned data -sharing.[8]



Data Breach Incidents: Responsibilities of The Parties and Possible Defences

Under the CBN Guidelines, the bank and third-party service provider have a duty to implement measures to prevent a data breach. They are also mandated to develop a data breach policy.[9] Where a breach occurs, the responsible parties (which can be either the bank or the third party service provider or both) must rely on their established data breach- policy to deal with the breach. The CBN Guidelines provide that such policy must be one that emphasises prevention, preparedness, structured assessment, and procedure to contain the breach. A data breach incident must also be promptly communicated to all relevant parties including the CBN, with a subsequent review to ascertain the underlying cause of the incident. The responsible party(ies) must promptly contain the incident, communicate with relevant parties, analyse root causes, and implement corrective measures. The bank and third-party provider must also ensure that there is strict adherence to the policy in the event of a data breach.

Step 01
Prevention
Implement measures & shape the policy.

Step 02
Containment
Promptly contain the incident.

Step 03
Notification
Communicate with the CBN & parties.

Step 04
Review
Root cause & corrective measures.

A data breach lawsuit would most likely be an action in tort based on the failure of the responsible party to protect the customer's data.[10] In the event of a data breach suit, the bank and third party may rely on the following possible defences depending on the nature of the suit:

- **Compliance with regulatory standards:** The Responsible party may raise the defence and tender evidence that it complied with the relevant legislations such as the Central Bank of Nigeria Open Banking Guidelines, 2023, and the Nigeria Data Protection Act, 2023.[11]
- **Third-Party Liability:** The bank can raise the defence that the data breach was caused by the third-party service provider.
- **Customer negligence:** The responsible party may raise the defence that customer negligence or carelessness with their data led to the data breach. The bank may also raise the defence of contributory negligence.
- **Force majeure:** An example of a force majeure is a sophisticated cybersecurity attack that bypassed industry-standard security measures.[12]

Dispute Resolution Mechanisms: Arbitration Clauses cs. CBN's Complaint Channels

Under the CBN Operational Guidelines for Open Banking 2023, participants are mandated to incorporate formal dispute resolution procedures within their bilateral Service Level Agreemnents (SLAs),[13] alongside providing clear complaint channels for end-users. In practice, banks and FinTechs routinely insert private arbitration clauses into these commercial SLAs, favouring arbitration for its confidentiality, speed and technical expertise. While arbitration provides an efficient bilateral forum, its utility across the broader Open Banking ecosystem is constrained by fundamental legal limitations.

First, end-users are not parties to inter-institutional SLAs and are therefore not bound by, nor can they benefit from arbitration clauses contained within bank-FinTech agreements under the doctrine of contractual privity.[14] Secondly, API chains involve multiple distinct actors – banks, API aggregators, middleware providers and consumer facing FinTechs – operating under separate contractual frameworks. Despite the procedural mechanisms for joinder and consolidation introduced under Sections 39 and 40 of the Arbitration and Mediation Act 2023, arbitrating multi-party API failures across disconnected agreements remains procedurally complex. This is because joinder and consolidation generally still require consent or proof that all entities are bound by the same underlying arbitration agreement.[15]

Importantly, the CBN Guidelines do not prescribe litigation, nor could any regulatory guidelines override the constitutional jurisdiction of Nigerian courts to adjudicate civil rights and commercial obligations[16]. Litigation remains fully available to aggrieved institutional participants and consumers. However, traditional court litigation presents significant practical drawbacks in API disputes. Public court records risk exposing sensitive software architecture or operational vulnerabilities, while formal judicial proceedings are often ill-equipped for the rapid technical remediation required in automated financial rails.

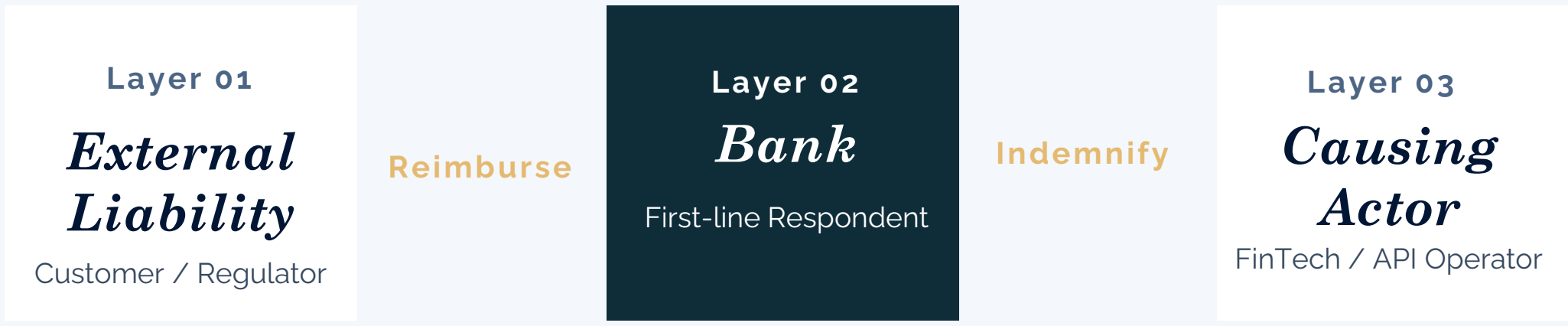
As an alternative to private arbitration and court litigation, the CBN framework mandates internal grievance procedures and permits unresolved customer disputes to be escalated to the CBN Consumer Protection Department.[17] However, while the Consumer Protection Department provides essential administrative oversight and consumer redress, its supervisory role is not designed to function as an adjudicatory court or arbitral tribunal capable of determining complex contractual damages, allocating multi-party tortious liability or enforcing cross-indemnities between institutional actors.

Indemnity Clauses and Risk Redistribution

Open Banking transactions involve multiple parties - banks, FinTechs, API providers, infrastructure partners, and customers — often operating under separate but interconnected contracts.

Indemnity clauses therefore serve as a redistributor, allowing a party that is externally liable — whether to a customer or regulator — to shift financial responsibility internally to the actor whose conduct caused the loss. For example, where a bank reimburses a customer for an unauthorised debit traceable to a FinTech's compromised API integration, the bank may rely on contractual indemnification to recover that loss.

Under Nigerian contract law, indemnity clauses are generally enforceable where clearly drafted and not contrary to public policy. However, courts interpret such provisions strictly. At the same time, overly expansive indemnities bear the risk of creating imbalance within the open banking ecosystem. Smaller FinTech participants may face disproportionate exposure, especially where losses stem from systemic or shared infrastructure failures beyond their exclusive control. The drafting challenge therefore lies in balancing effective risk allocation with commercial sustainability.



Limitation of Liability and Exposure Management

While indemnities redistribute loss, limitation clauses define its outer boundary; typically limit aggregate liability, exclude indirect or consequential losses, and carve out exceptions for fraud, willful misconduct, or gross negligence. Such clauses cannot ordinarily exclude liability for fraud or deliberate wrongdoing, and their enforceability depends on clarity and proper incorporation.

However, tension arises where liability stems from statutory breach. The Nigeria Data Protection Act 2023 imposes mandatory obligations on data controllers and processors, and regulatory fines imposed for statutory non-compliance may not be easily neutralized through contractual limitation. Thus, while parties may allocate financial responsibility amongst one another, they cannot avoid regulatory accountability through their contracts. This distinction becomes particularly significant in disputes involving data breaches or systemic API failures.

Conclusion

Nigeria's pioneer adoption of Open Banking under the regulatory stewardship of the CBN has established a commendable framework for financial solid regulatory and technical foundation for data sharing and FinTech innovation.[18] However, as this article has demonstrated, a significant divergence remains between Nigeria's advanced technical architecture and its legal and dispute resolution framework, the core vulnerabilities identified across this article include – the doctrine of contractual privity in multi-party API chains, the complex allocation of tortious liability during data breaches and the procedural limitations of existing dispute channels – reveal an ecosystem where systemic risks are easily shifted rather than effectively managed.

Left unaddressed, these structural gaps threaten to undermine institutional trust and slow the commercial adoption of open banking. Bridging this divide requires aligning private commercial arrangements with broader public regulatory objectives through a multi-pronged legal approach. Firstly, the CBN should issue supplemental regulatory guidance that explicitly defines statutory default rules for liability allocation and indemnification in common multi-party scenarios. Secondly, industry stakeholders must move away from fragmented bilateral dispute mechanisms toward a dedicated, institionalised Open Banking Dispute Resolution Panel capable of adjudicating complex, multi-party API claims.[19] Finally, enhancing judicial familiarity with financial technology and data protection law through specialized judicial training will ensure that when open banking disputes reach court, judicial outcomes are technically sound and commercially sustainable.[20]

The clause governs loss between parties — it cannot govern accountability before the regulator.

Contributors



Okechukwu Ekweanya

Partner, TMT



Nnaedozie Ajogwu

Associate, TMT



Victory Uhunmwangho

Associate, TMT

For further information on the issues discussed in this article, contact our legal team at counsel@kennalp.com

Endnotes

1. Open Banking Nigeria, 'Frequently Asked Questions' < FAQs - Open Banking Nigeria > accessed 13 February 2026; G. O. Ojo & A. I. Okoh, FinTech and the Regulatory Landscape in Nigeria (2022) 14(2) Journal of African Law & Technology, p. 45.
2. Central Bank of Nigeria, Operational Guidelines for Open Banking in Nigeria (Circular PSM/DIR/PUB/CIR/001/043, 7 March 2023) https://www.cbn.gov.ng/out/2023/ccd/operational%20guidelines%20for%20open%20banking%20in%20nigeria.pdf accessed 28 July 2026.
3. Central Bank of Nigeria, Regulatory Framework for Open Banking in Nigeria (Circular BSD/DIR/GEN/LAB/14/008, 17 February 2021) https://www.cbn.gov.ng/out/2021/ccd/regulatory%20framework%20for%20open%20banking%20in%20nigeria.pdf accessed 28 July 2026.
4. Central Bank of Nigeria Operational Guidelines for Open Banking in Nigeria 2023
5. Central Bank of Nigeria Operational Guidelines for Open Banking in Nigeria 2023, Section 7.0; Central Bank of Nigeria Operational Guidelines for Open Banking in Nigeria 2023, Appendix 3.2(i)
6. Nigeria Data Protection Act 2023, Section 26; Nigeria Data Protection Act 2023, Section 29
7. Central Bank of Nigeria Operational Guidelines for Open Banking in Nigeria 2023, Section 6.0
8. Suzanne Gainey, 'APIs & Data Sharing', (Association of Corporate Counsel, 15 February 2024) <https://www.acc.com/sites/default/files/program-materials/upload/APIs%20%26%20Data%20Sharing%20%28February%202024%29%20-%20ACC%20Charlotte.pdf > accessed on 13 February 2026
9. Central Bank of Nigeria Operational Guidelines for Open Banking in Nigeria 2023, Section 9.3.3
10. Vincent R. Johnson, 'Data Security and Tort Liability' (2008), 11 J. Internet L.22
11. <https://commons.stmarytx.edu/facarticles/467/ > accessed 10 February 2026
12. Bernard Bell, 'A Regulatory Compliance Defense for Data Breach Actions' (Yale Journal on Regulation, 6 December 2028) <https://www.yalejreg.com/nc/a-regulatory-compliance-defense-for-data-breach-actions/ > accessed 13 February 2026;
13. Haafiz Suleman and Kate Scott, 'Data Litigation: A Toolkit for Defendants' (Clifford Chance, October 2020) <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/data-litigation-a-toolkit-for-defendants.pdf > accessed 12 February 2026
14. Peter Lumley-Savile and Sanjay Pritam, 'Force Majure and Cloud Computing Contracts', (Lexology, 6 November 2012) <https://www.lexology.com/library/detail.aspx?g=70004d0e-6d81-4e55-b3e3-1f8484ab858b > accessed 12 February 2026
15. Central Bank of Nigeria, Operational Guidelines for Open Banking in Nigeria (Circular PSM/DIR/PUB/CIR/001/043, 7 March 2023) ss 8.1.2, 12.0 and App IV https://www.cbn.gov.ng/out/2023/ccd/operational%20guidelines%20for%20open%20banking%20in%20nigeria.pdf accessed 29 July 2026.
16. Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd [1915] AC 847 (HL); see also Reptico SA Geneva v Afribank (Nig) Plc (2013) 14 NWLR (Pt 1373) 172 (SC).
17. Arbitration and Mediation Act 2023, ss 39–40
18. Constitution of the Federal Republic of Nigeria 1999 (as amended), s 6(6)(b).
19. Central Bank of Nigeria, Consumer Protection Regulations 2019, reg 6.3.
20. Central Bank of Nigeria, Operational Guidelines for Open Banking in Nigeria (Circular PSM/DIR/PUB/CIR/001/043, 7 March 2023
21. Open Banking Limited, Dispute Management System Code of Best Practice: Principles and Best Practice Standards (OBIE 2028) https://www.openbanking.org.uk/wp-content/uploads/Dispute-Management-System-Code-of-Best-Practice.pdf accessed 29 July 2026.
22. Constitution of the Federal Republic of Nigeria 1999 (as amended), s 6(6)(b); Nigeria Data Protection Act 2023, s 51 (jurisdiction of courts over data protection breaches).



CONTACT

LAGOS
Kenna Place
8, Ogunyemi Road, Palace Way, Oniru PO Box 73002, Victoria Island,
Lagos

ABUJA
1st Floor, Novare Central,
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285,
Abuja

ENUGU
Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner, 400211
Enugu State.

+234 811 395 1052, +234 811 395 1053 | counsel@kennalp.com | www.kennalp.com