

Legal 500

Country Comparative Guides 2025

United Arab Emirates

Fintech

Contributor

KARM Legal
Consultants



Kokila Alagh

Founder and Managing Partner | kokila@karmadv.com

Akshata Namjoshi

Associate Partner | akshata@karmadv.com

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

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

United Arab Emirates: Fintech

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

In the UAE, fintech companies are regulated by multiple authorities depending on their jurisdiction. The Central Bank of the UAE (**CBUAE**) oversees fintech firms providing payment services, stored value facilities, and digital banking. The Dubai Financial Services Authority (**DFSA**) regulates fintech activities in the Dubai International Financial Centre (**DIFC**), while the Financial Services Regulatory Authority (**FSRA**) supervises fintech firms in the Abu Dhabi Global Market (**ADGM**), including payment service providers, digital assets and crowdfunding platforms.

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

The multiplicity of regulators—CBUAE, DFSA, and FSRA—can create overlapping requirements, adding complexity for firms operating across jurisdictions. Stricter AML/CFT measures, potential licensing delays, and restrictions on digital assets could also impact growth. However, continued regulatory clarity, sandbox initiatives, and open banking frameworks may mitigate these risks and foster innovation.

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

Yes, fintechs in the UAE are generally required to be licensed or registered depending on their activities and jurisdiction. Under the CBUAE, fintechs offering payment services must obtain a Stored Value Facilities (SVF) license or a Retail Payment Services and Card Schemes (RPSCS) license. In the ADGM, the Financial Services Regulatory Authority (FSRA) licenses fintech firms under categories like Money Services, Crowdfunding, and Digital Assets. In the DIFC, the DFSA licenses firms under Providing Money Services, including payments, remittances, and stored value facilities, alongside its Innovation Testing License (ITL) for startups. Virtual Assets Regulatory Authority (VARA) issues licenses for activities such as custody, exchange, broker-dealer services, and advisory related to virtual assets, ensuring compliance with AML/CFT regulations and investor protection frameworks.

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

In the UAE, CBUAE, DFSA (DIFC), and FSRA (ADGM) offer sandbox programs that provide regulatory flexibility, reduced compliance costs, and access to expert guidance. For example, DFSA's Innovation Testing License (ITL) and FSRA's Regulatory Laboratory (RegLab) allow startups to refine business models before full market entry. These sandboxes help fintechs navigate regulatory complexities, attract investment, and accelerate go-to-market strategies while ensuring consumer protection and financial stability.

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 the UAE, securities laws apply to Initial Coin Offerings (ICOs) and crypto assets based on their classification by regulators. The Securities and Commodities Authority (SCA) oversees and considers security tokens as regulated securities, requiring compliance with SCA's Crypto Asset Regulations. In Dubai (excluding DIFC), the Virtual Assets Regulatory Authority (VARA) regulates virtual asset activities, including token issuance, exchange, and custody, ensuring compliance with AML/CFT laws. In ADGM, the Financial Services Regulatory Authority (FSRA) treats digital assets as commodities, securities, or derivatives depending on their nature. Companies must obtain the relevant license, implement KYC/AML measures, and comply with investor protection rules to ensure 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?

In the UAE, cryptocurrency exchanges must adhere to strict AML and KYC requirements under the VARA in Dubai and the Financial Services Regulatory Authority (FSRA) in ADGM. VARA mandates exchanges to implement customer due diligence (CDD), transaction

monitoring, and suspicious activity reporting in line with UAE's AML-CFT laws. FSRA classifies virtual assets as regulated financial instruments, requiring firms to comply with FATF guidelines, robust KYC procedures, and risk-based AML frameworks. To ensure compliance, companies should adopt automated KYC solutions, blockchain analytics for transaction monitoring, and regular regulatory reporting to prevent illicit activities and maintain regulatory approval.

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 in the UAE, including licensing and regulatory oversight by VARA, FSRA, and SCA, impact cryptocurrency and blockchain companies by imposing compliance, operational, and reporting requirements. While these frameworks ensure market integrity and investor protection, they also create cost, complexity, and jurisdictional fragmentation for businesses. To navigate these challenges, companies can adopt multi-jurisdictional licensing strategies, leveraging sandbox programs for phased entry, and structuring operations through specialized zones like ADGM and DIFC for regulatory efficiency. Additionally, integrating RegTech solutions for automated AML/KYC compliance, blockchain analytics for real-time risk assessment, and fostering regulatory partnerships can help businesses remain agile and compliant while scaling operations.

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 in the UAE must comply with governmental tax reporting and digital asset obligations under the new Corporate Tax regime (9%), where applicable. While virtual assets are not currently subject to VAT, businesses engaging in crypto activities must assess tax residency, income classification, and potential withholding tax obligations. Compliance measures include accurate record-keeping of transactions, tax filings aligned with UAE Corporate Tax regulations, and adherence to global reporting frameworks like the OECD's Crypto-Asset Reporting Framework (CARF). Companies should also implement audit-ready financial controls, seek tax structuring advice, and monitor evolving UAE tax

policies on 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 in the UAE must balance data privacy regulations with the inherent transparency of decentralized networks. Compliance with the UAE Personal Data Protection Law (PDPL), DIFC Data Protection Law, and ADGM Data Protection Regulations requires implementing privacy-by-design principles, encryption, and selective data anonymization while maintaining blockchain security. To address these challenges, companies can use zero-knowledge proofs (ZKPs) for private transactions, off-chain data storage for sensitive information, and smart contracts with role-based access controls. Establishing data residency frameworks and ensuring cross-border data transfers align with UAE laws will further enhance compliance while preserving blockchain's core benefits.

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, such as restrictions on H-1B and L-1 visas, have had a positive impact on the UAE's fintech sector by attracting highly skilled international talent looking for alternative opportunities. The UAE's Golden Visa, Green Visa, and tech-focused residency programs offer fintech professionals and entrepreneurs a stable regulatory environment, competitive tax benefits, and access to a growing financial ecosystem. With DIFC and ADGM serving as global fintech hubs, UAE-based companies can easily recruit displaced talent from the U.S., fostering innovation and strengthening the region's position as a leading fintech destination.

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?

Fintechs entering the UAE must address licensing, AML/CFT compliance, data protection, and consumer protection regulations. Depending on their activities, they may require approval from CBUAE (payments, banking),

DFSA, FSRA,, or VARA. Key compliance steps include:

1. Obtain the correct license based on business scope.
2. Implement AML/KYC frameworks in line with FATF guidelines.
3. Ensure data privacy compliance under UAE, DIFC, or ADGM laws.
4. Maintain transparent financial reporting per UAE Corporate Tax rules.

To stay compliant, fintechs should engage legal experts, leverage RegTech solutions, and maintain proactive regulatory engagement.

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 enter the UAE market, a fintech should prioritize compliance with local regulations, such as those set by the CBUAE for financial services or the DFSA for firms in the DIFC. Collaborating with local banks, like Mashreq or First Abu Dhabi Bank, can facilitate trust and customer acquisition. The UAE's supportive regulatory environment for fintech, offers opportunities for testing new products in a controlled setting, fostering innovation while ensuring compliance.

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 and operational risks for a fintech entering the UAE market include regulatory compliance risks, market competition, operational challenges, and cybersecurity threats. To mitigate regulatory risks, fintechs must comply with regulations set by bodies like CBUAE or DFSA, ensuring proper licensing and adherence to financial laws. To tackle market competition, focusing on niche segments or offering innovative solutions can provide a competitive edge. Operational risks, such as infrastructure setup, can be mitigated by partnering with local banks or service providers. Additionally, robust cybersecurity measures aligned with UAE data protection laws are essential to protect sensitive customer information and build trust.

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

In the UAE, outsourcing is governed by several regulations, including the **CBUAE's Outsourcing Regulations** for financial institutions and the **DFSA's Outsourcing Rules** for firms operating in the DIFC. These regulations set out specific requirements for outsourcing arrangements, including ensuring that critical functions, such as the **MLRO, CFO, CTO, and DPO**, are retained within the company. The regulations also mandate that outsourcing agreements must be carefully documented, with appropriate risk assessments and controls in place. Regulators have the right to approve or reject outsourcing arrangements based on their alignment with local laws, risk management, and operational integrity.

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?

In the UAE, fintech companies can protect their proprietary algorithms and software through intellectual property (IP) rights such as copyright and trade secrets. The UAE's Patent Law provides protection for inventions, but algorithms themselves may not be patentable unless they involve a novel technical process. In the DIFC, the DIFC Intellectual Property Law offers protection for copyrights and trademarks, while ADGM provides IP protection under its ADGM Regulations. Fintechs should also use confidentiality agreements and ensure compliance with UAE's Data Protection Law and DIFC Data Protection Law to further safeguard proprietary information.

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

In the UAE, fintech companies can safeguard their trademarks and service marks by registering them with the UAE Ministry of Economy under the UAE Trademarks Law. This provides exclusive rights to use the mark within the jurisdiction. In the DIFC, fintechs can register trademarks through the DIFC Intellectual Property Law, while ADGM provides similar protections under its ADGM Regulations. Registration offers legal recourse in case of infringement, helping protect the brand identity. Additionally, fintechs should monitor for potential infringements, use non-disclosure agreements with

partners, and maintain proper usage guidelines to preserve their marks' integrity and prevent dilution.

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?

In the UAE, the use of open-source software in fintech products is legal but requires careful adherence to open-source licensing agreements. Fintech companies must comply with the terms of the specific open-source license, such as GPL, MIT, or Apache, which may include obligations like attribution, modification disclosures, or the requirement to release source code. Non-compliance could result in legal disputes or loss of IP rights. Companies should conduct thorough due diligence, include proper license audits, and establish clear contractual terms with developers to ensure compliance. Additionally, companies should align their practices with the UAE Copyright Law to avoid infringement.

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

Fintech startups in the UAE can navigate intellectual property (IP) ownership complexities by establishing clear agreements with third-party developers or partners. It is crucial to define IP ownership, usage rights, and confidentiality provisions in collaboration agreements to avoid disputes. Startups should ensure that any software or innovation developed is explicitly assigned to the company, and any third-party contributions are covered under work-for-hire clauses or licensing terms. Additionally, fintechs should use non-disclosure agreements (NDAs) to protect proprietary information. Aligning with UAE's Copyright Law and DIFC/ADGM IP regulations ensures legal protection for the startup's IP in case of conflicts.

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 in the UAE should take proactive steps to prevent and address IP infringements by first registering their trademarks, patents, and copyrights with

relevant authorities, such as the UAE Ministry of Economy, DIFC, or ADGM. They should monitor the market for unauthorized use through IP audits and market surveillance. If infringement occurs, companies can issue cease-and-desist letters, seek mediation, or initiate legal action under UAE's Copyright Law or DIFC Intellectual Property Law. Additionally, establishing non-disclosure agreements (NDAs) with employees and partners helps protect proprietary technology and branding from unauthorized use.

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 the UAE, fintech companies using AI for credit scoring and lending must comply with UAE's Data Protection Law and DIFC Data Protection Law, ensuring transparency and fairness in AI algorithms. They are required to provide clear information to customers about the data used and the decision-making process. Additionally, fintechs must check if their AI-driven services trigger any financial regulatory licenses from authorities like the CBUAE or DFSA. To prevent biased or discriminatory outcomes, fintechs should conduct regular algorithm audits, implement bias detection tools, and ensure their AI systems adhere to principles of fairness, accountability, and non-discrimination.

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?

Fintech companies developing proprietary AI models in the UAE should focus on protecting their AI algorithms and data sets through copyright and trade secret laws. If the AI models meet the criteria for patentability, fintechs may seek patent protection under UAE Patent Law. It is essential to define clear ownership in collaboration agreements if third parties contribute to development. Companies should use non-disclosure agreements (NDAs) to safeguard proprietary information. When using third-party AI tools, fintechs must comply with the terms of service or license agreements of those tools, ensuring no infringement on the intellectual property of the third-party provider. Additionally, fintechs should ensure that any third-party tools do not expose them to unexpected

IP claims or risks.

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?

Fintechs deploying AI solutions in the UAE must comply with regulations from bodies like the CBUAE and DFSA. For financial services, fintechs need to adhere to anti-money laundering (AML) and know-your-customer (KYC) requirements, ensuring AI applications do not facilitate fraudulent or illegal activities. They must also ensure compliance with the UAE Data Protection Law and DIFC Data Protection Law regarding data privacy and security. The UAE AI Strategy 2031 and the ADGM Financial Services Regulatory Authority (FSRA) offer frameworks for responsible AI use, encouraging fairness, transparency, and accountability. Fintechs should conduct regular AI audits, implement bias detection mechanisms, and ensure their AI models are aligned with these regulatory guidelines to ensure compliance and ethical operation.

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

Fintech companies should adopt comprehensive risk management strategies to mitigate legal liabilities associated with AI technologies. These strategies include conducting regular AI audits to ensure compliance with data protection laws (e.g., UAE Data Protection Law, DIFC Data Protection Law), addressing algorithmic bias through testing and monitoring, and implementing transparency measures in AI decision-making. Fintechs should also ensure that AI systems comply with anti-money laundering (AML) and know-your-customer (KYC)

regulations. Additionally, companies should establish clear contractual agreements with third-party AI providers, use non-disclosure agreements (NDAs), and maintain insurance coverage for potential legal disputes or regulatory fines related to AI-driven activities.

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

Yes, the UAE has witnessed significant disruption through fintech, particularly in digital payments, blockchain, and lending. PayTabs, a UAE-based fintech, revolutionized the payment gateway sector by offering seamless cross-border payment solutions for businesses. Comera Pay, another example, has disrupted the digital financial services space by offering services such as digital wallets, remittance solutions, and prepaid cards. Additionally, Sarwa, a robo-advisory firm, has transformed investment management by providing automated wealth management solutions. The Dubai International Financial Centre (DIFC) and Abu Dhabi Global Market (ADGM) have also fostered fintech innovation with regulatory sandboxes, encouraging startups to test their solutions.

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

In the UAE, fintech sectors attracting investment include digital payments, insurtech, and wealth management. Notable examples include Sarwa, a robo-advisory firm that raised a Series A round to scale its wealth management platform. YAP, a digital banking platform, also secured Series A funding to expand its customer base and enhance its banking services. In the Series B stage, Tabby, a buy-now-pay-later (BNPL) provider, raised significant funds to expand its operations across the GCC. These sectors are receiving attention as digital transformation accelerates, with the UAE's regulatory environment in DIFC and ADGM supporting fintech growth.

Contributors

Kokila Alagh

Founder and Managing Partner

kokila@karmadv.com



Akshata Namjoshi

Associate Partner

akshata@karmadv.com

