Legal 500
Country Comparative Guides 2025

Egypt
Fintech

Contributor

Shehata & Partners
Law Firm

Ibrahim Shehata

Partner | is@shehatalaw.com

Tasneem El-Naggar

Mid-Level Associate | tn@shehatalaw.com

Omar Mohamed

Junior Associate | om@shehatalaw.com

Mohamed Abed

Junior Associate | ma@shehatalaw.com

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

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

Egypt: Fintech

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

Egypt is establishing itself as a regional hub for Financial Technology (**"Fintech"**) innovation, supported by a robust regulatory framework that fosters industry growth while ensuring effective oversight of Fintech activities across both banking and non-banking sectors. The Fintech industry in Egypt is regulated by several key entities, each responsible for specific services and operating within their respective jurisdictions.

There are two main regulators for the Fintech industry in Egypt:

1. ***Central Bank of Egypt*** (**CBE**), which oversees the regulation of any Fintech activity within the banking financial sector[1].
2. ***Financial Regulatory Authority*** (**FRA**), which oversees the regulation any Fintech activity within the non-banking financial sector[2].

Other regulators might also be involved in the Fintech industry, such as:

1. ***Anti-Money Laundering and Terrorist Financing Unit*** (**AMLU**), which is a unit formed in the CBE to combat (a) financial crimes in accordance with the Anti-Money Laundering Law No. 80 of 2002 ("**AML Law**") and (b) the compliance of Fintech companies to its provisions[3].
2. ***National Telecommunications Regulatory Authority*** (**NTRA**), when it comes to organizing the communications facility and developing and disseminating all its services in a manner that keeps pace with the latest technology and meets all users' needs[4], including the Fintech sector.
3. ***Information Technology Industry Development Authority*** (**ITIDA**), which plays a supportive role in the Fintech sector by fostering innovation and digital transformation.

These regulatory authorities primarily oversee Fintech activities through the legal framework governing the Fintech sector in Egypt, which includes the following:

1. Fintech Law No. 5 of 2022 ("**Fintech Law**"), which regulates the use of fintech in the non-banking sector (including real estate funding, small, medium and microfinance, finance leasing, factoring and consumer financing activities that utilize fintech).
2. The Banking Law No. 194 of 2020 ("**Banking Law**"), which regulates fintech businesses operating in the banking sector.

Footnote(s):

[1] Article (201) of the Banking Law.

[2] Article (2) of the Banking Law.

[3] Article (3) of Presidential Decree No.164 of 2002.

[4] Article (4) of the Telecommunications Law No.10 of 2003.

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

Certain risks may pose challenges to the burgeoning Fintech market. As this dynamic sector continues to evolve, it faces a range of uncertainties that have the potential to impact its trajectory. It is crucial for industry participants, regulatory bodies, and stakeholders to remain vigilant and proactive in addressing these challenges. From regulatory complexities to cybersecurity threats and competition dynamics, a comprehensive understanding of these risks is essential to foster a resilient and sustainable Fintech ecosystem. In light of the foregoing, several risks merit attention:

Regulatory Challenges**:** Changes in regulations or the introduction of new regulatory requirements can impact on the Fintech sector. Striking the right balance between fostering innovation and ensuring consumer protection may pose challenges.

Cybersecurity Threats**:** The increasing reliance on digital financial services makes the sector more susceptible to cybersecurity threats. Fintech companies need robust security measures to protect sensitive customer data and maintain trust.

Access to Funding**:** The growth of Fintech companies often relies on access to funding. Economic uncertainties or difficulties in attracting investments might impede the development of new Fintech solutions.

***Consumer Trust*:** Fintech success is closely tied to consumer trust. Any major security breaches, data leaks, or fraud incidents can erode trust in digital financial services, hindering the adoption of Fintech solutions.

***Infrastructure and Connectivity*:** In certain regions, challenges related to infrastructure and internet connectivity could limit the reach of Fintech services, particularly in rural areas.

***Competition and Market Saturation*:** Increased competition within the Fintech sector may lead to market saturation, making it challenging for new entrants to differentiate themselves and gain market share.

***Financial Inclusion Barriers*:** While Fintech has the potential to enhance financial inclusion, there may be barriers related to literacy, access to smartphones, or the reluctance of certain demographic groups to adopt digital financial services.

***Global Economic Factors*:** Global economic conditions, such as economic downturns or currency fluctuations, can have indirect effects on the Fintech market in Egypt.

***Skills Shortage*:** There may be a shortage of the skills required to develop and operate digital financial services.

***Financial Literacy*:** Some consumers may have limited awareness of digital financial services and how to use them.

Integration with the Traditional Financial System: There may be challenges in integrating digital financial services with the traditional financial system.

Nevertheless, in July 2023, during the Seamless North Africa Conference, the CBE released the latest edition of the "Financial Technology Landscape" report, covering developments up to 2022.[5] This updated report highlights several key indicators:

Growth of FinTech Startups: The number of FinTech startups in Egypt has reached unprecedented levels, indicating a vibrant and expanding ecosystem.

Investment Attraction: Despite global economic challenges, Egyptian FinTech startups attracted approximately $800 million in investments, underscoring sustained investor confidence in the sector.

These findings suggest that while previous challenges identified in the previous reports may still be relevant, the sector has demonstrated resilience and growth. The increased investment and startup activity reflect a positive trajectory for FinTech in Egypt.

Footnote(s):

[5] CBE.

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

Fintech companies operating in Egypt are required to obtain licenses or approvals from regulatory bodies such as the FRA or the CBE, depending on the nature of their activities. These regulations ensure that Fintechs comply with standards of transparency, security, and operational accountability while fostering trust in financial services.

Licensing for Non-banking financial activities: Non-banking financial activities, encompassing the use of several technology activities, such as digital platforms, digital applications, blockchain, digital contract and digital ID, generally require the prior issuance of one of the following licenses or permits from the FRA.

- ***Fintech License:*** A license to undertake non-banking financial activities will require that the applicant company (a) only carries out its licensed activities (b) to establish clear shareholding structure depicting the direct and indirect ownership interests and the concerned parties thereto, and (c) that it is equipped with the proper technology infrastructure and security means to carry out these activities pursuant to the FRA board requirements in this respect.[6]
- ***Fintech Permit:*** These could be granted directly to companies already licensed to adopt Fintech solutions or outsource operations. In addition to the FRA license for non-banking financial activities, obtaining the FRA Fintech permit would necessitate meeting the following conditions:[7]
  - The applicant possesses the necessary information technology systems and security equipment in accordance with the FRA board requirements;
  - The applicant shall not be in breach of the law regulating its activity; and
  - The necessary fees shall be paid, which will be equivalent to half of the license fee.

FRA Temporary License: the Fintech Law enables the FRA to issue a temporary license for startups in the non-banking financial activities for up to two (2) years, to enable startups to test their Fintech with real consumers under the supervision of the FRA.[8] In this respect, the FRA **Decree No. 268 of 2023** delineates the crucial procedures for the incorporation and licensing of non-banking financial activities for startups delving into the realm of Fintech, which requires the company to meet certain

requirements, including, *inter alia*, the following: (i) the company must be incorporated in the form of a joint stock company; (ii) there shall be a minimum of fifteen (15) million EGP as the issued and paid capital; and (iii) there shall be a minimum of 25% shareholding ownership by technology or Fintech specialists. Additionally, FRA **Decree No. 58 of 2022**, establishes the terms and procedures required for establishment, licensing and approval for startups operating in specific financial activities, including real estate finance, Small and Medium-sized Enterprises (**"SMEs**") finance, microfinance, financial leasing, factoring, and consumer finance.[9]

CBE License: The CBE primarily regulates the banking financial activities using Fintech, as providers of digital finance associated with providing an electronic payment or collection service shall obtain the CBE's approval before providing these services, in accordance with the rules and procedures to be determined by a decision issued by the CBE.[10]

Footnote(s):

[6] Article (4) of the Fintech Law.

[7] Article (5) of the Fintech Law.

[8] Article (9) of the Fintech Law.

[9] Article (1) of the FRA Decree No. 58 of 2022.

[10] Article (205) of the Banking Law.

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

The regulatory sandbox is a virtually constructed and well-defined space, within which applicants can experiment their innovative Fintech solutions in a live and relaxed regulatory environment for a limited period of time on a small scale and under a well-defined parameter, where challenges and risks to the financial system and ordinary Fintech consumers have been strictly contained.[11]

The regulatory sandbox aims to support and facilitate the entry of startups with innovative solutions into the market, enhance regulatory understanding of Fintech, and improve regulatory practices to support sustainable and inclusive financial growth.[12] Therefore, the regulatory sandbox is embedding compliance within the Fintech ecosystem at an early stage. This will not only allow Fintech innovators to focus on their core offering but also ensure that consumers and other players in the market are not adversely affected by the regulatory uncertainty of the disruptive Fintech activities.

There are two main types of sandboxes in Egypt:

- ***One for the banking Fintech sector***, which operates under the umbrella of the CBE; and
- ***One for the non-banking Fintech sector***, which operates under the umbrella of the FRA.

A. Banking Fintech Sector: CBE Sandbox

As part of its role as a catalyst for change and supporter of the Fintech industry, the CBE launched its **"CBE Sandbox"** in May 2019, which serves as a testing environment for Fintech businesses developing new business models facing challenges from stringent authorization requirements and regulatory uncertainties. The CBE Sandbox functions as a virtual and well-defined space, giving applicants the opportunity to experiment with their innovative Fintech solutions. This experimentation occurs within a live, relaxed regulatory environment for a limited duration, on a small scale, and under precisely defined parameters.

The CBE Sandbox is designed to contain challenges and risks to the financial system and ordinary Fintech consumers, ensuring a controlled testing environment. The primary goal of the CBE Sandbox is to integrate compliance into the Fintech ecosystem at its early stages. By doing so, it enables Fintech innovators to concentrate on refining their core offerings while simultaneously safeguarding consumers and other market participants from adverse effects related to regulatory uncertainties stemming from disruptive Fintech activities.

B. Non-Banking Fintech Sector: FRA Sandbox (CORBEH)

In March 2023, Egypt introduced its first FRA authorized Sandbox, called (**"CORBEH Sandbox"**), to facilitate the testing of Fintech applications. This Sandbox, established with the authorization of the FRA, involves a collaboration with Egypt securities exchange. The framework aims to balance innovation promotion and risk management by providing a controlled environment for experimentation. It is governed by the Fintech Law and related FRA decrees. Key features include adaptable licensing and capital flexibility, the involvement of authorized founders' agents, compliance obligations, ongoing monitoring and reporting, and a focus on consumer protection and risk mitigation. The core ongoing obligations within CORBEH Sandbox stress the establishment of governance structures, ensuring compliance and maintaining

transparency.

Considering the above, the regulatory sandbox provides a wide range of benefits to Fintech startups in Egypt, such as:

***Encourages Innovation*:** One of the key advantages of a regulatory sandbox is that it provides a safe space for start-ups to experiment, develop, and innovate. Start-ups can test their products and services in a controlled environment without worrying about full regulatory compliance encouraging start-ups to be more creative and take risks that they might not be able to take in a more controlled, regulated environment.

Consumer Protection: Regulatory sandboxes ensure that consumer protection is maintained while promoting innovation. Participating start-ups in the sandbox must comply with specific consumer protection requirements, meaning consumers can feel more secure when using their products and services.

Regulatory Certainty: Regulatory sandboxes allow Fintech start-ups to engage with regulators and receive guidance on regulatory compliance, helping to reduce regulatory uncertainty while providing start-ups with greater certainty on how to comply with regulations once they leave the sandbox.

Faster Time-to-Market*:* Regulatory sandboxes offer Fintech start-ups a quicker time-to-market by reducing the time and costs associated with regulatory compliance. Start-ups can test their products and services more quickly in the sandbox, which can help them to bring the marketplace once they leave the sandbox.

Competitive Advantage*:* Start-ups that successfully complete the regulatory sandbox program may gain a competitive advantage by demonstrating to customers, investors, and regulators that their products and services have been rigorously tested and comply with regulatory requirements.

Improved Regulation: regulatory sandboxes provide regulators with a better understanding of Fintech innovation, helping them to develop more effective and proportionate regulations, leading to a more efficient and effective regulatory environment for Fintech start-ups.

Footnote(s):

[11] https://www.cbe.org.eg/-/media/project/cbe/page-content/media/cbe—regulatory-sandbox-may-en.pdf

[12] Article (3) of the FRA Decree No. 163 of 2024.

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?

The **Capital Markets Law No. 95 of 1992** regulates the issuance and trading of securities in Egypt; however, it does not specifically mention the application of its provisions to Initial Coin Offerings (**"ICOs"**) and other crypto assets.

The landscape for ICOs in Egypt remains ambiguous, posing significant challenges for both issuers and investors. The absence of specific regulations governing ICOs adds to the uncertainty surrounding their legal implications as a fundraising mechanism. Moreover, the CBE has issued multiple cautionary warnings emphasizing the risks associated with ICOs and virtual currencies. These warnings reflect a stance of regulatory prudence rather than a comprehensive regulatory framework.[13]

A notable aspect of the current situation is the varied approaches adopted by several local startups that have ventured into ICOs. However, this trend has raised concerns regarding potential scams and highlighted the urgent need for stronger investor protection measures. Despite these challenges, there are indications of increasing government interest in the blockchain technology, hinting a possible move towards establishing regulations for the crypto space.

ICOs represent one category of crypto assets, alongside other categories such as cryptocurrency, Non- Fungible Tokens (**NFTs**), and utility tokens.

Cryptocurrency:

By virtue of Article 206 of the Banking Law, the trading, issuing and promotion of cryptocurrencies and electronic money are explicitly prohibited without obtaining a license from the CBE, adhering to the standards set forth by the CBE. However, contradicting this stance, in September 2022 and March 2023, the CBE reiterated its warning against cryptocurrencies, emphasizing their prohibition and emphasizing that they lack backing from any governmental authority. The prohibition is attributed to concerns related to e-piracy, significant market volatility, and the potential misuse of cryptocurrencies in financial crimes. Additionally, the Banking Law outlined stringent penalties for violations, including imprisonment and/or fines ranging from not less than one (1) million

EGP to a maximum of ten (10) million EGP.[14]

NFTs:

While the regulatory landscape for NFTs in Egypt is developing, existing regulations, such as the Banking Law, prohibit the use of virtual assets- cryptocurrencies and possibly NFTs – for financial transactions without obtaining a prior license from the CBE. However, the application of these regulations to NFTs used for non-financial purposes, such as art or collectibles, remains ambiguous.

Utility Tokens and Tokenization Regulations:

The CBE has issued Tokenization Regulations for Payment Cards on Electronic Devices' Applications (**"Tokenization Regulations"**), marking a significant step toward advancing Egypt's vision for financial inclusion and fostering a more cashless society. [15]

The Tokenization Regulations establish infrastructure requirements for banks and tokenization service providers to facilitate card tokenization. Their goal is to strengthen the digital payments ecosystem by broadening access to banking services and encouraging the adoption of digital financial solutions.

Furthermore, issuance of these Tokenization Regulations enables the integration of services from various international companies', such as Apple Pay and Samsung Pay, creating great opportunities to deliver innovative financial solutions that meet customer needs.

In this respect, companies are advised to remain up-to-date with the CBE's Tokenization Regulations, actively engage with the CBE and FRA, and seek guidance to clarify the classification and licensing requirements for crypto assets, including cryptocurrencies, utility tokens, and others.

Footnote(s):

13 https://www.cbe.org.eg/en/news-publications/news/2023/03/08/warning-statement

[14] Article (225) of the Banking Law.

15 https://www.cbe.org.eg/en/news-publications/news/2023/03/08/cbe-issues-the-regulations-of-the-payment-cards-tokenization-on-electronic-devices-applications

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?

All financial institutions in Egypt, including cryptocurrency exchanges, are required to comply with several AML and Know Your Customer (**"KYC"**) requirements, as outlined by the AML Law and its executive regulations. While Egypt does not yet have specific laws directly regulating cryptocurrency exchanges, the AML Law provides the legal framework for AML and KYC compliance.

- ***AML Compliance and Implementation Key Requirements for Fintech Companies:***
  - Notify the AMLU immediately of any suspected incidents involving money laundering, terrorist financing, or attempts to conduct such activities, regardless of their value. [16]
  - Establish systems that implement customer due diligence procedures and other rules and procedures related to combating money laundering and terrorist financing issued by the AMLU[17].
  - Continuously update their systems, rules, procedures and indicators to periodically monitor suspicious operations[18].
  - Develop and implement policies, along with necessary measures, to prevent the misuse of modern technological advancements for purposes of money laundering or terrorist financing[19].
  - Appoint a dedicated manager responsible for overseeing anti-money laundering efforts and ensuring full compliance with laws and regulations related to combating money laundering[20],[21].
- **KYC Compliance and Implementations Key Requirements for Fintech Companies:**
  - Retain customer and transaction records for a minimum of five (5) years, including identification documents, transaction history, and records of any due diligence checks[22].
  - Periodically update this data and ensure these records and documents are readily available to judicial authorities upon request[23].
  - For high-risk customers, implement enhanced due diligence by collecting additional and more frequent information about their financial background[24].

Footnote(s):

[16] Article (8) of AML Law No.80 of 2002.

[17] Article (8) of AML Law No.80 of 2002.

[18] Article 32(1) of AML Law No.80 of 2002 Executive Regulations.

[19] Article 32(3) of AML Law No.80 of 2002 Executive Regulations.

[20] Article (35) of AML Law No.80 of 2002 Executive Regulations.

[21] Article (36) of AML Law No.80 of 2002 Executive Regulations.

[22] Article (34) of AML Law No.80 of 2002 Executive Regulations.

[23] Article (9) of AML Law No.80 of 2002.

[24] Article (32) bis of AM Law No.80 of 2002 Executive Regulations.

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?

Impact of Regulations:

Government regulations in Egypt significantly influence the operations of cryptocurrency and blockchain companies, imposing strict licensing and compliance requirements.

Banking Law mandates that any activities involving the issuance, trading, or promotion of cryptocurrencies must be licensed by the CBE. Non-compliance with this requirement carries severe penalties, including imprisonment and fines ranging from 1 to 10 million EGP. This regulatory framework creates a high barrier to entry for companies seeking to operate in the sector, requiring substantial preparation and adherence to legal guidelines.

The FRA plays a pivotal role in overseeing blockchain applications and digital ledger technology (**"DLT"**). Under **FRA Decision No. 140 of 2023**, the use of DLT, including blockchain, requires prior approval from the FRA and adherence to specific criteria for licensing and operation. The Decision outlines infrastructure requirements such as peer-to-peer networks, consensus algorithms, and secure, decentralized databases to ensure transparency and security. Companies must also appoint a "General Coordinator" to manage technical operations and participant needs. The FRA allows for various blockchain models, including public, private, permissioned, and non-permissioned systems, and may involve cryptographic assets where applicable. This regulatory oversight shapes how companies design their systems, necessitating significant investments in infrastructure and compliance mechanisms.

Additionally, companies must comply with robust anti-money laundering and KYC obligations. These include implementing customer due diligence processes, monitoring suspicious transactions, and reporting such activities to the AMLU promptly. These measures aim to prevent the misuse of blockchain and cryptocurrency platforms for illicit activities, adding another layer of operational responsibility for companies in this space.

Overall, these regulations ensure market stability and consumer protection but require companies to navigate a complex compliance landscape, adapt their operations, and invest in systems to meet legal standards.

Strategies to Navigate Regulations:

Engage Early with Regulators. Proactively consult with the CBE and FRA to understand licensing requirements and secure necessary approvals before launching operations.

Strengthen Compliance Programs. Develop robust AML and KYC systems to meet regulatory expectations, including enhanced due diligence for high-risk customers and periodic updates to compliance protocols.

Adopt Best Practices for Data Security. Implement secure blockchain solutions that align with FRA Decision No. 140 of 2023, emphasizing data protection, digital identity verification, and secure contracting processes.

Leverage Local Partnerships. Collaborate with authorized entities such as "Meeza" to facilitate compliance and gain access to the domestic financial ecosystem.

Monitor Regulatory Updates. Stay informed about evolving regulations and adjust business strategies to ensure ongoing compliance.

Educate Stakeholders. Conduct training programs for staff, clients, and partners to raise awareness about compliance requirements and minimize operational risks.

By navigating these regulatory frameworks effectively, cryptocurrency and blockchain companies can mitigate risks, build trust with regulators and customers, and foster sustainable growth in Egypt's highly regulated financial environment.

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?

Under Egyptian law, cryptocurrency companies must operate within the frameworks established by the CBE and the FRA. Although tax laws specific to digital assets are not yet fully developed, companies can take the following measures to ensure compliance with existing laws and prepare for potential regulatory changes:

Obtain Necessary Licensing. Cryptocurrency companies must secure approval and licensing from the CBE before engaging in any activities involving cryptocurrencies or digital assets, as required by Article 206 of the Banking Law. Operating without such licensing is prohibited and subject to significant penalties.

Maintain Comprehensive Financial Records. Companies should retain detailed records of all transactions, revenues, and expenditures related to digital assets. These records will support accurate tax reporting and compliance with future regulations.

Monitor Regulatory Updates. Actively track updates from the CBE, FRA, and the Egyptian Tax Authority regarding digital assets and tax obligations. Staying informed will help companies adapt to new requirements promptly.

Voluntary Compliance with General Tax Laws. While specific tax laws for digital assets are undeveloped, companies should report revenues and profits from digital asset transactions under existing corporate tax and income tax laws to demonstrate good faith compliance.

Develop Internal Compliance Programs. Implement systems to ensure adherence to AML and KYC requirements, as stipulated by Egyptian law. This includes monitoring transactions for suspicious activity and reporting such incidents to the AMLU.

Engage with Legal and Tax Professionals. Seek guidance from experts familiar with Egyptian law and digital asset taxation to ensure proper interpretation of existing rules and readiness for upcoming regulations.

Avoid Unauthorized Activities. Cryptocurrency companies should not engage in unlicensed activities, such as issuing or trading cryptocurrencies, until explicitly permitted under Egyptian law.

Prepare for Future Obligations. Proactively establish systems and frameworks for tracking and reporting taxable activities involving digital assets. This will position companies to comply quickly when specific tax regulations are introduced.

While Egypt's tax laws for digital assets remain underdeveloped, cryptocurrency companies are required to adhere to existing regulatory frameworks established by the CBE and FRA. Companies should maintain transparent records, comply with general tax principles, and stay informed about evolving laws to ensure full compliance and minimize legal risks. Engaging with legal and tax professionals is essential to navigate this complex regulatory landscape effectively.

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 Egypt must address data privacy and protection regulations in compliance with the **FRA Decree No. 140 of 2023** and the **Data Protection Law No. 151 of 2020** (**"Data Protection Law"**).

According to the FRA Decree, blockchain systems are decentralized databases where transaction restrictions are agreed upon by peer-to-peer network members. These systems can be public, private, permissioned, or non-permissioned and may involve tokenized or non-tokenized crypto assets. Blockchain technology, with its chronologically serialized blocks secured through cryptographic methods, offers transparency and security.

Under the Data Protection Law, companies must comply with the following obligations regarding personal data:[25]

1. Collect personal data only for legitimate, defined purposes and ensure the data subject is aware of these purposes.
2. Ensure personal data is valid, accurate, and secured against breaches or unauthorized access.
3. Process personal data lawfully and solely for the purposes for which it was collected.
4. Retain personal data only for the duration necessary to fulfill its intended purpose.

For sensitive personal data, such as health, financial, or

biometric data, companies must obtain explicit written consent from the data subject and authorization from the yet-to-be-established data protection center.

Practical Measures for Blockchain Companies:

Data Anonymization and Encryption. Use encryption and anonymization techniques to protect personal data on public blockchains.

Permissioned Blockchain Networks. Consider using permissioned blockchains to restrict access to personal data and ensure compliance with consent requirements.

Off-Chain Data Storage. Store sensitive personal data off-chain with robust safeguards and process it in accordance with the Data Protection Law.

Obtain Consent and Authorization. Ensure data subjects provide explicit consent for processing their data, especially sensitive data.

Balancing Transparency and Privacy:

Blockchain technology inherently promotes transparency by recording transactions on a publicly accessible ledger. However, companies can implement privacy-preserving technologies, such as pseudonymization, zero-knowledge proofs, or selective data sharing, to meet privacy obligations while maintaining the benefits of transparency.

By adhering to these measures, blockchain companies can align with Egyptian regulations while leveraging blockchain technology's strengths in transparency and security.

Footnote(s):

[25] Article (3) of the Data Protection Law No. 151 of 2020.

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?

U.S. immigration policies, particularly the H-1B and L-1 visa programs, have an indirect impact on Egyptian Fintech companies by influencing global talent dynamics, international collaboration, and investment decisions.

Global Talent Competition:

Attracting Top Talent. U.S. immigration policies, such as the H-1B visa, draw skilled tech professionals globally, intensifying competition for top-tier talent. This can make it challenging for Egyptian Fintech companies to attract and retain highly qualified professionals.

Recruitment Challenges. The preference of skilled workers for opportunities in the U.S. reduces the global talent pool, limiting the availability of experienced professionals for Egyptian companies.

Impact on Global Companies Investing in Egypt:

Investment Decisions. If global companies with operations in Egypt face difficulties hiring or relocating talent due to restrictive U.S. policies, this may influence their investment strategies and local operations.

Knowledge Sharing and Mobility. Restrictions on U.S. work visas may hinder the mobility of personnel between U.S. and Egyptian operations of multinational firms, affecting talent transfer and cross-border knowledge exchange.

International Collaboration and Partnerships:

U.S. immigration policies can create barriers to talent exchange between U.S. and Egyptian Fintech companies, reducing opportunities for joint ventures, partnerships, and global knowledge sharing.

Indirect Benefits to Egyptian Fintech Companies:

Talent Retention. U.S. immigration restrictions could encourage skilled professionals to seek opportunities locally, strengthening the talent pool available to Egyptian Fintech companies.

Knowledge Transfer. Returning professionals or expatriates may bring global expertise and innovative ideas, enhancing local capabilities and helping Egyptian companies adopt best practices.

Enhanced Reputation. A diverse and skilled workforce can improve the global reputation of Egyptian Fintech firms, attracting foreign investment and boosting growth prospects.

Economic Contribution. International talent contributes to the local economy through spending, job creation, and skill sharing with local employees.

While U.S. immigration policies may create challenges for Egyptian Fintech companies by intensifying global talent competition and limiting international collaboration, they can also present opportunities to strengthen the local talent pool and stimulate the local economy. By strategically leveraging these dynamics, Egyptian Fintech

companies can enhance their competitive edge and build a globally recognized workforce.

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?

Fintech companies entering the Egyptian market must comply with a range of laws and regulations that govern financial, technological, and data-related activities. These include:

- **Fintech Law**: Regulates Fintech use in the non-banking sector, covering areas such as real estate funding, SMEs, microfinance, financing leasing, factoring and consumer financing.
- **Banking Law**: Governs Fintech businesses operating in the banking sector, requiring companies to obtain licenses from the CBE.
- **The FRA Decrees**: Provide detailed guidelines for non-banking financial activities.
- **Non-Cash Payment Law No. 18 of 2019**: Promotes the adoption of electronic payment methods.
- **Telecommunications Law No. 10 of 2003**: Regulates the use of telecommunications infrastructure.
- **E-Signature Law No 15. of 2004**: Governs the validity and use of electronic signatures in business transactions.
- **Data Protection Law:** Imposes requirements on the collection, processing, and storage of personal data.
- **Cybercrimes Law No. 175 of 2018**: Focuses on cybersecurity and regulates activities of internet service providers.
- **Egyptian Trade Law. 17 of 1999 and Companies Law No. 159 of 1981**: Establish the legal framework for commercial and corporate operations.
- **AML Law No. 80 of 2002**: Requires robust anti-money laundering measures.

Furthermore, to ensure adherence to these laws and regulations, Fintech companies should:

FRA and CBE Licenses. Secure licenses from the FRA (for non-banking Fintech activities) or the CBE (for banking-related activities).

AML and KYC. Implement robust AML and KYC systems to monitor transactions and comply with reporting obligations.

Engage with Regulatory Authorities. Obtain necessary licenses and approvals from the CBE and FRA, particularly if the company plans to operate in regulated sectors such as banking or non-banking financial services.

Leverage Regulatory Sandboxes. Participate in sandbox initiatives provided by the CBE or FRA to test innovative technologies in a controlled regulatory environment.

Build a Comprehensive Compliance Framework. Implement systems to monitor and meet obligations under key laws, such as customer due diligence for AML compliance or data protection measures for personal information handling.

Stay Updated with Regulatory Changes. Regularly monitor updates to laws, decrees, and guidelines from the CBE and FRA to avoid inadvertent non-compliance.

Adopt Technology Solutions. Use compliance tools and software to automate regulatory reporting and risk management processes, reducing the likelihood of errors.

Foster Relationships with Legal Experts. Partner with legal professionals who specialize in Egyptian Fintech regulations to address complex legal requirements and ensure comprehensive compliance.

By addressing these requirements and leveraging local resources such as sandboxes and compliance expertise, Fintech companies can navigate Egypt's regulatory landscape effectively and achieve long-term success.

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?

To effectively establish a presence in the Egyptian market, Fintech companies could take the following steps:

Understand the Target Customer Demographics

One of the key customer demographics in Egypt's is its burgeoning youthful population. Combined with increasing digital literacy and smartphone penetration, the youth segment presents a prime opportunity for Fintech companies. By focusing on Digital Financial Services ("**DFS**"), Fintechs can effectively tap into this demographic and drive financial inclusion.

A strategic market entry approach should prioritize the development of innovative solutions that cater to the

unique needs of young Egyptians. These solutions could include mobile payment apps, digital lending platforms, and insurance products accessible through mobile devices.

Leveraging partnerships with telecommunication providers and banks can accelerate market penetration and ensure seamless integration with existing financial systems. Furthermore, by adhering to regulatory guidelines and implementing robust cybersecurity measures, Fintech companies can build trust and confidence among young consumers. Ultimately, a successful market entry strategy in Egypt shall require a deep understanding of local cultural nuances, a commitment to customer experience, and a focus on providing accessible, affordable, and secure financial services.[26]

Another key customer demographic is Egypt's vibrant SMEs sector. While a cornerstone of its economy, SMEs have historically faced significant challenges in accessing adequate financing.

Fintech companies can revolutionize this landscape by leveraging technology to streamline lending processes, reduce operational costs, and expand financial access. By developing innovative digital lending platforms, Fintechs can offer tailored financial solutions to SMEs, addressing their specific needs and risk profiles. These solutions can range from working capital loans to equipment financing, enabling SMEs to invest in growth, create jobs, and contribute to economic development. Collaborating with traditional financial institutions can further amplify the impact of Fintechs by combining their technological expertise with the established networks and regulatory compliance of banks. A successful market entry strategy in Egypt should prioritize customer-centricity, regulatory compliance, and strategic partnerships to ensure long-term sustainability and growth.[27]

Understand How to Navigate Competitive Landscapes

The Egyptian Fintech ecosystem has witnessed significant growth in the recent years, with over 177 startups and Payment Service Providers ("**PSPs**") operating across fourteen (14) sub-sectors.[28]

However, this rapid growth has also led to increased competition from established players, such as Fawry, Halan, Instapay, Valu, and Vodafone Cash.

To successfully navigate this competitive landscape, Fintech companies entering the Egyptian market shall adopt a strategic approach. This includes identifying specialized market segments, offering innovative solutions, and forming strategic partnerships with established players and government entities. Additionally, prioritizing customer experience, leveraging technology, and ensuring regulatory compliance are crucial for long-term success.

Comprehend How to Localize Fintech Offerings

To successfully localize a Fintech offering in Egypt, it's essential to understand local cultural nuances, regulatory landscape, and customer preferences. This involves translating materials into Arabic, supporting local currencies and payment methods, and building strong partnerships with local financial institutions. Prioritizing mobile-first design, leveraging AI and machine learning, and focusing on financial inclusion by targeting underserved segments are crucial strategies. By adapting to the local market, Fintech companies can build trust, credibility, and long-term success in Egypt.

Leverage Strategic Partnerships

Strategic partnerships can significantly enhance a Fintech company's growth and market position. By collaborating with banks, telecom providers, e-commerce platforms, and other Fintech companies, Fintechs can access a wider customer base, share resources and infrastructure, improve brand visibility, navigate regulatory complexities, and mitigate risks. These partnerships can accelerate growth, reduce costs, and enhance the overall value proposition to customers.

Footnote(s):

[26] AFI Youth Financial Inclusion Policy Framework.

[27] https://www.codebtech.com/bridging-the-sme-financing-gap-by-leveraging.

[28] Fintech Egypt releases the 3rd edition of Egypt's landscape report 2023.

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?

Financial and operational risks may pose challenges to the expanding Fintech market in Egypt. As this dynamic sector continues to evolve, it faces a range of uncertainties that have the potential to impact its path. It is crucial for industry participants, regulatory bodies, and

stakeholders to understand these risks and adopt effective mitigation strategies essential for establishing a sustainable presence in this dynamic market.

Financial Risks

1. Funding and Capital Allocation

Fintech companies entering Egypt may face challenges in securing sufficient funding to support market entry and scaling. Inefficient allocation of resources, coupled with overestimating the market's immediate potential, can lead to financial strain. Diversifying funding sources, such as partnering with venture capital firms, leveraging government programs, and building relationships with local investors, is critical. Conducting feasibility studies and implementing lean operations can further optimize resource utilization.

2. Currency Volatility and Inflation

Egypt's economy is susceptible to currency fluctuations and inflation, which can increase operational costs and affect pricing strategies. These economic factors may also impact the affordability of services for target demographics. To address this issue, Fintech companies should consider financial hedging strategies, price their products and services in the local currency, and monitor economic indicators to adjust their operations proactively.

3. Payment Processing Challenges

A significant portion of Egypt's population relies on cash transactions, particularly in rural areas. This dependence on cash creates barriers to adopting digital financial services, reducing potential revenue streams. Fintech companies should focus on urban areas for initial market penetration and gradually expand to underserved regions. Partnering with local banks, mobile operators, and government programs can also help overcome these challenges.

Operational Risks

1. Regulatory and Compliance Challenges

Egypt's regulatory landscape for Fintech is evolving, with key frameworks like the Fintech Law and the Banking Law requiring companies to secure licenses from the FRA and CBE. In addition, non-compliance with laws such as the Data Protection Law and AML Law can result in penalties and operational disruptions. Companies must engage legal experts to navigate these regulations, maintain open communication with regulators, and participate in regulatory sandboxes to test their innovations in controlled environments.

2. Cybersecurity Threats

Handling sensitive financial and personal data makes Fintech companies attractive targets for cyberattacks, including hacking, data breaches, and ransomware. To mitigate these threats, firms must invest in advanced cybersecurity frameworks, implement encryption and multi-factor authentication, and conduct regular security audits. Training employees on cybersecurity best practices is equally essential to reduce risks.

3. Competition from Established Players

The Egyptian Fintech ecosystem includes prominent players, such as Fawry and Vodafone Cash, creating a highly competitive environment. New entrants must identify niche markets or underserved customer segments to differentiate themselves. Offering innovative solutions, such as AI-driven financial tools, blockchain-based payment systems, or embedded finance, can help Fintechs establish a competitive edge.

4. Infrastructure and Connectivity Issues

Limited digital infrastructure in rural areas poses a significant challenge to expanding digital financial services. Fintech companies should focus on solutions that work in low-connectivity environments, such as USSD-based platforms. Partnering with telecommunications providers to improve access and investing in scalable infrastructure can help bridge the gap.

In conclusion, entering Egypt's Fintech market requires navigating a complex mixture of financial and operational risks, including funding challenges, regulatory compliance, cybersecurity threats, and competition. By adopting a proactive approach that includes building partnerships, fostering trust, and tailoring services to local needs, Fintech companies can overcome these hurdles. With the right strategies, Fintechs can tap into Egypt's growing digital ecosystem, drive financial inclusion, and achieve sustainable growth.

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

Non-Banking Sector

Under Article (3) of the Fintech Law, Fintech companies cannot operate their activities, whether inside, or outside Egypt for residents or entities conducting activities in

Egypt, without obtaining a license from the FRA. However, licensed companies engaging in non-banking financial activities may outsource these activities to registered outsourcing service providers in Egypt, subject to FRA approval.[29]

In this respect, **FRA Decree No. 141 of 2023** establishes the Outsourcing Service Providers Registry for entities offering outsourcing services. Only entities listed in this registry are authorized to provide outsourcing services. Notably, the FRA decree does not specify whether the registered entities are permitted to provide outsourcing services solely within Egypt or extend their services to offshore locations. Companies listed in this registry must meet stringent requirements, including:

- Being an Egyptian joint stock company or committing to convert to one within 12 months of registration.
- Meeting minimum capital requirements set by the FRA.
- Possessing relevant expertise in their field.
- Implementing robust governance policies to ensure strong internal controls.
- Demonstrating sufficient technological capabilities to protect customer data and maintain confidentiality.

As a result of this regulation, four registered companies have entered into agreements with approximately 40 non-banking financial institutions, with additional agreements underway. Therefore, while outsourcing is permitted in the non-banking sector, it must comply with the Fintech Law and FRA requirements, ensuring oversight and data protection.[30]

Banking Sector

In the banking sector, the Banking Law prohibits banks from outsourcing services to unregistered providers. Banks that engage with unregistered entities remain fully accountable for any issues arising from these collaborations.[31] The CBE closely monitors compliance with this regulation to ensure quality and security in outsourced banking services.

Footnote(s):

[29] Article (5) of the Fintech Law.

[30] https://sis.gov.eg/Story/279776/%D8%B1%D8%A6%D9%8A%D8%B3-%D9%87%D9%8A%D8%A6%D8%A9-%D8%A7%D9%84%D8%B1%D9%82%D8%A7%D8%A8%D8%A9-%D8%A7%D9%84%D9%85%D8%A7%D9%84%D9%8A%D8%A9-%D9%8A%D8%B4%D8%A7%D8%B1%D9%83-%D9%81%D9%8A-%D9%85%D8%A4%D8%AA%D9%85%D8%B1-%D8%A5%D9%8A-%D8%A7%D9%81-%D8%AC%D9%8A-%D9%87%D9%8A%D8%B1%D9%85%D9%8A%D8%B3-%D8%A7%D9%84%D8%A7%D8%B3%D8%AA%D8%AB%D9%85%D8%A7%D8%B1%D9%8A-%D9%81%D9%8A-%D9%84%D9%86%D8%AF%D9%86?lang=ar

[31] Article (96) of the Banking Law.

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 providers can safeguard their intellectual property (**IP**) rights by leveraging the encompassing legal framework provided by the **Intellectual Property Law No. 82 of 2002** (the "**IP Law**"). This protection becomes effective upon official registration with the competent intellectual property office or through publication. Indeed, Fintech companies can use a combination of patent protection, copyright, and trade secret protections to comprehensively secure their proprietary algorithms and software, depending on the nature of their innovations.

Patent Protection

By interpreting the provisions of the IP Law, proprietary algorithms and software could be eligible for patent protection if they demonstrate novelty, creativity, and industrial applicability. However, abstract ideas or purely mathematical methods shall not qualify without a clear technical application.[32] Further, a patent grants the owner the right to prevent others from exploiting the invention in manner. It is important to note, however, that the patent owner's right to restrict others from importing, using, selling or distributing the patented product is exhausted if the patent owner markets it in any country or authorizes others to do so.[33] Fintech companies must thoroughly evaluate whether their innovations satisfy these criteria or not.

Trade Secret Protections

Trade secrets offer an effective method to protect information related to proprietary algorithms and software. Under IP Law, information qualifies as a trade secret if they meet the following requirements:[34]

- It is confidential and is not generally known or common within the scope of which the information falls.
- It derives its commercial value from its secrecy.

- It depends on the effective measures taken by the person lawfully in control of it to keep it confidential.

Implementation strategies of trade secrets may include using non-disclosure agreements (NDAs) with employees, contractors, and third parties to maintain confidentiality, restricting unauthorized access to sensitive data, encrypting software code and securing storage systems to protect against data breaches, and maintaining internal policies to ensure employees understand and adhere to confidentiality requirements.

Copyright Protection

Copyright provides automatic protection for the source code and object code of software from the moment of their publication, treating them as literary works under the IP Law.[35] Copyright also extends to associated creative elements such as user interfaces (UI) and design layout. While formal registration is not required, it strengthens the ability to enforce rights in case of disputes.

Combining Patents, Copyrights, and Trade Secrets

Fintech companies can adopt a layered approach to protect different aspects of their software and algorithms:

- Patents for technical innovations and processes that meet the required criteria.
- Copyright for the source code, user interfaces, and design layout.
- Trade secrets for confidential implementation details, optimization techniques, and training data.

This holistic approach maximizes protection by combining the strengths of each IP mechanism while addressing potential gaps in coverage.

Technological Safeguards

To further secure proprietary algorithms and software, Fintech companies should employ advanced technical measures, such as using encryption to prevent reverse engineering, implementing blockchain, deploying real-time monitoring tools, and continuously update software to address vulnerabilities and maintain security. Finally, clear contractual agreements are critical to safeguarding intellectual property when working with third parties or licensing proprietary software.

In essence, Egyptian Fintech companies can shield their proprietary algorithms and software by establishing a proprietary framework combining trade secret protections, patent applications and robust technical protective mechanisms. With a strategic combination of secure coding, unequivocal legal agreements, and regulatory compliance, Fintech companies can effectively protect their intellectual property and prosper in Egypt's competitive landscape.

Footnote(s):

[32] Articles (1) and (2) of the Intellectual Property Law No. 82 of 2002.

[33] Article (10) of the Intellectual Property Law No. 82 of 2002.

[34] Article (55) of the Intellectual Property Law No. 82 of 2002.

[35] Article (163) of the Intellectual Property Law No. 82 of 2002.

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

To protect its brand identity and safeguard its trademarks and service marks in Egypt, a Fintech company should ensure their trademarks are registered with the relevant authorities. As per the IP Law, registration bestows a ten (10)-years protection period, with the option for extension upon the owner's request. The registered trademark is duly published in an official Gazette, marking its formal acknowledgment. Trademark owners, armed with registration, hold the right to prevent unauthorized usage, sale, distribution, or other forms of exploitation. In the event of infringement, owners can file claims before the competent court, seeking prohibitory measures. Penalties for trademark infringement may involve imprisonment and/or fines.[36]

Fintech innovators are strongly encouraged to promptly register their trademarks to harness the full scope of its legal protections, creating a secure environment for the flourishing of their inventive creations.

Footnote(s):

[36] Article (48) of the Intellectual Property Law No. 82 of 2002.

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?

Implications of Using Open-Source Software

There is no specific law in Egypt that explicitly regulates free and open-source software ("**OSS**") as a distinct category. The use of OSS in Egypt could be governed by general laws related to intellectual property, cybersecurity, data protection, and sector-specific regulations, as open-source licenses could be treated as binding contracts under Egyptian law.

In light of the above, the use of open-source software in Fintech products presents a range of impacts, both beneficial and challenging, that companies must carefully navigate. OSS allows Fintech companies to access, modify, and distribute source code under specific licensing terms, promoting flexibility, cost savings, and innovation. This flexibility enables Fintechs to develop customized solutions tailored to specific market needs, enhancing their ability to adapt to rapidly evolving industry demands. Additionally, OSS fosters collaboration and innovation by leveraging global developer communities to improve and maintain software, reducing the time and resources required for development.

However, using OSS also introduces certain legal, operational, and compliance risks. One key impact is the need to comply with open-source licenses, such as GPL or MIT, which impose obligations like providing proper attribution, sharing modifications, and adhering to redistribution conditions. Non-compliance with these terms can lead to copyright infringement claims or legal disputes. Security is another critical consideration, as OSS, while transparent, may introduce vulnerabilities if not properly maintained or updated. Fintech companies must implement robust security measures to address these risks and comply with regulations like the Cybercrimes Law and Data Protection Law.

OSS also affects intellectual property management. While the software itself is protected under IP laws, the licensing terms may limit the company's ability to claim proprietary rights over modified or integrated software. Fintech companies must carefully evaluate the terms of OSS licenses to safeguard their IP interests. Additionally, operational reliance on OSS may require companies to develop in-house expertise or engage third-party support to manage, maintain, and secure the software effectively.

Ensuring Compliance with Open-Source Licensing Agreements

Ensuring compliance with open-source licensing agreements is critical for companies using OSS to avoid legal risks and maintain operational integrity. The first step is to thoroughly understand the terms of each OSS license. Common licenses, such as GPL, MIT, and Apache, come with varying obligations, such as providing attribution to the original creators, sharing modifications under the same license (for copyleft licenses), or restricting integration with proprietary software. Reviewing these terms is essential before incorporating OSS into any product or service.

Companies should maintain a detailed inventory of all OSS components used in their operations, along with their associated licenses. This inventory should be updated regularly, ensuring that no license terms are overlooked. Alongside this, businesses must establish clear internal policies for OSS usage, modification, and redistribution. These guidelines should be communicated to all employees and contractors to ensure consistent compliance.

Implementing formal compliance processes is also crucial. Companies should vet all OSS components before use, ensuring their licenses align with the company's business model and operational requirements. Proper attribution to the original developers must always be provided as required by the license, and any modifications or derivative works should be shared under the specified terms if the license mandates it.

Regular audits are essential to verify that OSS usage adheres to licensing terms. These audits can identify compliance gaps early, preventing potential legal disputes. Additionally, companies distributing products containing OSS must bundle license texts, provide source code when required, and notify users of their rights under the license. Training programs for developers, legal teams, and other stakeholders can further enhance awareness and understanding of OSS compliance.

By adopting these measures, companies can effectively manage OSS usage while minimizing risks. A proactive approach, combining legal diligence, robust internal policies, and technical tools, allows businesses to leverage OSS benefits while ensuring full compliance with licensing agreements.

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

Managing intellectual property ownership is a critical aspect of collaborations between Fintech startups and third-party developers or partners. To address the

complexities of ownership and ensure smooth cooperation, Fintech companies should adopt a multi-faceted strategy that includes clearly defined legal agreements, proactive operational measures, and robust governance frameworks.

At the outset, companies should formalize IP ownership through well-drafted contracts that outline the rights and obligations of each party. These agreements should specify ownership over any pre-existing assets, such as proprietary software or algorithms, as well as new derived IP or IP developed during the collaboration. For example, agreements may include clauses such as:

> *"All intellectual property created during the course of this collaboration shall be owned exclusively by [Party A]."*

> *"Any modifications, extensions, or derivative works based on pre-existing IP contributed by [Party B] shall remain the property of [Party B], unless explicitly agreed otherwise in writing."*

> *"Each party retains exclusive ownership of their pre-existing intellectual property, as detailed in Schedule A, which is incorporated into this agreement."*

Clauses covering licensing terms, usage rights, and restrictions should also be included to prevent unauthorized use or distribution of sensitive innovations. For instance, a licensing clause may state:

> *"The license granted to [Party B] for use of [Party A]'s pre-existing software is non-exclusive, non-transferable, and valid solely for the duration of the project."*

In addition to contractual clarity, startups should implement operational safeguards to protect their IP. These include securing software repositories, limiting access to sensitive information, and ensuring that third-party developers sign non-disclosure agreements (NDAs). Work-for-hire clauses are particularly effective in ensuring that any IP created by contractors is automatically assigned to the Fintech company. For example:

> *"All intellectual property created by the contractor during the engagement shall be deemed work-for-hire and will be assigned exclusively to [Party A] upon creation."*

To avoid potential disputes, companies should establish processes for resolving conflicts over IP ownership, such as mediation or arbitration. Furthermore, exit strategies should be clearly defined in the agreement, outlining how IP rights will be managed in the event of partnership termination.

By combining legal measures, operational controls, and clear governance, Fintech startups can effectively navigate the complexities of IP ownership, safeguard their innovations, and build successful partnerships.

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?

Fintech companies should adopt a comprehensive strategy to prevent and address potential IP infringements, aligning with the provisions of Egyptian law, including the IP Law, and leveraging international frameworks where applicable. Here are some key steps:

1. Register patents, copyrights and trademarks to secure legal recognition and protection for proprietary technology, software, and branding. This provides a basis for enforcement in case of infringement.
2. Use NDAs to safeguard trade secrets when dealing with employees, contractors, and partners. These agreements should clearly define confidential information and outline penalties for breaches.
3. Apply international strategies for Fintech companies operating internationally:
    - Utilize the **Paris Convention** to file a patent application in one member country and claim priority in others within a certain timeframe[37].
    - Employ **Patent Cooperation Treaties** (**PCTs**) for streamlined patent filing across multiple countries.
    - Consider regional patent systems like the **African Regional Intellectual Property Organization** (**ARIPO**) for efficient IP registration and protection within member states.[38]
    - Use the **Madrid System** for international trademark registration, enabling streamlined applications across multiple jurisdictions.
4. Ensure compliance with Egyptian laws that impose various penalties on those who infringe IP rights. Such measures are designed to protect the rights of IP owners.[39] Companies must understand the enforcement mechanisms, including litigation and administrative complaints through entities like the newly established **Egyptian Authority for Intellectual Property** (**EIPA**).[40]
5. Actively monitor the market for unauthorized use of IP and take action through negotiations or legal proceedings to address infringements effectively.

In light of the foregoing, by implementing these proactive measures, Fintech companies can significantly reduce the risk of IP infringement and protect their valuable assets.

Footnote(s):

[37] Paris Convention for Protection of Industrial Property; https://www.wipo.int/treaties/en/ip/paris/summary_paris.html.

[38] African Regional Intellectual Property Organization; https://www.aripo.org/.

[39] Intellectual Property Law No. 82 of 2002.

[40] https://beta.sis.gov.eg/en/egypt/culture/cultural-institutions/egyptian-authority-for-intellectual-property/.

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?

Non-banking Sector

Fintech companies leveraging AI algorithms for credit scoring and lending decisions must adhere to legal principles of transparency, fairness, and accountability. Although there is no dedicated legislation for AI fairness, existing frameworks, such as **FRA Decree No. 139 of 2023**, provide indirect guidance through their focus on technological infrastructure and security requirements. The Decree defines "**Information Systems**" as systems consisting of databases and applications, including AI applications, designed to support business operations, improve automation, and enhance accuracy and speed. It also defines "**Protection & Security Mechanisms**" as methodologies and tools used to prevent technological risks that could compromise the confidentiality, integrity, and availability of Information Systems, infrastructure, and data.[41] Therefore, AI algorithms, as part of Information Systems, must comply with the following Protection & Security Mechanisms:[42]

1. **Next-Generation Firewall (NGFW).** Protects networks and information from unauthorized access, ensuring that data used in AI systems remains secure and unaltered during transmission.
2. **Web Application Firewall (WAF).** Safeguards web-based AI systems, preventing unauthorized access to applications or data that could skew AI outputs.
3. **Data Encryption.** Ensures that data input into AI algorithms is encrypted according to global standards, protecting it from tampering or unauthorized disclosure.
4. **Activity Logging and Transaction Records.** Logs all activities and system events, creating an audit trail that can verify the integrity of AI algorithm decisions, such as credit scoring outcomes. These records must be retained for at least five (5) years.
5. **Security Isolation.** Segments AI systems from other services based on security levels, reducing the risk of unauthorized interference or contamination from other systems.
6. **Penetration Testing.** Conducted annually to identify and mitigate vulnerabilities in AI systems, ensuring robust defenses against potential cyber threats that might compromise fairness or transparency.
7. **Incident Reporting.** Mandates reporting of any security incidents affecting AI systems to the FRA, ensuring accountability and prompt resolution.
8. **Regular Updates and Maintenance.** Requires periodic updates to operating systems, applications, and AI algorithms to fix vulnerabilities and improve functionality, ensuring accurate and reliable operations.

How These Mechanisms Ensure Transparency and Fairness

Data Integrity and Accuracy: Firewalls and encryption ensure that data input to AI algorithms is secure and unaltered, maintaining the integrity of credit scoring and lending decisions.

Auditability: Activity logging and transaction records allow Fintechs to trace every decision made by AI systems, enabling transparent reviews in case of disputes or audits.

Bias Detection: Regular penetration testing and system updates help identify and mitigate potential biases or errors in AI algorithms, ensuring fair treatment of all customers.

Accountability: Security incident reporting ensures that any breaches or malfunctions are promptly addressed, minimizing the risk of inaccurate or unfair outcomes.

Data Privacy: Encryption and isolation protect customer data used in AI algorithms, aligning with privacy laws and fostering trust in Fintech services.

By adhering to the outlined in aforementioned FRA

Decree, Fintech companies can ensure that their AI algorithms operate securely, transparently, and fairly. These measures not only enhance the accuracy and reliability of AI-driven decisions in credit scoring and lending but also build trust with customers and regulators, ensuring compliance with legal and ethical standards.

On another note, Egypt's **National AI Strategy (2025-2030)** complements the FRA Decree by emphasizing responsible and ethical AI deployment across industries, including Fintech. The strategy highlights principles of transparency, fairness, and accountability in AI systems, aligning directly with the need for unbiased and explainable decision-making in credit scoring and lending. It prioritizes data privacy and security, ensuring compliance with frameworks such as the Data Protection Law and emphasizing the importance of protecting sensitive customer information. Additionally, the strategy's focus on governance underscores the need for regular audits and oversight of AI algorithms to prevent bias and maintain accuracy. By promoting fairness, ethical standards, and innovation, the strategy supports Fintech companies in meeting regulatory requirements while fostering trust and inclusion in financial services.[43]

Banking Sector

Banks employing AI algorithms for credit assessment and lending must comply with strict regulations to ensure transparency, fairness, and accountability in their operations. These obligations include adhering to existing laws, reporting any significant violations to the CBE, implementing robust governance and internal controls, and maintaining a transparent and trustworthy relationship with the CBE.[44]

In this regard, banks shall establish credit rules for its customers, including procedures for verifying creditworthiness, the accuracy of the information provided, and the procedures for granting credit and monitoring its usage. [45] By aligning AI systems with these regulatory expectations, banks can enhance efficiency in credit assessments while maintaining trust and compliance with the CBE's standards.

Ensuring AI Systems Are Free from Bias and Discrimination

To ensure the fairness and accuracy of AI systems, it is crucial to address potential biases in the training data. One common strategy is to re-weight the data, using techniques like over-sampling or under-sampling to mitigate class imbalances.

To enhance the transparency and accountability of AI systems, it is essential to document the algorithms and decision-making processes. Regular audits and testing should be conducted to identify and address potential biases within the algorithms. Additionally, developing techniques to explain the reasoning behind AI decisions can increase trust and transparency.

To mitigate potential risks and ensure ethical AI practices, it is crucial to implement human oversight to review and correct AI-generated decisions, especially in high-stakes scenarios. Additionally, establishing clear accountability mechanisms is essential for identifying and addressing issues related to AI bias and discrimination.

To ensure ethical AI practices, it is crucial to align AI systems with ethical guidelines and principles, such as those outlined in the Egyptian Charter for Responsible AI.[46]

To foster a collaborative and regulatory-friendly environment for AI development, it is crucial to actively engage with the CBE and other relevant regulatory bodies to discuss AI-related challenges and seek guidance. Additionally, collaborating with other Fintech companies and industry associations can help develop best practices and advocate for fair AI.

Footnote(s):

[41] Article (1) of FRA Decree No. 139 of 2023.

[42] Article (2) of FRA Decree No. 139 of 2023.

[43] AIstrategy Arabic 16-1-2025-1.pdf.

[44] Article (83) of the Banking Law.

[45] Article (99) of the Banking Law.

[46] https://mcit.gov.eg/en/Media_Center/Press_Room/Press_Releases/66939

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?

The development of proprietary AI models by Fintech companies introduces unique intellectual property challenges and opportunities. In Egypt, the existing IP

framework could provide protections for AI technologies, but gaps remain, especially concerning AI-generated works. Below are key considerations and strategies for protecting AI innovations and managing the use of third-party AI tools.

Protecting Proprietary AI Models

Fintech companies can safeguard their proprietary AI models and data sets by leveraging Egypt's IP Law as follows:

- **Patents:** AI processes or models meeting patentability criteria of novelty, inventiveness, and industrial applicability can be patented under the IP Law. However, AI itself cannot be recognized as an inventor due to the lack of legal personality, leaving AI-generated inventions unprotected.
- **Trade Secrets:** AI training data and information can be protected as trade secrets through confidentiality agreements, restricted access, and robust security measures.
- **Copyrights:** The software code underlying AI models qualifies for protection as a literary work under the IP Law, though the outputs generated by AI may not be eligible for the same protection.
- **Trademarks:** AI-driven products or services can be branded and protected through trademarks, enhancing their market identity.

Using Third-Party AI Tools

When Fintech companies use third-party AI tools, they must address specific legal and operational considerations. For instance, companies should carefully review licensing terms to avoid violating restrictions on usage, modification, or distribution. Additionally, contracts must clearly define the ownership of outputs generated using third-party AI tools to prevent future disputes. Companies must also safeguard proprietary and customer data when integrating third-party tools, ensuring compliance with Egyptian data protection laws. Finally, companies shall verify whether third-party tools align with local laws, including cybersecurity and financial regulations, to avoid operational and legal risks.

Future Implications for AI and IP in Egypt

The Artificial Intelligence National Council (**AINC**), established by Prime Ministerial Decree No. 2889 of 2019, oversees Egypt's national AI strategy. It coordinates the development and governance of AI in collaboration with experts and stakeholders. The AINC's efforts, combined with the CBE's initiatives to train Fintech professionals in AI, indicate a growing emphasis on aligning Egypt's regulatory framework with global AI advancements.

Egypt is expected to address the intersection of AI and IP laws more comprehensively in the coming years. Efforts to establish a dedicated AI law could resolve ambiguities around AI-generated works and patentability. These advancements would provide clearer protections for Fintech companies developing proprietary AI models, fostering innovation and legal certainty.

In conclusion, although Egypt's IP Laws does not yet fully address the complexities of AI, Fintech companies can protect their proprietary technologies through patents, trade secrets, copyrights, and trademarks. Companies must remain vigilant about legislative updates while addressing challenges like ownership ambiguity and the use of third-party tools. By adhering to existing laws and engaging with national AI governance efforts led by the AINC, Fintechs can navigate the current landscape while preparing for future advancements in AI-related IP protections.

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?

Financial Regulations for Fintechs Deploying AI Solutions

Fintech companies deploying AI solutions in Egypt must adhere to financial regulations that ensure transparency, fairness, accountability, and data protection. While Egypt does not yet have AI-specific financial regulations, several existing laws, decrees, and frameworks indirectly govern the use of AI in financial services. Additionally, financial regulatory bodies like the CBE and the FRA provide guidelines that affect AI deployment.

Key Financial Regulations Relevant to AI Deployment

- **Banking Law**:
  Requires all financial activities conducted by banks to be transparent, secure, and compliant with governance principles. AI systems must adhere to these standards by ensuring unbiased decision-making and secure data processing.
- **Fintech Law**:
  Governs the use of Fintech solutions in non-banking financial services, emphasizing the need for operational integrity, customer protection, and

compliance with financial laws.

- **Data Protection Law**:
  Mandates explicit consent for processing personal data, which is critical for AI solutions that handle sensitive customer information.
- **Consumer Protection Law No. 181 of 2018**:
  Requires Fintech companies to maintain transparency and fairness in automated decisions, ensuring customers understand how AI affects their financial interactions.
- **FRA Decree No. 139 of 2023**:
  Provides guidelines for technological infrastructure, requiring secure and auditable Information Systems, including AI applications. The FRA emphasizes that AI-driven financial solutions must include robust Protection & Security Mechanisms, such as:[47]
  - Firewalls (e.g., NGFW, WAF) to safeguard data.
  - Activity logging and retention of records for at least five years to ensure auditability.
  - Regular penetration testing to ensure system security.
  - Incident reporting to address breaches promptly.

Ensuring Compliance of AI Applications

To comply with these regulations, Fintechs should:

Adopt Transparent AI Practices:

Ensure that AI decision-making processes are explainable and auditable. This includes documenting how algorithms are trained, tested, and deployed.

Integrate Security Measures:

Implement protection mechanisms, such as encryption, secure data storage, and firewalls, to safeguard customer data and algorithmic operations.

Conduct Regular Audits:

Perform internal and external audits of AI systems to verify compliance with financial and data protection laws, ensuring the systems are free from bias or errors.

Engage Legal and Regulatory Experts:

Work with legal counsel and regulatory consultants to navigate complex compliance requirements and stay updated on evolving laws.

Focus on Data Integrity:

Ensure that data used for training and operating AI solutions is accurate, diverse, and representative, avoiding biases in financial decisions.

Customer Communication:

Clearly inform customers of how AI is used in financial services, particularly in automated decision-making, to align with consumer protection laws.

Finally, Fintech companies deploying AI solutions in Egypt must adhere to a combination of existing financial, data protection, and consumer laws while incorporating guidelines from the FRA and CBE. Ensuring compliance involves implementing transparent and secure AI systems, conducting regular audits, and aligning operations with ethical and regulatory principles. As Egypt's AI regulatory framework evolves, Fintechs should remain proactive in adapting to new guidelines to foster innovation while maintaining trust and accountability in financial services.

Footnote(s):

[47] Article (2) of FRA Decree No. 139 of 2023.

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

AI is essential in developing the Fintech landscape in Egypt. However, the use of AI also exposes Fintech companies to significant legal risks, including issues related to data privacy and protection, intellectual property, cybersecurity, and other issues related to international guidelines. To navigate these risks, Fintech companies must adopt comprehensive risk management strategies, as follows:

- ***Addressing Data Privacy Risks:*** Strong data privacy policies minimize the risk of data breaches and legal actions related to the misuse of personal information. To mitigate potential risk related to personal data arising from the use of AI, Fintech companies shall (a) obtain explicit consent from the personal data owner in order to use the data[48] (b) must not retain the data for a period longer than the period necessary to fulfil the purpose specified for it and (c) comply with the requirements prescribed by the Data Protection Law and its Executive Regulations.[49]
- ***Complying with International Ethical Guidelines:*** The Organization for Economic Co-operation and Development (**OECD**) AI Principles promote the use of AI that is innovative and trustworthy and that respects human rights and democratic values, to which Egypt adhered to in 2021.[50]
- ***Safeguarding AI Intellectual Property****:* Fintech companies shall file for patents and copyrights to

protect AI innovations and clearly define IP ownership in agreements.
- ***Implementing Cybersecurity Measures:*** Fintech companies using AI as service providers, are under the obligation to implement sufficient measures to secure data and information and maintain its confidentiality.[51]

Additionally, strong governance policies are another key strategy for mitigating AI risks. Companies should implement ethical guidelines that outline principles for AI use, focusing on transparency, fairness, and accountability. Regular employee training ensures teams are equipped to handle AI-related risks and adhere to compliance requirements. Contractual safeguards, such as non-disclosure agreements and liability clauses in vendor agreements, further protect sensitive data and allocate responsibility for AI-related risks.

Furthermore, continuous monitoring and adaptation are crucial for long-term risk management. Fintechs should deploy tools to monitor AI performance in real-time, identifying errors that could lead to legal challenges. Updating AI models and security measures regularly ensures compliance with evolving regulations and technological advancements. Establishing internal review processes for customer grievances and utilizing alternative dispute resolution mechanisms like mediation can help resolve disputes efficiently, minimizing litigation risks.

By adopting these strategies, Fintech companies can mitigate legal liabilities associated with AI technologies. A proactive approach that combines compliance, technical safeguards, governance policies, and ongoing monitoring ensures AI applications are secure, fair, and aligned with regulatory expectations, fostering trust and innovation.

Footnote(s):

[48] Article (2) of the Data Protection Law No.151 of 2020.

[49] Article (3) of the Data Protection Law No. 151 of 2020.

[50] https://mped.gov.eg/adminpanel/sharedFiles/OECD_Artificial_Intelligence_Review_of_Egypt_c9a.pdf

[51] Article (2) of Cybercrimes Law No.175 of 2018.

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

There are several strong examples of disruption through Fintech in Egypt, across various areas of the financial services landscape:

***Vodafone Cash (VodaCash)*:** With over 40 million registered users, VodaCash has become a ubiquitous mobile money platform, enabling peer-to-peer transfers, bill payments, and even online shopping, significantly enhancing financial inclusion and convenience.

InstaPay: As a mobile app that enables users to manage their finances directly from their phone, InstaPay can connect bank accounts from different banks to one app, transfer money instantly 24/7, pay bills, and even donate to charities. It's fast, secure, and easy to use.

***ValU*:** As a digital lending platform, ValU uses social networks and transaction data to offer flexible credit options for individuals and small businesses, simplifying the loan application process and boosting financial inclusion.

Fawry: Fawry acts as a one-stop solution for various bill payments including utilities, transportation, and subscriptions, through a network of physical agents and online channels. It also offers other services like mobile top-up, online shopping, and government payments, simplifying how people manage their finances.

***Paymob*:** Paymob provides businesses with integrated payment gateways, allowing them to accept online payments, credit card transactions, and mobile wallets conveniently. They also offer value-added services like data analytics and fraud prevention.

These examples represent a glimpse into the ever-evolving landscape of Fintech disruption. In addition to banking, Fintech is reshaping industries such as insurance, trade finance, and financial literacy. The effectiveness of these Fintech solutions stems from their ability to:

- Serve segments overlooked by traditional banks, providing convenient, accessible, and affordable financial services.
- Incorporate AI, big data, and mobile technology, automate processes, personalize financial services, and extend their reach to new customers.
- Prioritize enhancing customer satisfaction by focusing on user-friendly interfaces, straightforward onboarding processes, and seamless digital experiences.

While challenges like regulatory obstacles and limited financial literacy persist, the ongoing growth and success of these disruptive Fintech entities underscore the transformative potential of innovation within the Egyptian

financial sector.

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

Based on the **Egypt FinTech Landscape Report 2023**, several Fintech sectors in Egypt are attracting significant investment across various funding stages. The growth of these sectors is driven by the increasing demand for digital financial services, supported by a strong regulatory framework and collaborative ecosystem.[52]

Payments and Remittance

- **Investment Focus**: Payments and remittance solutions dominate the Fintech ecosystem, accounting for 36% of startups in Egypt. Companies like Fawry, Vodafone Cash, and InstaPay are leading innovations in digital transactions.
- **Funding Levels**: Startups in this sector attract funding across Seed, Series A, and Series B stages, with established players securing Series C or later-stage investments to scale operations.

Lending and Alternative Finance

- **Investment Focus**: Digital lending platforms, including Halan and valU, address financial inclusion by providing microloans and Buy Now, Pay Later (**BNPL**) solutions. These platforms use AI-driven credit scoring to serve underbanked populations.
- **Funding Levels**: Investments typically start at Seed and Series A, with Series B funding supporting technological upgrades and geographic expansion.

B2B Marketplaces

- **Investment Focus**: Platforms offering B2B financial solutions, such as supply chain finance and payment automation, represent 10% of Fintech startups. These solutions improve operational efficiency for businesses.
- **Funding Levels**: Primarily Seed and Series A, with some reaching Series B as demand grows.

Insurtech

- **Investment Focus**: The emerging Insurtech sector simplifies access to health and life insurance through mobile-first platforms. These innovations cater to underserved populations, increasing insurance penetration.
- **Funding Levels**: Investments are mostly at the Seed and early Series A stages.

Blockchain and Digital Assets

- **Investment Focus**: Although cryptocurrency is tightly regulated, blockchain technology is gaining attention for its applications in secure payments and decentralized finance (**DeFi**).
- **Funding Levels**: Primarily at the Seed stage, reflecting the nascent state of the sector in Egypt.

Regtech

- **Investment Focus**: Regulatory technology (**Regtech**) startups help financial institutions comply with regulations like AML and KYC. This segment is expanding as compliance becomes more complex.
- **Funding Levels**: Attracting Seed and early Series A investments as the sector develops.

Financial Inclusion and Edtech-Fintech Hybrids

- **Investment Focus**: Startups targeting financial literacy and inclusion, particularly in rural or underserved areas, are gaining momentum.
- **Funding Levels**: Primarily at the Seed stage, with a focus on building scalable business models.

Finally, payments, lending, and B2B marketplaces dominate Fintech investments in Egypt, attracting significant capital at Seed, Series A, and Series B stages. Emerging sectors like Insurtech, Regtech, and blockchain are gaining traction, primarily at early funding stages. The robust growth of the Egyptian Fintech ecosystem reflects its potential to become a regional leader, driven by increasing investment and strong regulatory support.

Footnote(s):

[52] Fintech Egypt News and Events|Fintech Egypt.

Contributors

Ibrahim Shehata
Partner
is@shehatalaw.com

Tasneem El-Naggar
Mid-Level Associate
tn@shehatalaw.com

Omar Mohamed
Junior Associate
om@shehatalaw.com

Mohamed Abed
Junior Associate
ma@shehatalaw.com