Legal 500
Country Comparative Guides 2025

Nigeria
Fintech

Contributor

Duale, Ovia & Alex-Adedipe

Adeleke Alex-Adedipe

Managing Partner | a.alex-adedipe@doa-law.com

Chika Oke

Senior Associate | c.oke@doa-law.com

Christiana Ossai

Associate | c.ossai@doa-law.com

Abdulrasheed Badmus

Associate | a.badmus@doa-law.com

Bankole Oke

Associate | b.oke@doa-law.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in Nigeria.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Nigeria: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

In Nigeria, the regulation of fintech companies is multi-faceted, involving several key agencies responsible for overseeing specific aspects of the sector:

- Central Bank of Nigeria (CBN): The Central Bank of Nigeria (CBN) is the primary regulator of the financial sector, overseeing fintech companies that engage in payments, digital banking, and remittance services. It issues various licenses such asPayment Service Provider (PSP) licenses, Mobile Money Operator (MMO) licenses, and Payment Service Bank (PSB) licenses. The CBN has also introduced frameworks such as the Regulatory Sandbox Operations Framework to encourage innovation while maintaining financial system stability. Through its guidelines, the CBN ensures compliance with financial regulations while supporting fintech growth and fostering financial inclusion.
- Securities and Exchange Commission (SEC): The Securities and Exchange Commission (SEC) is responsible for regulating fintech companies involved in securities and investment-related activities. This includes crowdfunding platforms, digital investment schemes, and tokenized securities. Under the Crowdfunding Regulations 2021, the SEC ensures that platforms adhere to transparency and disclosure requirements, safeguarding investors and fostering market integrity. Fintech firms dealing in crypto assets classified as securities are also subject to SEC oversight, ensuring compliance with Nigeria's securities laws.
- National Data Protection Commission (NDPC): The National Data Protection Commission (NDPC), established under the Nigeria Data Protection Act 2023, oversees data privacy and protection in Nigeria. Fintech companies that process personal data are required to comply with NDPC guidelines, including obtaining lawful consent, limiting data collection to necessary information, and implementing robust security measures. The NDPC plays a crucial role in aligning Nigeria's data protection standards with global best practices, ensuring the secure handling of customer information by fintech companies
- National Information Technology Development Agency (NITDA): The National Information Technology Development Agency (NITDA) continues to play a critical role in fostering digital innovation in Nigeria. While oversight of data protection has transitioned to the NDPC, NITDA enforces IT standards and cybersecurity guidelines. It provides regulatory frameworks that guide fintechs on implementing secure IT infrastructure, ensuring operational reliability and compliance with national and international cybersecurity requirements.
- Nigerian Communications Commission (NCC): The Nigerian Communications Commission (NCC) regulates the telecommunications infrastructure that underpins fintech operations in Nigeria. This includes USSD services, SMS-based payment platforms, and mobile network reliability. By ensuring seamless integration between telecom and fintech services, the NCC promotes efficient operations while protecting consumers from telecom-enabled financial fraud. Its regulations are integral to creating a secure and interoperable financial ecosystem.
- Federal Competition and Consumer Protection Commission (FCCPC): The Federal Competition and Consumer Protection Commission (FCCPC) focuses on safeguarding consumer interests and promoting fair competition within the fintech industry. The FCCPC ensures that fintech companies provide clear and accurate information about their products and services, resolve consumer complaints effectively, and avoid anti-competitive practices. Its oversight fosters consumer trust and supports a balanced competitive environment for fintech operators.
- Corporate Affairs Commission (CAC): The Corporate Affairs Commission (CAC) oversees the incorporation and registration of fintech companies in Nigeria. Registration with the CAC is a prerequisite for obtaining licenses from other regulatory bodies. It ensures that fintech companies comply with Nigeria's corporate laws and maintain proper governance structures, thereby providing a solid legal foundation for their operations.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

The fintech sector in Nigeria is on a robust growth trajectory, with numerous opportunities for expansion. However, like any rapidly evolving industry, there are a few challenges that may shape the growth of fintech in the short and medium term.

- Enhanced Regulatory Clarity: One such challenge is the need for enhanced regulatory clarity in areas such as cryptocurrency and blockchain technologies. While the Central Bank of Nigeria (CBN) has made strides in regulating digital financial services, further clarity and alignment on regulations governing fintech services, particularly in the blockchain and cryptocurrency space, will support greater investor confidence and foster a more innovative environment.
- Cybersecurity Concers: Cybersecurity concerns are an area of focus for fintechs, especially as they handle sensitive financial data. Proactively addressing these through robust security protocols will ensure long-term stability and consumer trust.
- Infrastructure Development: Infrastructure development is another key area for improvement. The ongoing expansion of digital payment networks and mobile penetration is expected to drive fintech growth in underserved regions, but continued investment in reliable internet connectivity and power supply remains essential.

While these factors present challenges, they also offer significant opportunities for fintech companies to develop solutions that address these needs and further accelerate market growth.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

Yes, fintech companies in Nigeria must obtain licenses or registrations specific to their operational activities. This regulatory approach promotes transparency, consumer protection, and financial system stability. Examples of licensing requirements include:

- Payment Service Licenses: Issued by the Central Bank of Nigeria (CBN), these licenses are categorized based on the scope of activities, such as Payment Service Banks (PSBs), Mobile Money Operators (MMOs), and Switching and Processing licenses.
- Crowdfunding Intermediary Licenses: Regulated by the SEC under the Crowdfunding Regulations 2021, these licenses enable fintech platforms to facilitate equity or debt-based crowdfunding.
- Data Protection Compliance: Companies must register with the NDPC and comply with its guidelines, if they process personal data, ensuring compliance with Nigeria's data protection laws.
- Other sectors, such as blockchain and cryptocurrency businesses, may require additional regulatory approvals or compliance with specific laws, especially as new frameworks are developed.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

A Regulatory Sandbox is a controlled environment set up by regulators, allowing fintech companies to test innovative products, services, and business models with fewer regulatory restrictions.

In Nigeria, the CBN and SEC established regulatory sandboxs to support the growth of fintech startups. It enables firms to pilot their solutions without full regulatory compliance in exchange for regular reporting and oversight. This initiative helps mitigate regulatory risks while allowing fintechs to gain valuable feedback on their products before full-scale market entry.

The sandbox provides an opportunity for fintech startups to innovate in the financial services sector, refine their offerings, and build investor confidence.

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

In Nigeria, crypto assets may be classified as securities if they meet certain characteristics, according to the Securities and Exchange Commission (SEC). ICOs, which involve the sale of tokens to raise funds, fall under the purview of these securities laws.

The law that governs securities and investments in Nigeria is the Investment and Securities Act 2007 (“ISA”) and the Rules and Regulations of the Security and Exchange Commission 2013 as amended from time to time. Section 315 of ISA defines securities to mean (a)debentures, stocks or bonds issued or proposed to be issued by a government; (b) debentures, stocks, shares, bonds or notes issued or proposed to be issued by a body corporate; (c) any right or option in respect of any such debentures, stocks, shares, bonds or notes; or (d) commodities futures, contracts, options and other derivatives, and which may be deposited, kept or stored with any licensed depository or custodian company as provided under ISA.

In September 2020, the Security and Exchange Commission (“SEC”) issued “Statement on Digital Assets and their Classification and Treatment” where it recognized crypto currency and other virtual crypto assets as securities. The New Rules on Issuance, Offering Platforms and Custody of Digital Assets 2022 (“Digital Assets Rules”) require registration of digital assets offering with SEC. The registration will be precluded by

initial assessment filing. During the assessment filing SEC shall determine whether the digital asset proposed to be offered, constitutes a "security" under the ISA.

SEC issued the Framework on Accelerated Regulatory Incubation for Onboarding Virtual Assets Service Providers ("VASP") and other Digital Investment Service Providers ("DISPs") 2024 ("ARIP Framework"). The ARIP Framework seeks to facilitate the onboarding of entities that are proposing to deal in virtual asset whose applications have been filed with the SEC, as well as potential applicants that intend to deal perform such activities in Nigeria.

Companies conducting ICOs are required to register their offerings with the SEC, disclose essential details about the token's purpose, utility, and risk, and comply with transparency and investor protection rules. To ensure compliance, companies should conduct thorough legal assessments, prepare detailed white papers, and adopt sound business practices such as anti-fraud measures and proper token valuation.

Legal counsel should be engaged to navigate the evolving regulatory landscape to prevent potential non-compliance.

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

Licensed cryptocurrency exchanges are considered as capital market operators and are bound by Anti-Money Laundering ("AML") and Know Your Customer ("KYC") for capital market operators. Paragraph 5.1 (i) of the Digital Asset Rules require VASPs to have in place adequate policies, procedures and controls to mitigate against money laundering, terrorism financing and counter proliferation financing requirements and comply with Anti Money Laundering/Combating Financing of Terrorism and Proliferation Financing ("AML/CFT/CPF") laws and regulations.

The SEC Capital Market Operators Anti-Money Laundering and Combating the Financing of Terrorism) Regulations, 2022 ("SEC AML Regulation") provides AML/CFT/CPF guidelines for capital market operators including VASPS. Some of the notable provision of the SEC AML Regulations include the obligation imposed on VASP to provide information to the SEC, Nigerian Financial Intelligence Unit and other relevant law enforcement agencies on AML/CFT/CPF matters. The SEC AML Regulations also prevents a capital market operator from keeping anonymous accounts or accounts in fictitious names; and where nominee accounts are maintained, details of the beneficial owners shall be provided on request.

Additionally, a VASP shall undertake Customer Due Diligence (CDD) measures when:

- business relationship is established;
- carrying out occasional transactions above the sum of $1,000 or its equivalent or such other thresholds as may be determined by SEC from time to time,
- there is a suspicion of money laundering, terrorist financing or proliferation financing regardless of any exemptions or any other sum referred to in these Regulations; or
- there are doubts about the veracity or adequacy of previously obtained clients identification data;

VASPs can implement effective compliance programs by appointing or designating AML/CFT/CPF compliance officer to monitor compliance with the AML/CFT/CPF program, regular training of staff on AML/CFT/CPF compliance, implementation of customer due diligence measures, timely reporting of suspicious transactions, periodic independent AML/CFT/CPF audit, regular screening of customers names against sanctions list, among others.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

Government regulations mandating licensing and regulatory oversight have a profound impact on the operations of cryptocurrency and blockchain companies in Nigeria. The Central Bank of Nigeria (CBN) and the Securities and Exchange Commission (SEC) play critical roles in defining the regulatory framework for this sector. For example, the CBN's 2021 directive prohibited financial institutions from facilitating cryptocurrency transactions, creating operational challenges for crypto-based businesses. While this measure was intended to mitigate risks such as fraud and money laundering, it also restricted access to traditional banking services, compelling companies to rely on peer-to-peer (P2P) networks and alternative payment methods.

Regulatory uncertainty in this space can also impact

investor confidence and the ability of businesses to scale, as companies face difficulties in aligning with undefined or evolving policies. For blockchain companies offering services such as tokenized assets, smart contracts, or decentralized finance (DeFi), adhering to anti-money laundering (AML) and know-your-customer (KYC) regulations has become increasingly vital. This compliance requires significant investment in technology and expertise to implement systems that monitor transactions, flag suspicious activity, and secure user identities.

To navigate these varying requirements, companies should adopt a proactive compliance strategy. This includes maintaining open lines of communication with regulatory authorities like the CBN and SEC to remain updated on policy developments and ensure alignment with emerging guidelines. Additionally, companies can engage legal and compliance experts to assess regulatory risks and develop robust internal policies tailored to Nigerian laws. For instance, implementing blockchain analytics tools can help ensure compliance with AML/KYC requirements and foster trust with regulators.

Furthermore, participating in regulatory sandboxes offered by the CBN or SEC allows companies to test innovative solutions within a controlled environment while ensuring compliance with legal frameworks. Collaboration with industry associations and peer companies can also help advocate for balanced regulations that promote innovation while protecting consumers and the financial system. By adopting these strategies, cryptocurrency and blockchain companies can effectively navigate regulatory requirements, reduce operational risks, and position themselves for sustainable growth in Nigeria's evolving fintech landscape.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

Cryptocurrency companies operating in Nigeria must adhere to the Federal Inland Revenue Service (FIRS) and state regulations regarding tax reporting and obligations associated with digital assets. While the Nigerian tax framework for cryptocurrencies is still evolving, FIRS requires companies to report all income generated from cryptocurrency-related transactions, including capital gains, profits from trading, and earnings derived from crypto-to-fiat conversions. Proper compliance ensures businesses avoid penalties and establishes trust with regulatory authorities.

To comply effectively, companies should implement robust systems for maintaining accurate and detailed transaction records. This includes tracking the purchase and sale prices of digital assets, timestamps of transactions, and the applicable exchange rates at the time of conversion. Establishing an automated tax reporting tool or integrating blockchain analytics software can simplify the process of calculating tax liabilities and generating accurate reports.

Additionally, companies should engage the services of tax professionals with expertise in cryptocurrency to navigate the complexities of the tax code and ensure that filings comply with both local laws and international best practices. Businesses must also stay informed of evolving guidelines, as Nigerian authorities continue to refine the regulatory framework for digital assets. For instance, remaining aware of potential obligations such as value-added tax (VAT) on crypto services or withholding taxes on transactions involving foreign entities will help businesses remain proactive.

Education and transparency are also critical. Companies should establish internal training programs to ensure their teams understand tax obligations and compliance procedures. Clear communication with stakeholders, including investors and customers, about how taxes are managed can further build confidence in their operations.

By leveraging technology, engaging qualified advisors, and staying abreast of regulatory developments, cryptocurrency companies in Nigeria can effectively navigate tax compliance, contributing to a more stable and trustworthy ecosystem for digital assets.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

Blockchain companies operating in Nigeria are required to comply with the Nigeria Data Protection Regulation (NDPR) and the National Data Protection Act (NDPA). These frameworks, enforced by the National Data Protection Commission (NDPC), aim to safeguard personal data and ensure organizations uphold data privacy principles. While the decentralized nature of blockchain technology promotes transparency, companies must navigate these regulations carefully to ensure compliance without compromising the benefits of decentralization.

To address these requirements, blockchain companies should implement privacy-focused technologies such as data encryption, pseudonymization, and anonymization. These techniques ensure that personal data is protected while maintaining the integrity of blockchain operations. For instance, leveraging zero-knowledge proofs allows companies to validate transactions or verify user identities without exposing sensitive data, thereby aligning with both the transparency and privacy mandates of the NDPR and NDPA.

Consent management is another critical aspect of compliance. Under the NDPA, companies must obtain explicit and informed consent from users before collecting, processing, or sharing personal data. Blockchain companies can integrate smart contracts to automate consent processes, ensuring that data collection and processing adhere to regulatory requirements. Additionally, companies should provide users with clear mechanisms to exercise their rights under the NDPR and NDPA, such as data access, correction, and deletion requests.

Regular compliance audits are essential to assess adherence to these regulations. Blockchain companies should also establish and regularly update data protection policies that outline how they manage user data. Employing a Data Protection Officer (DPO) or working with legal experts can help ensure alignment with the NDPR and NDPA while addressing the unique challenges posed by blockchain technology.

Lastly, maintaining robust network security is crucial to prevent data breaches. Companies should implement best practices in cybersecurity, such as conducting regular penetration tests, encrypting data, and ensuring that their decentralized applications (dApps) meet security standards.

By adopting these measures and fostering close collaboration with the NDPC, blockchain companies can balance compliance with data protection laws while preserving the transparency and security that underpin blockchain technology.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

While Nigeria does not have a direct equivalent of the U.S. H-1B or L-1 visa programs, it has provisions that allow foreign nationals to work within the country under specific conditions. The Nigerian Immigration Service (NIS) issues work permits, particularly for skilled professionals in high-demand sectors like fintech. Companies aiming to hire international talent for specialized roles may need to apply for expatriate quotas, residence permits, and visas for foreign employees.

Navigating the immigration process requires a thorough understanding of the applicable work permits and compliance with Nigerian labor laws.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all applicable laws and regulations?

To operate in Nigeria, fintech companies must comply with a range of regulatory and compliance requirements overseen by bodies such as the Central Bank of Nigeria (CBN), the Securities and Exchange Commission (SEC), the National Insurance Commission (NAICOM), and the National Data Protection Commission (NDPC). Depending on the nature of services offered, fintechs may require specific licenses, such as a Payment Service Bank license, a Microfinance Bank license, or registration with the SEC for capital market activities.

Ensuring compliance involves conducting a comprehensive legal and regulatory audit to understand the applicable laws, including data protection requirements under the NDPR and NDPA, anti-money laundering obligations, and consumer protection standards. Engaging local legal and regulatory experts is essential to navigate the nuances of Nigeria's financial ecosystem.

Additionally, fintechs should adopt a proactive compliance framework, including robust internal controls, staff training, and regular audits, to ensure ongoing adherence to all applicable regulations.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

A successful market entry strategy for fintechs in Nigeria begins with an in-depth analysis of target customer demographics. With a predominantly young, tech-savvy population and increasing mobile penetration, fintech

solutions addressing digital payments, credit access, and wealth management are well-positioned for growth.

Understanding the competitive landscape is equally crucial. Fintechs should identify gaps in existing offerings and design solutions tailored to underserved segments. Collaborating with local banks, microfinance institutions, and mobile network operators can facilitate market penetration, leveraging established networks and regulatory expertise.

Investing in localized branding, consumer education, and customer support can foster trust and adoption. Additionally, partnerships with local fintech related associations, can provide valuable insights and advocacy support.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure a smooth transition and sustainable growth?

The primary financial risks include fluctuating foreign exchange rates, high inflation, and economic volatility, which can affect pricing and profitability. Operational risks include navigating a complex regulatory environment, infrastructure limitations, and cybersecurity threats.

To mitigate these risks, fintechs should adopt a localized pricing strategy to account for currency fluctuations and partner with financial institutions to share operational costs. Establishing strong compliance protocols and maintaining close communication with regulatory bodies can minimize legal risks.

Cybersecurity should also be prioritized, with investment in advanced security systems and regular penetration testing to safeguard customer data and assets. Building local talent and leveraging partnerships with experienced local stakeholders can further mitigate operational challenges.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

Yes, Nigerian laws permit certain business functions to be outsourced to offshore locations, provided such outsourcing complies with relevant regulatory requirements. For example, the Central Bank of Nigeria (CBN) permits financial institutions to outsource non-core functions but mandates that the service provider meets data protection and cybersecurity standards, including compliance with the NDPR and NDPA.

When outsourcing, fintechs must ensure that service-level agreements (SLAs) include robust data protection clauses and guarantee compliance with Nigerian laws. Collaborating with reputable vendors who adhere to global best practices can help mitigate risks and maintain operational efficiency.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

Fintech companies can protect proprietary algorithms and software through a combination of strategies including intellectual property rights protection such as copyright and patents, and adopting contractual and operational protections. These are discussed below:

a. Copyright protection: Algorithms and software are intellectual property that can be protected as copyright. In Nigeria, by virtue of the Copyright Act No. 8 2022 ("Copyright Act") computer programmes, including software and algorithms, are regarded as literary works which are eligible for copyright protection. The Copyright Act protects computer programmes by granting rights to reproduce the programmes, distribute copies commercially, adapt or modify it, and make it available to the public online. These rights ensure control over the creation, use, and distribution of software and algorithms while safeguarding their commercial and functional applications. This protection is available for a duration of 70 years after the death of the copyright holder.

Under the Copyright Act, no formality is required to confer copyright protection of any eligible work provided they meet the eligibility requirement in Section 2 of the Copyright Act being that:

- some effort has been expended in creating the computer programmes, to give them an original character; and
- the computer programmes have been fixed in any medium from which they can be perceived, reproduced or otherwise communicated either directly or with the aid of any machine or device.

Notwithstanding, for added protection, the fintechs may voluntarily notify the Nigerian Copyright Commission to establish a public record of their copyright in such

software and algorithms.

b. Patents: In Nigeria, patents can be another strategy for the protection of software and algorithm where they are new, result from inventive activity and are capable of industrial application, or where the software and algorithms constitute an improvement upon a patented invention. While patents do not protect the software codes or algorithms themselves, it offers protection of their novelty and functionality. Patent grants the fintechs exclusive rights to use, assign, or license their software and algorithms for 20 (twenty) years, subject to annual renewal fees payable to the Nigerian Trademarks, Patents and Designs Registry (the "Registry").
c. Contractual Protections: Fintechs must adopt the use of water-tight non-disclosure agreements (NDAs), non-compete provisions, and appropriate licensing agreements should be used with employees, contractors, and partners to prevent unauthorized use or disclosure of the source codes of their software.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

To safeguard trademarks and service marks, fintechs must procure trademark registration of its tradenames and logos in the appropriate trademark classes with the Trademarks, Patents and Designs Registry. In Nigeria, the procedure for trademark registration is as follows:

- conducting an availability search on the proposed mark under the relevant trademark class. The purpose of the search is to confirm that no same or similar mark has been registered prior at the Registry.
- Where the search report confirms that no same or similar mark exists, the trademark application and supporting document is filed vide the Registry's online filing portal and an acknowledgment notice is issued by the Registry in favour of the filed mark(s).
- The Registrar of Trademarks thereafter conducts an independent examination of the Trademark Register to confirm that there is no conflicting or similar registration that may pose a problem to the application process, and that the mark is not deceptive, scandalous or in any way disallowed under extant laws. Upon such confirmation of the above, an Acceptance Notice is thereby issued by the Registrar of Trademarks in favour of the filed mark(s).
- Post-examination, the mark will be published in the Trademarks Journal. In the absence of any third-party opposition or objection received by the Registry within two months after the publication, the proprietor of the mark will be issued a Certificate of Registration.

Upon registration of its service marks and tradename, a fintech should regularly monitor for potential infringements through trademark watch services or by leveraging technology to track unauthorized use.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

Using open-source software ("OSS") in fintech products in Nigeria comes with important legal and operational risks due to the sensitive nature of handling financial transactions and personal data. Some OSS licenses, such as copyleft licenses, require companies to disclose or share the source code of their derivative works, which may conflict with the need to protect proprietary fintech algorithms or business models.

While OSS is often considered secure because of its collaborative development, its open nature also makes it vulnerable. Attackers can study the freely available source code to exploit weaknesses, which is especially concerning in Nigeria's high-risk cybersecurity environment. These could lead to data breaches, cybersecurity risks and financial loss, exposing companies to potential legal and regulatory challenges.

To mitigate these risks and ensure compliance with open-source licensing agreements, fintech companies should:

- Review the specific terms of each OSS license agreement to address requirements like attribution, redistribution rules, and obligations that may conflict with proprietary goals.
- Maintain a software bill of materials (SBOM) to track licensing obligations.
- Implement a robust internal policy for evaluating, approving, and maintaining OSS to ensure its safe and compliant use.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

Fintech companies must carefully manage intellectual property (IP) ownership when collaborating with third-party developers or partners to avoid disputes and

protect proprietary assets. Clear contracts should define ownership of any IP created during the collaboration, with IP assignment clauses to ensure rights are transferred to the fintech company. Where joint ownership is unavoidable, agreements must specify each party's rights and obligations regarding licensing, use, and commercialization.

To safeguard sensitive information, Non-Disclosure Agreements (NDAs) and confidentiality clauses are critical. Additionally, conducting due diligence on collaborators helps identify pre-existing IP that could complicate ownership or lead to infringement risks.

Engaging legal counsel and pursuing enforcement through cease-and-desist letters or litigation when necessary are effective ways to protect their IP.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

To prevent and address intellectual property ("IP") infringements, fintech companies should take a proactive approach. This includes registering all IP assets, such as patents, trademarks, and copyrights, in relevant jurisdictions and using monitoring services to detect unauthorized use of their technology or trademarks.

Upon detecting infringements, companies should issue cease-and-desist letters and, if necessary, pursue litigation to deter further violations. For copyright infringements through online contents, Section 54 of the Copyright Act allows IP owners to take down rights. This involves notifying the service providers on whose system or network the infringing online content is hosted, who must then inform the infringing party (its subscriber) and proceed to take down or disable access to infringing content. If the service provider receives repeated infringement notices, they may suspend the subscriber's account.

Employee training is also key to identifying and reporting IP misuse, while robust cybersecurity measures help prevent the theft of proprietary technology or trade secrets.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

In Nigeria, although there is no specific legislation explicitly defining the legal obligations of fintech companies using Artificial Intelligence (AI) for credit scoring and lending decisions, fintechs are subject to various legal and regulatory frameworks that enforce transparency, fairness, and non-discrimination. These include data protection laws, anti-discrimination legislations, and specific regulations issued by regulatory bodies such as the Central Bank of Nigeria (CBN). The overarching legal obligations primarily concern compliance with anti-discrimination laws, data protection regulations, and transparency in automated decision-making processes.

- Compliance with Anti-Discrimination and Consumer Protection Laws
  While the 1999 Constitution of the Federal Republic of Nigeria (as amended) does not directly address fintechs, Section 42 guarantees the right to freedom from discrimination based on ethnicity, gender, religion, place of origin, or other status. This provision extends to all economic transactions, including credit and lending decisions. As such, AI algorithms used in credit scoring and lending must not result in discriminatory outcomes based on any prohibited characteristics. Any failure to ensure equitable treatment could expose fintechs to legal challenges, regulatory sanctions, and significant reputational harm.
  Additionally, the CBN's Consumer Protection Regulations 2019 mandate that fintechs licensed by the CBN treat consumers equitably without bias throughout their business relationship. This requires fintechs to provide equal access to financial services for all eligible consumers, irrespective of their gender, age, religion, ethnicity, or other protected characteristics. Consequently, fintech companies must ensure that their AI algorithms are designed and implemented in a manner that avoids discriminatory outcomes that disadvantage certain individuals or groups.
- Data Protection and Privacy Laws
  The Nigeria Data Protection Act (NDPA) 2023 plays a critical role in regulating the collection, processing, and use of personal data. It mandates that personal data be processed in a fair, lawful, and transparent manner, and that customers are informed about how their data will be used. This includes obtaining informed consent from customers before their data is

processed for purposes such as credit scoring and lending. The NDPA further gives customers control over their data, allowing them to access, correct, or request the erasure of their personal data. Crucially, the NDPA prohibits fintechs from making decisions solely based on automated processing, including profiling, that produce legal effects or significantly affect customers unless expressly authorized by law or customer's consent. Customers also have the right to contest automated decisions and request human intervention. Fintechs must, therefore, ensure that they provide clear and transparent information to customers about the use of their data and the potential impacts on credit decisions. However, non-compliance with data protection obligations under the NDPA could lead to severe penalties, including fines and reputational damage. As such, fintechs must ensure their AI systems comply with these data protection and transparency requirements to avoid legal repercussions.

Fintechs can take several proactive steps to ensure that their AI systems are fair, transparent, and free from biases, especially in credit scoring and lending decisions:

- Fintechs should conduct periodic assessments to detect and address any inadvertent biases in their AI models. Independent third-party audits can help identify any potential discriminatory outcomes. Regular evaluations can also assess the impact of AI algorithms on different groups, particularly those protected under anti-discrimination laws, using fairness metrics such as demographic parity or equal opportunity.
- Transparency is crucial for fostering trust among customers and regulators. Fintechs should ensure that their AI models are explainable, and consumers should have access to information regarding the factors influencing credit decisions. Publishing regular reports that outline the rationale behind credit decisions can help build trust and demonstrate accountability.
- To avoid discriminatory outcomes, fintechs must ensure that the data used to train AI models is representative of diverse demographics, including gender, ethnicity, and socio-economic background. Using biased or non-representative data risks reinforcing existing societal inequalities. Fintechs must actively address data imbalances and ensure that historically marginalized or underserved groups are not disproportionately harmed by lending decisions.
- The accuracy and relevance of the data used for AI-based credit decisions are crucial. Fintechs must ensure that their models rely on high-quality data and that the data used is both accurate and relevant to the creditworthiness assessment. Inaccurate or outdated data can distort AI predictions and lead to unfair outcomes.
- Once an AI system is deployed, fintechs must continually monitor its performance to detect any emerging biases or adverse impacts. If discriminatory patterns are identified, fintechs should be prepared to make adjustments to ensure compliance with fairness standards and legal obligations.
- Fintechs should establish clear and transparent processes that allow consumers to challenge automated credit decisions. This includes providing an option for manual review if a customer believes that the AI model has treated them unfairly or if the decision is contested. Such mechanisms help ensure that consumers' rights are protected, and their concerns are addressed.
- Collaborating with independent auditors to assess the fairness and transparency of AI systems is essential. Third-party audits can provide an unbiased evaluation of the AI models and ensure compliance with applicable laws. Additionally, fintechs should maintain regular communication with Nigerian regulators such as the CBN to stay ahead of evolving regulatory frameworks and ensure that their AI systems align with regulatory expectations.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

Advancements in AI technology, particularly in the fintech industry, may be protected by intellectual property (IP) laws. When fintechs develop proprietary AI models, algorithms, or datasets, it is crucial to understand how to safeguard these innovations against unauthorized use or infringement. Protecting AI-related inventions through IP rights not only ensures exclusivity but also provides a competitive edge. Nigerian IP laws, including the Copyright Act 2022 and the Patents and Designs Act, provide avenues for protecting AI-related technologies.

In addition to IP protections, fintechs may use contracts to secure their AI-related technologies. These contracts should clearly define ownership of any IP created during the development of AI models and prevent unauthorized use by employees, contractors, or third parties. Examples of such contracts includes employment agreements,

NDAs etc. These agreements are vital for preserving the confidentiality and ownership of fintechs' AI technologies.

Many fintechs rely on third-party AI platforms, tools, or pre-trained models. It is essential to understand the licensing terms of these tools, ensuring compliance with restrictions related to use, modification, or distribution. Special attention should be paid to IP ownership clauses when using third-party tools, as they can impact who owns the AI models created from these tools. Using third-party tools in violation of licensing agreements can expose fintechs to legal risks, including IP infringement claims. If a third-party AI model or dataset infringes on another party's IP rights, the fintech could face significant legal consequences, such as damages, injunctions, or forced discontinuation of the technology.

22. What specific financial regulations must fintechs adhere to when deploying AI solutions, and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

In Nigeria, there are currently no specific regulations that exclusively address the use of AI by fintech companies. However, fintechs operating in Nigeria are required to comply with a range of financial regulations aimed at protecting consumers, ensuring fairness, and maintaining a stable financial system. These regulations, though not AI-specific, provide a solid framework for fintechs deploying AI technologies in areas like credit scoring, lending, and payment systems. The key regulations fintechs must adhere to include the following:

a. **Central Bank of Nigeria (CBN) Regulations**

The Central Bank of Nigeria (**CBN**) plays a pivotal role in regulating Nigeria's financial sector under the Central Bank of Nigeria Act 2007 and the Banks and Other Financial Institutions Act 2020. As the primary regulator of financial institutions, CBN issues a variety of guidelines and regulations that govern fintech operations. Some of the most relevant CBN guidelines for fintechs using AI include:

- CBN Guidelines on Operations of Electronic Payment Channels in Nigeria
- CBN Guidelines on Mobile Money Services in Nigeria
- CBN Guidelines on International Money Transfer Services in Nigeria
- CBN Regulations on Instant (Inter-Bank) Electronic Funds Transfer Services
- CBN Regulatory Framework for the Use of USSD for Financial Services in Nigeria
- CBN Customer Due Diligence Regulations 2023
- CBN Consumer Protection Regulations 2019

These regulations cover essential aspects of fintech operations, such as licensing, capital requirements, payment services, and digital banking, among others. Specifically, fintechs using AI for mobile payments, money transfers, or fraud detection must ensure that AI systems are secure, transparent, and protect consumer data. AI solutions must not compromise the integrity of financial systems or enable fraudulent activities.

To comply with these requirements, fintechs should focus on implementing transparent AI solutions that are secure and designed to safeguard user data, thus preventing fraud and system vulnerabilities.

b. **Securities and Exchange Commission (SEC) Regulations**

For fintechs operating in the areas of investment management, securities trading, or financial advisory services, compliance with the Investment and Securities Act 2007 and the SEC's Consolidated Rules 2013 (as amended) (the "**Regulations**") is critical. These Regulations focus on market conduct, investor protection, and fair trading practices, all of which can be influenced by AI technologies, particularly in market prediction, trading algorithms, or automated financial advice.

Fintechs deploying AI in securities trading must ensure that their algorithms meet the Regulations' requirements on transparency, fairness, and investor protection. This includes disclosing how AI-based systems operate, preventing market manipulation or giving unfair advantages to certain investors through biased or opaque algorithms.

c. **Federal Competition and Consumer Protection Guidelines**

The Federal Competition and Consumer Protection Commission (**FCCPC**) plays a pivotal role in safeguarding the rights of consumers in Nigeria. As the primary regulatory body for consumer protection, the FCCPC has the authority to investigate complaints, enforce compliance with consumer protection regulations, and impose sanctions on financial institutions or digital lenders that violate consumer rights. This is especially significant in the rapidly evolving digital lending landscape, where the use of AI-driven technologies raises

critical concerns about fairness, transparency, and consumer impact.

In response to the growing influence of digital lenders and the need to regulate this sector effectively, the FCCPC introduced the Limited Interim Regulatory/Registration Framework and Guidelines for Digital Lending (the "**Guidelines**"). These Guidelines require all digital lenders to obtain the approval of the FCCPC before engaging in lending activities. The objective is to establish clear rules for digital lending practices, promote transparency, and ensure that consumer interests are adequately protected.

For fintechs planning to deploy AI solutions in the digital lending space, strict compliance with the Guidelines is essential. Key provisions include:

- Digital lenders must seek and obtain approval from the FCCPC before commencing lending operations in Nigeria. This includes submitting relevant documentation and demonstrating compliance with regulatory standards.
- AI systems used in lending decisions must ensure fairness and transparency, preventing bias or discrimination. Compliance with the FCCPC's consumer protection standards is critical to avoiding legal penalties or reputational harm.
- Digital lenders must ensure that AI algorithms do not unfairly disadvantage certain groups of consumers, such as marginalized or underrepresented populations, and must offer clear and accessible dispute resolution mechanisms for consumers who are dissatisfied with AI-driven decisions.

By adhering to these requirements, fintechs can ensure that their AI solutions in the digital lending space are aligned with the regulatory expectations set forth by the FCCPC. This compliance not only protects consumers but also mitigates the risk of sanctions, fines, and reputational damage, ensuring that fintech companies can operate sustainably within Nigeria's legal framework.

d. **Nigeria Data Protection Act 2023 (NDPA)**

As AI systems heavily rely on large datasets, fintechs must comply with the Nigeria Data Protection Act 2023 (**NDPA**), which governs the collection, processing, and storage of personal data. AI systems must obtain explicit consent from consumers for data usage, implement data anonymization and encryption to protect sensitive information, ensure consumers have rights to access, correct, and delete their data. Thus, fintechs must prioritize data protection measures when deploying AI-driven solutions.

e. **Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Laws**

Fintech companies offering financial services must also comply with the Money Laundering (Prevention and Prohibition) Act 2022 and CBN Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations. AI tools designed for fraud detection, identity verification, and transaction monitoring must be designed to detect and prevent suspicious activities such as money laundering or terrorism financing.

AI systems must accurately identify and flag suspicious transactions, and align with AML/CFT regulations to prevent illegal activities in the financial system.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

To mitigate these risks, fintechs must implement robust risk management strategies that prioritize legal compliance and consumer protection such as:

- Fintechs must ensure full compliance with the NDPA regarding obtaining explicit, informed consent from users before processing their data for AI-powered decisions. Additionally, fintechs must implement both organizational and technical measures, such as data encryption, anonymization, and secure data storage practices, to protect personal data.
- To avoid legal liabilities and reputational harm, fintechs should regularly audit their AI systems for bias. These audits help ensure that AI algorithms do not produce discriminatory outcomes based on protected characteristics such as race, gender, age, or geographic location.
- Fintechs should stay vigilant by continually monitoring legislations impacting AI in the financial sector. This includes regulations from bodies such as the CBN, the Nigerian Data Protection Commission (NDPC).
- Fintechs should establish dedicated internal compliance teams to oversee and ensure that their AI technologies align with data privacy, anti-discrimination, financial regulations, and consumer protection laws. Creating a comprehensive AI governance framework is essential, outlining ethical principles for the development, deployment, and continuous monitoring of AI technologies.
- Consumers must have access to a fair and transparent process for contesting AI-driven decisions, such as loan denials or credit score assessments. Fintechs can implement a Human-in-

the-Loop (HITL) system, where a human supervisor reviews cases flagged by AI, providing consumers with the opportunity to challenge automated decisions. This ensures that consumers are not unfairly impacted by automated systems and that their concerns are addressed promptly.
- Fintechs should implement regular performance assessments to ensure that their AI systems function as intended and do not introduce unexpected errors or vulnerabilities over time. Ongoing monitoring and performance reviews help identify and address such issues before they result in significant legal liabilities or consumer harm. Timely detection of system errors minimizes the risk of costly legal actions and ensures that AI models remain effective and fair.
- Fintechs often rely on third-party vendors for AI technology, data, or infrastructure. It is crucial for fintechs to conduct thorough due diligence on their vendors to ensure compliance with legal requirements such as data protection and anti-discrimination regulations. Fintechs can be held legally responsible for the actions of their third-party vendors, including violations of data privacy or the use of discriminatory algorithms. By vetting vendors carefully and ensuring that they comply with relevant laws, fintechs can minimize the risk of legal issues arising from vendor practices, such as data breaches or discriminatory outcomes.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

Yes, Nigeria's fintech sector has experienced significant disruption, particularly in digital payments and financial inclusion. In 2024, the adoption of mobile wallets surged, facilitating seamless transactions and reducing reliance on cash. This shift was partly driven by the Central Bank of Nigeria's (CBN) National Financial Inclusion Strategy (NFIS), aiming for a 95% financial inclusion rate by 2024.

A notable example is Moniepoint, a Nigerian fintech company that secured $110 million in funding in October 2024, achieving “unicorn” status with a valuation exceeding $1 billion. Moniepoint processes over 800 million transactions monthly, valued at over $17 billion, and offers digital payment and banking solutions across Africa.

Additionally, the proliferation of point-of-sale (POS) terminals has transformed payment processing, with total cashless POS transactions rising by 45.41% year-on-year to NGN39.58 trillion.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

Nigeria's fintech sector remains a key player in Africa's digital transformation, attracting significant local and international investment. In 2024, the sector secured over $2 billion in funding, underscoring its status as one of the continent's most dynamic and innovative ecosystems.

a. Key Areas Attracting Investment:

- Digital Payments and Mobile Money: Digital payment platforms continue to lead in attracting investments due to the high demand for cashless solutions.
  In October 2024, Moniepoint raised $110 million in funding from investors, including Google, achieving unicorn status with a valuation exceeding $1 billion. The company processes over 800 million transactions monthly, valued at $17 billion, and has ambitious plans to expand across Africa.
  Flutterwave, a market leader raised $250 million in its Series D round in 2022, pushing its valuation to over $3 billion.
- Lending and Credit Platforms: Platforms like Carbon and FairMoney address the financing needs of underserved populations by offering microloans and BNPL (buy-now-pay-later) services. These startups consistently attract Series A and B funding as they scale operations.
- WealthTech and Investment Platforms: Startups such as RiseVest, Bamboo, and Cowrywise are providing Nigerians access to local and global investment opportunities, attracting early and mid-stage investments to support their growth.
- InsurTech: Startups like Casava are offering innovative and affordable insurance products. Casava raised $4 million in pre-seed funding in 2022, reflecting growing investor interest in this space.
- Cryptocurrency and Blockchain Solutions: Despite regulatory uncertainties, blockchain and crypto companies like Patricia and Bundle Africa have secured seed and Series A investments, focusing on crypto trading and blockchain-based financial services.
- Embedded Finance and BaaS (Banking-as-a-Service): Startups like Mono, Okra, and OnePipe enable seamless integrations between fintech platforms and traditional financial institutions. Mono raised $15 million in a Series A round in 2022, a testament to the growing interest in embedded finance.

b. Investment Levels:

- Pre-Seed and Seed Funding: Startups in emerging areas like insurtech and blockchain often receive early-stage funding from local angel investors and international accelerators like Y Combinator.
- Series A and B Funding: Established players in digital payments and lending secure these rounds to scale operations and enhance product offerings.
- Growth and Late-Stage Funding: Unicorns like Flutterwave and Moniepoint dominate this stage, with funding rounds exceeding $100 million to fuel expansion across Africa and beyond.

Contributors

Adeleke Alex-Adedipe
Managing Partner
a.alex-adedipe@doa-law.com

Chika Oke
Senior Associate
c.oke@doa-law.com

Christiana Ossai
Associate
c.ossai@doa-law.com

Abdulrasheed Badmus
Associate
a.badmus@doa-law.com

Bankole Oke
Associate
b.oke@doa-law.com