Legal 500
Country Comparative Guides 2025

Cayman Islands
Fintech

Contributor

Appleby

Peter Colegate

Partner | pcolegate@applebyglobal.com

Dean Bennett

Partner | dbennett@applebyglobal.com

Marsha Williamson

Senior Associate | mwilliamson@applebyglobal.com

Ross McLeod

Associate | rmcleod@applebyglobal.com

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

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

Cayman Islands: Fintech

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

The principal regulator is the Cayman Islands Monetary Authority (**CIMA**). CIMA is responsible for the regulation and supervision of financial services firms operating in and from the Cayman Islands (including fintechs) and the monitoring of compliance with financial services laws (including anti-money laundering, counter-financing of terrorism and counter-proliferation financing (**AML/CTF/CPF**) laws). Some fintechs fall outside of the scope of CIMA's regulatory framework if they are not carrying out regulated activities.

Depending on the nature of business, the following regulators and governmental bodies may also perform an oversight role for both regulated and unregulated fintechs:

- the Cayman Islands Data Protection Ombudsman (**Ombudsman**) with respect to data protection and privacy;
- the Department for International Tax Cooperation (**DITC**);
- the Cayman Islands Registrar with respect to the beneficial ownership regime and other corporate authorisations and filings;
- the Cayman Islands Financial Reporting Authority (**FRA**) with respect to sanctions; and
- the Department of Commerce and Investment with respect to trade and business licences.

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

While the fintech sector has developed in recent years, most notably relating to virtual assets and tokenised products, the following key risks could impact growth:

1. Changes to the legal, regulatory and tax landscape for fintechs (most notably virtual asset service providers (**VASPs**)) which reduce regulatory burdens and barriers to market entry or expansion in onshore jurisdictions, particularly in the United States. This could lead to less demand for offshore structures;
2. Competition from other jurisdictions developing more fintech-friendly regulation and incentives to attract business, such as the Dubai Virtual Assets Regulatory Authority;
3. The potential introduction of more extensive regulatory standards on a national and global level increasing the cost of compliance, particularly relating to virtual assets and AML/CTF/CPF measures;
4. General market volatility in the global virtual assets markets and a reduction in investor confidence from potential high-profile business failures;
5. Availability of skilled talent on a local level (particular in cybersecurity, artificial intelligence and software engineering roles) and competition for talent acquisition with other attractive expatriate jurisdictions; and
6. Lack of digital infrastructure and innovation amongst local service providers and limitations on access to local banking for VASPs.

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

It is fact-specific and depends on the nature of the fintech's activities to be carried out in or from the Cayman Islands.

Generally, fintechs may require a CIMA licence or registration under the following financial services legislation:

- the Virtual Asset (Service Providers) Act (**VASPA**) for entities conducting certain virtual asset services (such as exchanges, custodians and broker dealers);
- the Securities Investment Business Act (**SIBA**) for entities carrying out securities and investment business (such as dealing or advising on investments); and
- the Banks and Trust Companies Act and/or Money Services Act for entities, such as challenger banks, involved in deposit-taking, trust services, or money services business.

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

A regulatory sandbox allows entities to develop and test products, technologies and business models in a controlled, supervisory-lite environment with the aim of fostering innovation, growth and market competition.

There is currently no regulatory sandbox in the Cayman Islands. The VASPA provides a framework for CIMA to grant sandbox licences to VASPs and other fintech service providers for up to one year in certain circumstances (including where the proposed service presents higher supervision, AML or systemic risks). However, the introduction of the sandbox is still awaited. While there is no sandbox, in our experience, CIMA is open to discussion with fintechs and new entrants regarding potential applications for licensing or registration, new business models, and the application of the regulatory framework.

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 VASPA is intended to provide a flexible framework to promote the use of new technology and innovative enterprise in the Cayman Islands while complying with newly adopted international standards set by the Financial Action Task Force (**FATF**). The new legislation provides for the supervision of persons and entities facilitating virtual asset activities as a business.

Under the VASPA a "virtual asset" is defined as a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, but does not include digital representations of fiat currencies.

"Virtual asset services" are businesses providing one or more of the following services or operations:

- issuing (selling) of virtual assets;
- exchanges between virtual assets and fiat currencies;
- exchanges between one or more other forms of convertible virtual assets;
- transfers of virtual assets;
- virtual asset custody services; or
- the participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset.

Under the VASPA, from 31 October 2020, all virtual asset service providers (VASPs) need to apply to register with CIMA. Phase 2 of VASPA will come into force on 1 April 2025 and requires virtual asset custodians and exchange or trading platforms to apply for a separate VASP licence.

The VASPA provides for various exceptions including:

- platforms which are mere meeting places where sellers and buyers may post bids and offers and where the parties trade in a peer-to-peer environment only;
- fintech service providers that use innovative technology to improve, change or enhance financial services but which are not virtual asset services;
- virtual service tokens which are not transferable or exchangeable and include tokens whose sole function is to provide access to an application or service; and
- tokenised equity does not qualify as a "virtual asset".

VASPs are subject to a number of general obligations including:

- extensive anti-money laundering obligations;
- strict data protection and cybersecurity requirements;
- the filing of annual accounts with CIMA as the regulator of VASPs;
- the requirement for senior officers and beneficial owners to be fit and proper persons;
- the prior approval of senior officer appointments by CIMA;
- any issuance of virtual assets requiring the prior approval of CIMA; and
- CIMA approval before the issuance or transfer of any shareholding in a VASP entity above 10%.

The primary piece of legislation regulating securities and investment business in the Cayman Islands is the SIBA. SIBA provides for the licensing and control of persons engaged in securities investment business in or from the Cayman Islands. Importantly, SIBA is essentially consumer protection legislation, designed to protect the investing public and to be construed broadly. When determining whether a business activity is caught by SIBA, therefore, the emphasis is on substance rather than form.

SIBA sets out an exhaustive list of financial instruments that constitute "securities". SIBA has been amended to include virtual assets in that list. A virtual asset that can be sold, traded or exchanged and that represents, can be converted into or is a derivative of any of the existing SIBA-listed securities will also qualify as a security although certain exemptions may still apply.

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?

The Cayman Islands has long been committed to implementing best international practices and is

compliant with the anti-money laundering and anti-terrorist financing requirements of the OECD and FATF. As a member of the Caribbean FATF, the Cayman Islands implements recommendations promulgated by the FATF.

All Cayman Islands-incorporated entities are subject to the Proceeds of Crime Act which sets out the principal money laundering offences.

Certain "relevant" businesses (which would include, for instance, entities caught within Cayman financial services regulations (including VASPs and those registered or licensed under SIBA) and other entities thought to be at a higher risk of money laundering) are further subject to the Anti-Money Laundering Regulations (**AML Regs**) which prescribe certain identification, record keeping and internal control procedures for such businesses. CIMA's Guidance on Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation also applies.

Importantly, businesses in the Cayman Islands need to adopt a risk-based approach to the collection of know-your-client (KYC) information. Under the risk-based approach, the latest guidelines from the FATF permit the digital verification of identities and receipt of electronic copies of documents instead of traditional "wet ink" paper-based processes.

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?

The regulatory framework applicable to regulated cryptocurrency and blockchain companies includes (i) the application for registration or licensing, typically under the VASPA or SIBA and (ii) ongoing supervisory obligations, including reporting, transaction monitoring, and extensive AML/CTF/CPF compliance obligations (as summarised in Q.6 above). The main operational impacts are on skilled resource requirements, costs of compliance and customer onboarding process.

At the application stage, it is important for applicants to seek legal advice on the proposed activities to assess structuring options, economic substance requirements, and the extent to which the activities fall within the regulatory perimeter. Applicants should also seek early engagement with CIMA on the proposed business model and application.

Group structuring plays an important role – it may be optimal for a company to carry out certain regulated activities through an entity licensed or registered in the Cayman Islands with other activities (such as software development or intellectual property licensing) carried out in alternative jurisdictions, like the British Virgin Islands or the Seychelles.

Where a company does not have local regulatory expertise, it can engage local service providers (such as AML or compliance officers) to help navigate compliance monitoring and reporting obligations. Companies may outsource certain activities to other group companies or third-party service providers in other jurisdictions, subject to the outsourcing laws and CIMA outsourcing guidance. In all cases, ultimate responsibility for complying with the jurisdiction's regulatory requirements sits with the senior management of the company.

With the rise in RegTech, companies can also leverage technology to assist with its regulatory obligations, particularly electronic KYC (including digital identity checks) and transaction monitoring tools.

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?

The Cayman Islands is a tax neutral jurisdiction. Any fintech company registered in the Cayman Islands will not be subject to any direct taxes in the jurisdiction.

There is an economic substance regime in the Cayman Islands governed by the International Tax Co-operation (Economic Substance) Act (as revised) (the **ES Act**). A fintech may be within scope of the ES Act if it is carrying out one or more of the relevant activities (such as banking business) and an exemption does not apply. If so, it will be required to submit an annual report to the Tax Information Authority (**TIA**) and provide the TIA with such other information as it may require to make an assessment or determination regarding economic substance. The TIA may share information provided to it under the ES Act in accordance with international standards and arrangements.

In addition, if a fintech falls within the definition of a financial institution for the purposes of the US Foreign Account Tax Compliance Act (**FATCA**) or the OECD Common Reporting Standard (**CRS**), it will need to comply with exchange of information requirements, have in place appropriate policies and procedures, and submit all applicable FATCA and CRS filings.

There are no taxation laws or regulations in the Cayman Islands specifically related to digital assets.

In order to ensure compliance with all tax reporting obligations, fintechs should have in place robust accounting, governance and record-keeping policies and procedures to ensure all accounting records (including relating to virtual asset transactions) are accurate and up-to-date. Entities should also engage appropriately qualified advisers to assist with the determination of economic substance at set-up and annually thereafter and ensure all necessary filings are made in accordance with the prescribed deadlines.

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

As for all Cayman Islands entities, blockchain companies processing personal data must comply with the requirements of the Data Protection Act (2021 Revision) (**DPA**) and the Ombudsman's supplementary guidance. The DPA is based on EU-style data protection principles, including (i) the requirement for a lawful basis for data processing, (ii) data minimisation, (iii) compliance with international data transfer restrictions and safeguards and (iv) implementation of data protection policies and procedures.

Blockchain companies should ensure that technical architectures are built for compliance with the data privacy laws and good industry practice – which could include, for example, hashing, encryption, cryptographic techniques / masking, shielded transactions, use of private or permission chains, and off-chain storage for sensitive personal information. Companies should also have in place clear data handling and security procedures and conduct regular audits (including of their smart contracts).

The very nature of immutable blockchains poses challenges to compliance with data privacy laws (for example, data erasure requirements) and, like in many jurisdictions, the DPA has not kept pace with technological advancements. Data privacy requirements and privacy-first blockchain principles may also conflict with transparency or reporting requirements under financial services laws and international standards. We expect to see further innovation and regulatory developments in this area.

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?

The Cayman Islands has a comprehensive immigration and work permit regime primarily set out in the Immigration (Transition) Act (2021 Revision) and the Immigration Regulations. There are various options available to fintechs hiring international talent.

Employers can obtain work permits for skilled overseas workers to work and reside in the jurisdiction. Under the immigration laws, priority must be given to local, suitably qualified candidates for all roles and the jurisdiction benefits from an educated and skilled local workforce (particularly in accounting, compliance and fund administration). Permits may be expedited where there is a local skills shortage.

The Special Economic Zones (SEZs) operated by Cayman Enterprise City offer fast-tracked business set-up and five-year work permits (amongst other incentives) for innovative businesses satisfying the eligibility criteria. SEZ companies are exempt from certain work permit requirements, including the requirement to test the local labour market prior to hiring. The Technology City SEZ is popular with Web3, AI, blockchain and fintech companies.

A private initiative, Tech Cayman, also offers streamlined set-up, relocation and work permit packages to technology and intellectual property companies.

U.S. visa classifications like H-1B and L-1 do not affect hiring in the Cayman Islands, though may be relevant to a Cayman Islands fintech with operations or offices in the United States.

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?

At the outset, a new entrant should work with legal advisers to determine the optimal corporate structure and whether its proposed business activities fall within the regulatory perimeter and the economic substance regime. This will assist it to identify all applicable legal, regulatory and compliance requirements.

If the fintech will carry out regulated activities, it must apply for the relevant licence or registration from CIMA

before it commences those activities. Depending on the complexity, the application process can take several months and it is advisable for the fintech to seek early engagement with CIMA. Once licensed or registered, the entity must comply with all regulatory requirements, which include reporting, completion of annual surveys, notifying CIMA of material changes to its business. Regulatory capital requirements vary, depending on the nature of the entity and the scale of its business.

Entities falling with the AML/CTF/CPF regime (which includes all regulated entities) must comply with the AML laws and regulations and associated guidance and put in place policies, procedures and controls (see Q.6 above for more information).

Where the fintech will have a physical presence in the jurisdiction and hire staff, it will need to identify what trade and businesses licences (if any) and work permits it requires and understand the application process and timelines.

New entities processing personal data must put in place adequate policies, procedures and controls designed to comply with the DPA and ensure its staff are trained on such requirements.

New market entrants should engage professional advisers at an early stage to advise on establishing a business in the jurisdiction. Where senior management do not have experience in the jurisdiction, they should consider appointing one or more local directors and/or officers with deep knowledge of the jurisdiction's laws, regulations and business practices to guide them. Senior management should be aware of all material legal requirements (such as annual reports and filings) and ensure that regular risk assessments are conducted to monitor ongoing compliance with local laws and requirements.

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?

As with any new market entry – the entity should conduct a preliminary assessment of the commercial, legal and regulatory, and tax landscape of the jurisdiction. This could include engaging local service providers to advise on the market opportunities and competitive landscape if the fintech plans to provide services within the Cayman Islands.

A new fintech should consider seeking early engagement with CIMA and relevant industry bodies, such as Cayman Finance, to better understand the customer and regulatory environment and whether the entity is well-suited to doing business in the jurisdiction.

If a fintech intends to provide services to the local population, it should ensure it understands the fairly unique needs of the jurisdiction and its economy – for example, fund administration, wealth management and corporate services make up a significant proportion of the economy and fintechs in or complementary to these sub-sectors may have a larger market opportunity. Partnerships with local, regulated institutions may be regarded favourably by CIMA and could provide opportunities for customer acquisition and streamlined compliance processes (e.g. sharing of customer KYC information, where permitted).

We'd note it is more common for market entrants to establish a business in the Cayman Islands to service overseas customers rather than the local population, often setting up an 'exempted company' structure. For example, the Cayman Islands is the second largest jurisdiction for alternative investment funds globally and many global Web3 companies operate from the jurisdiction.

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 financial risks associated with fintechs entering the market primarily relate to the regulatory framework. It is imperative for fintechs to obtain professional advice to determine if its proposed activities will fall within the regulatory perimeter, given the potential penalties for undertaking regulated activities without authorisation. For regulated entities, the costs of initial set-up and licensing or registration with CIMA, as well as the ongoing costs of compliance, may be significant (particularly for small start-ups).

Where the fintech intends to have a physical presence, it should plan for the costs of hiring and operating in the jurisdiction.

Fintechs should engage with local service providers (lawyers, accountants, registered office providers and, if needed, compliance service providers) at an early stage

of planning to ensure they have a clear and comprehensive view of expected costs, timelines for various steps, and regulatory requirements.

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

Yes – generally entities can outsource business functions to external providers, including in other jurisdictions.

Entities subject to the economic substance regime may only outsource relevant activities to third-party service providers located within the Cayman Islands. Outsourcing cannot be used to circumvent the economic substance test (see Q.8 for more details).

Regulated entities must comply with the regulatory rules on outsourcing as set out in CIMA's 'Statement of Guidance: Outsourcing Regulated Entities 2023'. Requirements on outsourcing entities include that the entity must: conduct due diligence on the service provide and regular risk assessments of the arrangements; put in place policies, procedures and controls to monitor the arrangements; have a written outsourcing agreement containing mandatory provisions; and put in place and business continuity and contingency / exit plans. Responsibility and accountability for effective oversight of all regulated activities, whether outsourced or not, ultimately rests with the governing body and senior management of the regulated entity.

Where personal data will be transferred to other jurisdictions under an outsourcing arrangement, the entity must comply with the requirements on international data transfers set out in the DPA and Ombudsman's guidance (see Q.9 above). In short, personal data must not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data. Generally, data transfer agreements including the standard contractual clauses (SCCs) approved by the European Commission or the Ombudsman (once published) will satisfy this requirement.

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?

The Cayman Islands is a common law jurisdiction that has a robust intellectual property protection regime.

In 2017, the Cayman Islands updated its copyright laws to bring them in line with the most recent developments under the UK Copyright, Designs and Patents Act (as revised), which expressly includes computer programs and databases within the definition of "literary works" and therefore protects them as such for a duration of 50 years.

Patents and industrial designs registered in the UK or at the European level can also be protected in the Cayman Islands by extension with the Cayman Islands Register of Patents and Trademarks. In addition, the patent regime has been amended to provide innovators with additional protections against abusive challenges to their rights by entities that obtain patents for the sole purpose of taking legal action against those who innovate and develop new products. The Cayman Islands patent laws have been amended to prohibit bad faith infringement claims by so-called patent trolls.

Trade secrets are protected in the Cayman Islands through a combination of common law and rules of equity. A range of remedies are available where trade secrets have been improperly acquired, disclosed or used.

Confidential information is protected through a contractual agreement to keep certain information confidential or through the common law obligation to keep information confidential, because of the nature of the relationship between the discloser and disclosee, the nature of the communication or the nature of the information itself.

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

The main IP rights available to protect branding are registered and unregistered trade and service marks. Fintech companies will generally own a combination of an established brand or trade name — and this can include logos or icons — protected as registered or unregistered trademarks.

Trade mark rights give registered owners the right to prevent others using identical or confusingly similar marks to their registered mark. Brand owners can also rely on unregistered trade mark rights through the law of passing off. This allows the owner to prevent others from damaging their goodwill with customers by using branding or get-up that is identical or confusingly similar

to its own.

Since 2017, the Cayman Islands has had a standalone trade mark regime which requires separate examination and registration of new trade marks by the Cayman Islands Intellectual Property Office. Extension of existing UK or EU marks is no longer possible.

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?

Open-source code is not separately regulated or protected in the Cayman Islands. It is possible for every contributor to the open-source code to own the copyright to their contribution, although in practice most contributors are likely to agree to license their material under the same licence as the original work. It can sometimes be difficult to ascertain who should make a legal complaint if someone decides to use the program in a way that violates its licence. To avoid this issue, contributors can explicitly assign the copyright in their contributions to a centralised body that administers the open-source project, making enforcement of the licence easier. An alternative approach would be to have contributors license their contributions to the project's administrative body under a licence agreement that permits the body to relicense these individual contributions.

The following safeguards should be considered by fintechs when using open-source software:

- identifying and complying with any open source licence terms – for example, common licences such as MIT, Apache, and GPL have obligations relating to attribution, distribution and modifications;
- identifying and avoiding open source licence conflicts by reviewing licence agreements to ensure they are compatible. There is a risk that combining different licences to cover a single product could impose open-source obligations on proprietary code'
- implementing an open-source usage policy;
- maintaining an internal register of all open-source components to track licensing obligations; and
- monitoring all updates (including security patches and version updates) to ensure continued compliance and mitigate vulnerabilities.

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

Fintechs should identify their key markets and focus first on the intellectual property laws in those markets.

When negotiating contracts or licences with third parties it is important that the owner of the intellectual property is clearly defined. This includes defining ownership of any upgrades, improvements or new intellectual property developed during the course of the agreement. If ownership remains with the third party, fintechs should seek to secure an irrevocable and sufficiently broad licence to use and adapt the intellectual property for the fintech's core business. Fintechs should also obtain express assignments of rights from individual developers, including moral rights waivers where relevant, to ensure that all relevant intellectual property is owned by the entity.

Where the fintech owns the intellectual property, it should avoid granting perpetual licences and include owner termination provisions to ensure that there is no deemed assignment of any intellectual property to the licensee. Agreements should also contain robust non-disclosure obligations to prevent the loss of proprietary information.

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

To prevent potential infringements of intellectual property rights owned by the fintech company, it should actively monitor key markets and relevant online platforms (e.g. app stores, domain names) for any infringement indicators. To prevent hacks or theft of proprietary information, the company should put in place robust cyber security measures and ensure that any security patches and updates are actioned immediately.

Where an infringement is identified consider whether a cease and desist letter demanding immediate cessation of unauthorised usage or other court proceedings for injunctions and damages are appropriate.

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?

There are no specific laws, regulations or formal guidance addressing the use of artificial intelligence in the Cayman Islands in respect of financial services (including credit scoring or lending) or otherwise.

The following general principles under the DPA are relevant in the context of the use of AI in decision-making: (i) personal data must be processed fairly and (ii) data should be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected or processed. The Ombudsman's data protection guidance explains that the fairness principle means personal data must not be processed in a way that is unduly detrimental, unexpected or misleading to the individuals concerned, and that data controllers must be clear, open and honest with individuals about how and why it handles their personal data.

Specifically, section 12 of the DPA sets out requirements relating to solely automated decisions made by a data controller that significantly affect an individual (**Significant Automated Decisions**) – i.e. a process with no human involvement or mere token human involvement, such as where a human simply takes over the automated decision without any substantive appraisal. Ombudsman guidance gives the example of an automatic refusal of an online credit application as a decision having a 'significant effect'. Where there has been a Significant Automated Decision: (i) the individual may make a written request for the decision to be taken on a different basis than a solely automated basis and (ii) the data controller must, subject to certain exemptions, comply with an individual's written request to reconsider the decision or take a new decision otherwise than on a solely automated basis.

While the use of AI allows fintechs to use wider datasets to make decisions, the principle of data minimisation applies meaning that data controllers must identify the minimum amount of personal data it needs to fulfil its purpose (e.g. to make a credit decision) and not process any more than such minimum amount. Further, data controllers must review personal data held and delete any data no longer required (subject to any minimum retention periods required by law).

Generally, fintechs using AI algorithms for decisioning should adhere to industry good practice and frameworks for the responsible use of AI, to minimise the risk of bias or discrimination or other consumer harm. Such steps include:

- implementing robust policies, procedures and controls with an overarching governance framework and conducting regular audits;
- documenting the functionality / processes, data used and decision of AI models (including points of human intervention) and ensuring these are understood within the organization;
- completing regular testing and validation of AI models to identify potential bias and other issues; and
- ensuring that models are designed and developed in accordance with applicable laws and regulations.

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?

Please see our responses at section 4 above.

AI models and the code underlying them can potentially be protected by copyright (as software) in the Cayman Islands, provided they meet originality requirements.

Key model architectures, data sets, or training methodologies are trade secrets and should be kept confidential to maintain competitive advantage.

Fintechs should also take steps to ensure that licensing or third-party agreements protect the owner of the intellectual property and that robust cyber security measures are in place to prevent hacks and breaches.

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?

There are no financial regulations in the Cayman Islands governing the deployment of AI solutions and CIMA has not published any frameworks or guidance relating to AI. We anticipate that CIMA will consult on and introduce new regulations and guidance in the coming years, following the introduction of the AI Act in the European Union and guidance from other regulatory bodies such as the UK Financial Conduct Authority.

Fintechs must ensure their use of AI complies with existing financial laws and regulations and their ongoing

obligations, including relating to AML/CTF/CPF, cybersecurity and outsourcing. They should work closely with their compliance teams and locally appointed advisers to determine whether its AI solutions are compliant with the existing regime.

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

All fintechs using AI should include a comprehensive assessment of AI risks in their business risk assessments and consider mitigation steps for key legal risks. Mitigation steps could include:

- assessing what insurance coverage may be available to respond to legal risks associated with its use of AI (for example, under cybersecurity, product liability or directors and officers policies);
- designing decision-making processes to allow for human review or intervention, particularly for significant financial decisions with the potential to cause consumer harm (such as credit or mortgage decisions);
- disclosing the use of AI in decision-making, where appropriate, to consumers and ensuring there are avenues for review or redress;
- developing or implementing AI tools with data privacy and security principles in mind (e.g. data minimisation);
- if using third-party tools, performing due diligence and engaging trusted service providers;
- including AI-specific clauses in its service agreements with counterparties (for example, to exclude or limit AI-related liabilities, such as for defective performance); and
- having in place robust policies, procedures and controls and ensuring staff are trained on the acceptable and responsible use of AI.

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

Yes – the Cayman Islands has leveraged its position as a global financial services centre to attract fintech ventures, particularly in the realm of decentralized finance, digital assets, and other Web3-related projects.

The innovative Cayman Islands 'foundation company' structure is popular with decentralized autonomous organisations (DAOs), VASPs and other ventures, resulting in a huge number of Web3-related foundation companies operating from the jurisdiction.
In addition, the flexible funds regulatory regime and the broad network of professional services providers with expertise in Web3, means the jurisdiction is a leading domicile for funds investing in cryptocurrencies, blockchain and Web3 projects worldwide. Tokenised funds (where an investor's interest is represented by a cryptographic token) have proved particularly popular in recent years.

InsurTech is a growing area of disruption in the Cayman Islands, as the second largest domicile globally for captives and as an increasingly prominent jurisdiction for reinsurance and insurance linked securities (ILS). There are a number of insurtech companies with a presence in Cayman already, and the Class B(iii) insurance licence provides an attractive route for new insurtech reinsurers to set up in Cayman. Other Cayman-based insurers and reinsurers are increasingly focussed on ways to embrace insurtech to help better identify risks, take decisions, and manage exposures.

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

Technologies companies operating in blockchain, digital assets and Web3 are attracting particular investment. Generally, funding is at seed or Series A level. According to public sources (as at January 2025), there are 229 fintechs in the Cayman Islands and 68 of those have raised investment. 11 of those have secured Series A financing and three have achieved 'Unicorn' status (i.e. a valuation of US$1billion or more).

There are opportunities for the jurisdiction to accelerate growth of the fintech sector and attract a wider range of fintech business, particularly in WealthTech, InsurTech and RegTech. The opportunity for fintechs to raise capital is strong, given the high number of private equity and venture capital funds, high net worth individuals and family offices, and individual entrepreneurs located within the jurisdiction.

Contributors

Peter Colegate
Partner
pcolegate@applebyglobal.com

Dean Bennett
Partner
dbennett@applebyglobal.com

Marsha Williamson
Senior Associate
mwilliamson@applebyglobal.com

Ross McLeod
Associate
rmcleod@applebyglobal.com