Legal 500
Country Comparative Guides 2026

Saudi Arabia
Fintech

Contributor

AX Law

Joelle Jleilaty

Associate | joelle@axlaw.com

Karim Fawaz

Partner | karim@axlaw.com

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

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

Saudi Arabia: Fintech

1. Who are the primary regulators overseeing fintechs in your jurisdiction, and how are regulatory boundaries evolving as innovation crosses traditional lines between payments, lending, wealth, and digital assets?

In the Kingdom of Saudi Arabia (KSA), the regulatory framework for fintech is primarily overseen by two main authorities:

(a) Saudi Central Bank (SAMA): SAMA regulates fintech companies that provide payments, e-money, digital wallets, and other financial services that are not classified as securities. This includes payment service providers, payment initiation services, merchant acquiring, and consumer financing activities.

(b) Capital Market Authority (CMA): CMA regulates fintech companies that operate in the capital markets space, such as robo-advisory platforms, crowdfunding portals, investment distribution platforms, and other services involving securities or investment products.

Regulation in Saudi Arabia is increasingly activity-based, meaning fintechs are regulated based on what they actually do, rather than how they describe themselves. As fintech "super-apps" combine payments, financing, and wealth features, it is now common for regulators to conduct dual-perimeter assessments across SAMA and CMA. Regulators are also placing greater emphasis on product governance, outsourcing controls, data protection, and customer outcomes, rather than corporate structure alone.

Recently, the first tokenization in KSA became regulated by the Real Estate General Authority (REGA) in collaboration with the CMA. While SAMA and the CMA remain the main fintech regulators, it is expected to see joint regulation in sector-specific initiatives.

2. As regulators adopt different rules for digital assets, AI, and consumer protection, what key regulatory and operational challenges could slow fintech innovation and growth in your jurisdiction over the next 12 months?

While KSA's fintech sector continues to grow, several challenges may slow innovation in 2026.

In 2025, Saudi regulators have licensed a large number of fintech players across multiple verticals, particularly in payments and consumer finance. However, not all licensees have been able to launch at scale or achieve the commercial traction and growth initially anticipated at the time of licensing. As a result, the market has begun to see and is expected to see more mergers, acquisitions, restructurings, and exits. This is likely to lead regulators to adopt a more measured and selective approach to issuing new licenses in the short term.

This trend should be viewed as a market-maturation phase rather than a slowdown in innovation. Consolidation is helping to strengthen the ecosystem by removing weaker business models, encouraging operational discipline, and ultimately creating space for better-capitalized and more resilient fintechs to enter the market.

At the same time, cybersecurity and technology risk remain central regulatory concerns. As fintech platforms handle increasing transaction volumes and sensitive customer data, regulators are placing greater emphasis on cybersecurity governance, incident reporting, and third-party risk management. In 2025, fintechs are expected not only to have cybersecurity policies in place, but also to demonstrate operational readiness and tested response capabilities, particularly where cloud services and outsourced technology providers are involved.

In addition, newer initiatives such as open banking, payment initiation services, and embedded finance continue to face implementation challenges. These models depend heavily on the technical readiness of traditional banks and financial institutions, many of which are still upgrading legacy systems. As regulators continue to refine technical standards, API requirements, and operational manuals, ongoing technology upgrades and infrastructure investment across the sector will be necessary, which may slow deployment timelines for some fintech products in the near term.

Moreover, increased regulatory requirements aiming at ensuring robust infrastructures for fintechs and the regulator's interference in pricing certain services are impacting the cost of business and profitability. It is our view however that this should encourage fintechs to offer

more innovative products that justify new revenue streams.

3. Are fintechs generally required to obtain licenses or registrations to operate in your jurisdiction, and if so, which activities typically trigger those requirements (e.g., lending, payments, digital assets custody)?

Fintech companies in KSA are generally required to obtain regulatory licenses or approvals before carrying out any activities that fall within the financial or capital markets regulatory perimeter.

Fintechs that offer payment processing, digital wallets, payment initiation services, merchant acquiring, or that store or handle customer funds are required to be licensed by SAMA, except where such activities are conducted under SAMA's regulatory sandbox, as discussed later in this article. In addition, companies offering BNPL services must obtain a specific BNPL license from SAMA, reflecting the regulator's strong focus on consumer protection, responsible lending, and transparency.

Fintechs that provide investment advice, robo-advisory services, crowdfunding platforms, or investment distribution activities fall under the supervision of CMA and must obtain the appropriate authorization, except where such activities are conducted under the Fintech Lab, as discussed later in this article.

Where a fintech's business model spans both payment or financing services and investment-related activities, dual regulatory oversight may apply. In such cases, fintechs must comply with the requirements of both SAMA and CMA, which often requires careful regulatory planning, early engagement with both authorities, and, in some cases, the maintenance of multiple licenses.

It is also worth noting that SAMA and CMA are increasing collaboration. For example, SAMA-licensed e-wallet providers are now permitted to be channels for the distribution of units in private funds that are regulated by CMA.

4. Are there emerging cross-functional or omnibus licensing regimes, such as those inspired by the U.S. GENIUS Act, the EU MiCA/DORA frameworks, or similar integrated models, that allow a single license to cover multiple fintech activities?

Saudi Arabia does not currently offer a single omnibus fintech license comparable to the EU's MiCA or DORA frameworks. Instead, licensing remains modular, with separate approvals required for each regulated activity.

5. How have regulatory sandboxes, innovation offices, or digital-testing frameworks matured in 2025, and what measurable impact have they had on time-to-market or capital formation for fintech start-ups?

Saudi Arabia has developed well-established and mature regulatory sandbox frameworks as part of its broader Vision 2030 agenda to encourage financial innovation.

a. SAMA Regulatory Sandbox: Operated by SAMA, this sandbox allows fintech companies and financial institutions to test innovative financial products and services that may not yet be fully addressed by existing regulations. Participants are permitted to test their solutions with real customers for a limited period, subject to defined safeguards and regulatory oversight.

b. CMA FinTech Lab (Experimental Permit – ExPermit): Operated by CMA, this framework enables fintechs operating in the capital markets space, such as robo-advisory and investment platforms, to test new business models under a simplified regulatory regime before applying for full authorization.

In 2025, these sandbox frameworks became an established entry point for innovative fintech models. They have helped companies validate their business models at an early stage, reduce regulatory uncertainty through direct engagement with regulators, and improve credibility with investors and commercial partners. While participation in a sandbox does not replace the need for full licensing, it often shortens time-to-market, supports capital raising, and allows fintechs to refine their products before scaling.

6. How are regulators adapting their supervisory approaches (e.g., RegTech-enabled supervision, API-based reporting) to oversee fintechs operating across jurisdictions or with embedded finance models?

Saudi regulators are increasingly adopting more structured and technology-enabled supervisory approaches to keep pace with the growing complexity of

fintech business models, particularly those involving embedded finance and cross-border operations.

A key development has been the expansion of open banking and API-based frameworks.

Through SAMA's Open Banking Framework, regulators are setting clearer technical standards for data sharing, payment initiation, and system security. This allows regulators to better monitor how fintechs and banks interact within broader financial ecosystems and ensures accountability across all participants.

Regulators are also placing greater emphasis on governance and operational controls, rather than relying solely on periodic reporting. Fintechs are increasingly expected to demonstrate real-time operational readiness, including effective risk management, incident response capabilities, and oversight of outsourced and cloud-based service providers. This reflects a shift toward more continuous, risk-based supervision.

For fintechs operating across jurisdictions, regulators are focusing on local accountability, even where technology platforms or group functions are based offshore. This includes clear responsibility for compliance, data protection, and customer outcomes within Saudi Arabia. In embedded finance models, supervisory attention is particularly directed at how financial services are integrated into non-financial platforms, ensuring that consumer protection, transparency, and regulatory responsibilities are not diluted.

Through robust connectivity with regulated entities, SAMA has implemented real-time monitoring which allows increased measures for the prevention of fraud and supervision of regulated entities.

Overall, the supervisory approach in KSA is evolving toward a more proactive and technology-aware model, combining standardized technical frameworks with closer scrutiny of governance, resilience, and consumer impact.

7. How do your jurisdiction's securities, commodities, and banking regulators interpret tokenization, DeFi, and stablecoin products under the current legal landscape, particularly in light of the U.S. state-level stablecoin acts and MiCA implementation in the EU?

KSA continues to take a cautious and practical approach to tokenization, DeFi, and stablecoin products, particularly where these products may be offered to retail users. Rather than regulating digital assets based on labels, regulators focus on the economic substance of the product.

If a token or digital asset looks and behaves like an investment or security, it is likely to fall within CMA's regulatory perimeter and be treated similarly to other capital markets products. On the other hand, if a product functions more like money, payments, or stored value, it is more likely to raise concerns for SAMA, as it may fall within payments or financial services regulation.

While global developments such as U.S. state-level stablecoin laws and the EU's MiCA framework provide useful reference points, Saudi regulators have so far taken a measured and localised approach. The focus remains on maintaining financial stability, protecting consumers, and managing AML and financial crime risks, rather than rapidly adopting foreign regulatory models.

The first tokenization launched in the KSA is in the real estate under the joint supervision of REGA and the CMA. More tokenization and cryptocurrency initiatives are expected to appear subject to the solidifying the current experience in real estate tokenization.

8. What are the AML/CFT and travel-rule obligations for virtual asset service providers currently, and how do they apply to "non-custodial" or "self-hosted wallet" models?

In KSA, there is no separate standalone AML regime exclusively for virtual assets. However, where crypto-related activities closely resemble regulated financial intermediation, regulators expect firms to apply the same AML and counter-terrorist financing standards that apply to traditional financial institutions.

For non-custodial or self-hosted wallet models, the absence of direct custody does not remove AML risk. Instead, compliance controls tend to shift toward transaction monitoring, wallet risk-scoring, enhanced due diligence triggers, and strict limits on exposure to higher-risk users or jurisdictions. Regulators are increasingly focused on how these risks are identified and managed in practice, particularly where platforms provide access, connectivity, or transaction-facilitation services.

Overall, the key principle is that substance prevails over form: if a crypto business performs functions similar to a regulated financial intermediary, it should expect AML, travel-rule-style controls, and supervisory expectations to apply accordingly.

9. What new prudential or reserve requirements are being imposed on stablecoin issuers or custodians?

In Saudi Arabia, there is currently no formal regulatory regime specifically for stablecoin issuers or custodians. If regulators were to permit or recognize stablecoins in the future, the likely requirements would include demonstrating full reserve backing with high-quality assets, clear redemption mechanisms, proper safeguarding and segregation of client assets, strong governance, and risk-management controls consistent with how money-like products are regulated.

10. How focused are regulators in your jurisdiction on data privacy, cybersecurity, and operational resilience for fintechs, and what enforcement or inquiry trends are emerging?

Regulatory focus in KSA on data privacy, cybersecurity, and operational resilience is high and continues to increase. A key driver is the Personal Data Protection Law (PDPL), which became fully enforceable in September 2024 and has significantly raised expectations around data governance, cross-border transfers, and vendor oversight. The year 2025 witnessed increased levels of enforcement and penalties to encourage the market to handle data and privacy seriously.

At the same time, SAMA's licensing frameworks place strong emphasis on governance, cybersecurity controls, outsourcing arrangements, and business continuity planning. Fintechs are expected not only to have policies in place, but also to demonstrate operational readiness, including tested incident-response procedures and effective third-party risk management.

From a supervisory perspective, regulators are increasingly conducting proactive reviews focused on incident preparedness, outsourced service providers, and data handling across complex ecosystems such as open banking and embedded finance.

11. What practical steps should cryptocurrency and blockchain companies take to detect and prevent fraudulent transactions, and how can they prepare for regulatory audits, inquiries, and enforcement actions?

In the absence of dedicated regulations for cryptocurrency and blockchain, companies, particularly those handling higher-risk transactions, should focus on building strong but practical control frameworks.

This starts with clear governance and accountability. Firms should also invest in effective transaction and wallet-monitoring tools, such as anomaly detection, sanctions screening, and risk-based alerts, to identify suspicious activity early. New regulations are expected to be released soon dedicated for such businesses.

12. How are fintechs adapting to changing immigration frameworks, such as revisions to U.S. H-1B and digital nomad visas in the EU and Asia, to attract tech and compliance talent globally?

Fintech companies operating in KSA are increasingly adopting flexible and hybrid talent strategies in response to tightening immigration frameworks in other jurisdictions, such as the U.S. and parts of Europe and Asia.

In practice, many fintechs are leveraging Saudi Arabia's talent-attraction initiatives, including Premium Residency pathways, which offer greater stability for senior and critical talent without reliance on traditional sponsorship models. These pathways are particularly attractive for leadership, technology, and compliance roles that benefit from long-term continuity.

In addition, multinational fintechs are making use of regional headquarters (RHQ) incentives to centralize leadership and strategic functions in Saudi Arabia. While not an immigration program in itself, the RHQ ecosystem supports talent mobility by encouraging companies to relocate decision-making and key personnel to KSA, while continuing to operate with globally distributed technical teams.

Overall, fintechs are increasingly combining local presence with global talent pools to remain competitive in a tightening international talent market.

13. What new geopolitical or sanctions-related risks (e.g., digital asset restrictions, AML screening mandates) have emerged that affect fintech operations in cross-border markets?

Fintechs operating across borders are increasingly exposed to geopolitical and sanctions-related risks, many of which directly affect KSA-linked operations. These risks are no longer limited to direct dealings with sanctioned jurisdictions or entities, but increasingly arise through indirect exposure across complex, multi-layered

payment and settlement chains.

A key risk area is sanctions exposure through counterparties, intermediaries, and nested payment structures, where funds may transit through multiple jurisdictions, correspondent banks, or service providers before reaching their final destination. This increases the risk of inadvertent sanctions breaches, particularly where upstream or downstream parties are subject to evolving sanctions regimes.

In response, regulators are imposing stricter expectations around real-time sanctions screening, transaction monitoring, and enhanced due diligence for cross-border activity. There is also growing regulatory emphasis on transparency of beneficial ownership, source of funds, and control structures, especially for corporate customers and digital-first business models operating across multiple jurisdictions.

In parallel, geopolitical tensions have accelerated scrutiny of digital assets and alternative payment rails, with certain jurisdictions imposing restrictions on crypto-related activities, wallet services, and cross-border transfers involving virtual assets.

Fintechs are therefore required to continuously reassess their risk exposure, screening frameworks, and jurisdictional footprint to ensure ongoing compliance with rapidly changing sanctions, AML, and counter-terrorist financing requirements.

14. How do immigration and workforce-mobility policies—like work visas, remote-work permits, and intra-company transfers—affect fintechs' ability to move key staff into new markets, and what practical steps can companies take to avoid talent shortages or delays?

Immigration and workforce-mobility requirements can have a direct impact on fintech launch timelines, particularly where regulated roles or senior leadership are expected to be physically present in the market. Visa processing timelines, localization requirements, and approvals for regulated functions such as compliance officers can all create delays if they are not addressed early in the planning process. To manage these challenges, fintechs are increasingly taking a proactive and structured approach. This typically includes identifying critical and regulated roles at an early stage, running parallel hiring tracks for both local and international talent, and relying on structured secondments or intra-group transfers supported by clear documentation and onboarding plans. From a KSA perspective, these challenges are partially mitigated by KSA's more flexible immigration framework under Vision 2030. Initiatives such as the Premium Residency Program allow eligible foreign professionals to live and work in KSA without traditional sponsorship requirements, providing fintechs with greater flexibility when relocating senior, technical, or compliance talent.

15. How do immigration rules and visa limitations influence the speed and strategy of fintech market entry, particularly when launching operations in multiple jurisdictions?

Immigration rules often play a decisive role in shaping fintech market-entry strategies. In practice, visa constraints can determine whether a fintech launches initially with a lean local presence supported by offshore teams, or whether it invests early in building a deeper in-country operating model, which is often preferred for regulated activities.

From a regulatory perspective, licensing readiness is frequently influenced less by documentation and more by operational substance, including the availability of qualified local staff, fit-and-proper management, and clear accountability on the ground. As a result, fintechs that integrate immigration planning into their licensing and expansion strategy from the outset are typically better positioned to enter the market efficiently and scale sustainably.

16. How can fintechs protect their proprietary algorithms and smart-contract code, balancing open-source use with trade-secret protections and any AI-related disclosure rules?

Fintechs can best protect their proprietary technology by adopting a layered and practical approach to intellectual property protection.

The KSA continuously upgrades its intellectual property laws and regulations under the supervision of the Saudi Authority for Intellectual Property (SAIP).

Where third-party developers or vendors are involved, fintechs should rely on robust development agreements that clearly assign intellectual property to the fintech, include confidentiality obligations, and address moral rights where relevant. These contracts are often the first line of defence in avoiding future ownership disputes and the KSA has recently adopted a thorough and detailed Civil Transactions Law which builds more certainty in contracts and commercial arrangements.

Open-source software can be used, but it must be

managed carefully. Fintechs should maintain open-source governance frameworks, including software inventories, licence compliance checks, and contributor policies, to ensure that open-source components do not unintentionally contaminate proprietary code.

Where AI-related transparency or disclosure obligations arise whether from regulators, partners, or customers fintechs should aim to disclose information only to the extent necessary, without revealing the underlying proprietary logic of their models.

17. What strategies are most effective for safeguarding trademarks and digital brands in an era of AI-generated impersonation, deepfakes, and synthetic media fraud?

Brand protection has become increasingly important as AI-generated impersonation, deepfakes, and synthetic media grow more sophisticated.

The starting point remains early trademark registration. In KSA, fintechs should register their trademarks and service marks with the SAIP to establish clear and enforceable rights. Registration also makes enforcement and takedown actions significantly easier.

Beyond registration, fintechs should actively monitor their brands online, including app stores, social media platforms, and domain registrations, and maintain clear takedown procedures for impersonation or misuse. Technical measures such as verified domains, anti-phishing controls, and clear customer communication protocols also play an important role in protecting users and preserving trust.

18. When fintechs collaborate with outside developers, partners, or open-source communities, how can they make sure they retain ownership of their technology and avoid disputes?

The most effective way to avoid disputes is to avoid ambiguity at the outset.

Fintechs should ensure that all collaboration agreements clearly address intellectual property ownership, specifying whether new developments belong exclusively to the fintech or are jointly owned. Contracts should also include restrictions on reuse, or creating derivative works, particularly where core technology is involved.

Non-disclosure agreements and, where appropriate, non-compete or non-circumvention provisions further help reduce the risk of misuse or leakage of valuable technology.

19. What steps should fintechs take to detect, prevent, and respond to competitors or third parties who might copy or misuse their technology, algorithms, or branding, and how do enforcement strategies differ across jurisdictions?

To protect their intellectual property, fintechs should take a proactive and ongoing approach. This includes registering key IP assets, regularly monitoring the market and competitors for signs of copying or misuse, and preserving evidence as soon as potential infringement is identified.

Initial enforcement often starts with cease-and-desist communications or platform takedown requests, which can be effective and commercially efficient. Where these measures are unsuccessful, fintechs may need to pursue regulatory complaints or court action, depending on the jurisdiction.

Enforcement strategies vary significantly across countries, particularly in terms of speed, cost, and the availability of interim relief. As a result, fintechs operating across multiple markets should tailor their IP enforcement approach to local legal frameworks, while relying on strong contracts and registrations as the foundation of their global IP strategy.

20. How are jurisdictions addressing cross-border IP enforcement for fintech products involving distributed infrastructure and decentralized code bases?

In Saudi Arabia, cross-border IP enforcement for fintech products involving distributed infrastructure and decentralized or open-source code bases remains grounded in traditional IP and contractual enforcement mechanisms, rather than bespoke regimes for decentralized technologies.

Saudi authorities continue to rely on established frameworks under the Copyright Law, Trademarks Law, and Anti-Cyber Crime Law, alongside contractual remedies, to address infringement risks linked to fintech platforms operating across borders.

Saudi courts and regulators place significant emphasis

on documented ownership of IP rights, clear licensing structures (particularly for open-source components), and contractual allocation of responsibility and control. As a result, the effectiveness of cross-border enforcement in the KSA context depends less on the decentralized nature of the technology itself and more on the robustness of IP documentation, the clarity of contractual rights and restrictions, and the ability to link enforcement actions to entities or assets within Saudi jurisdiction.

21. How should fintechs approach IP protection when licensing or selling software, smart contracts, or AI models to ensure ongoing control and compliance with different countries' laws?

When licensing or commercializing technology across borders, fintechs should take a carefully structured and jurisdiction-aware approach to IP protection.

Licensing agreements should clearly define the scope of permitted use, including territorial limits, duration, sublicensing rights, and restrictions on modification or reuse. Where software, smart contracts, or AI models are involved, it is particularly important to address ownership of derivatives, improvements, and outputs, as well as restrictions on reverse engineering or model training using licensed technology.

Fintechs should also include audit rights, security obligations, and compliance requirements to ensure that licensees adhere to applicable local laws, including data protection and consumer protection rules. Termination rights and post-termination obligations, such as disabling access or deleting licensed materials, are critical to maintaining long-term control.

Ultimately, strong licensing terms, combined with clear governance and ongoing monitoring, are essential for fintechs seeking to scale internationally while protecting their core technology and complying with different regulatory regimes.

22. Under emerging AI-governance frameworks, such as the EU AI Act and U.S. GENIUS Act, what legal obligations apply to fintechs using AI in underwriting, robo-advisory, and fraud protection?

While Saudi Arabia does not yet have a comprehensive AI statute comparable to the EU AI Act, fintechs operating in or from Saudi Arabia are increasingly expected to align with global AI-governance standards, particularly where their products are offered cross-border or rely on international partners.

In practice, fintechs using AI for underwriting, robo-advisory, or fraud prevention must comply with existing financial regulation, data-protection requirements under the PDPL, and consumer-protection rules. Regulators expect firms to understand how their AI systems operate, to maintain human oversight over high-impact decisions, and to ensure that automated tools do not lead to unfair or misleading outcomes.

Global developments such as the EU AI Act and similar U.S. initiatives are influencing expectations around risk classification, transparency, and accountability, even where these frameworks do not directly apply under Saudi law.

23. How can fintechs evidence algorithmic fairness, explainability, and bias mitigation in compliance with new supervisory expectations for automated credit and AML decisioning systems?

Fintechs are increasingly expected to evidence, rather than simply assert, that their AI systems are fair and explainable.

This typically involves documenting how models are designed and trained, testing for bias before and after deployment, and monitoring outcomes over time. Fintechs should be able to explain, in clear terms, how key decisions, such as credit approvals or AML alerts, are made, particularly when customers or regulators request clarification.

24. What are the IP and data-protection considerations around training proprietary AI models on financial data, and how can fintechs structure data-sharing agreements to minimize risk?

Training AI models on financial data raises both intellectual property and data-protection concerns.

From a data-protection perspective, fintechs must ensure compliance with the PDPL, including having a lawful basis for using personal data, applying data-minimisation principles, and managing cross-border transfers appropriately. From an IP standpoint, it is important to clearly define who owns the trained models, derived

outputs, and any improvements generated through training.

Data-sharing and vendor agreements should clearly address permitted use, ownership of outputs, confidentiality, security measures, and restrictions on re-use or onward training. These contractual protections are essential to prevent data leakage and unintended loss of proprietary rights.

25. How are regulators treating AI-driven investment or credit-decisioning tools for purposes of fiduciary duty, fair lending, and disclosure obligations under updated consumer protection frameworks?

Regulators are making it clear that the use of AI does not reduce a fintech's legal responsibility.

For investment-related tools, this means ensuring that robo-advisory systems meet suitability and disclosure expectations and that customers understand when decisions are automated. For credit and underwriting tools, regulators expect fintechs to comply with fair-lending principles and to avoid discriminatory decision-making.

In practice, AI is viewed as a tool, not a substitute for accountability. Fintechs remain responsible for the outcomes generated by their systems and for addressing customer complaints or regulatory inquiries.

26. What emerging liability theories (e.g., negligent model governance, failure to supervise AI) could expose fintechs to enforcement or civil litigation in the next 12 months, and how should firms build defensible risk management frameworks?

Over the next 12 months, fintechs may face increased exposure to liability based on weak AI governance, such as failure to properly supervise models, inadequate testing, or over-reliance on third-party AI tools without sufficient oversight.

Other risk areas include misleading statements about AI capabilities, insufficient data-protection controls, and discriminatory outcomes resulting from automated decision-making.

To build a defensible risk framework, fintechs should establish clear governance structures, assign responsibility for AI oversight at a senior level, maintain strong documentation and testing practices, and ensure ongoing monitoring of AI performance. Combining these measures with regular legal and compliance reviews will be key to managing both regulatory and litigation risk as AI use continues to expand.

Contributors

Joelle Jleilaty
Associate
joelle@axlaw.com

Karim Fawaz
Partner
karim@axlaw.com