Legal 500
Country Comparative Guides 2025

Japan
Fintech

Contributor

Anderson Mori & Tomostune

Ken Kawai

Partner | ken.kawai@amt-law.com

Akihito Miyake

Partner | akihito.miyake@amt-law.com

Kei Sasaki

Partner | kei.sasaki@amt-law.com

Takeshi Nagase

Partner | takeshi.nagase@amt-law.com

Kensuke Inoue

Partner | kensuke.inoue@amt-law.com

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

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

Japan: Fintech

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

In Japan, although there is no supervisory authority that regulates fintech companies in general, if the fintech company in question provides financial services, the company is primarily subject to the supervision by the Financial Services Agency (the "FSA").

For example, if a fintech company provides crypto asset trading services and the services fall under the category of CAES (defined below), the fintech company shall be regulated under the Payment Services Act (the "PSA"), which is under the FSA's jurisdiction.

In addition, if a fintech company engages in the business of remittances using electronic money, the business would fall under the category of 'fund remittance transaction (*kawasetorihiki*)' (Article 2, Paragraph 2, Item 2 of the Banking Act and Article 2, Paragraph 2of the PSA) and would be regulated under the Banking Act or the PSA under the FSA's jurisdiction.

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

At present, the Japanese Government is actively promoting fintech business and no imminent risks to the growth of the fintech market are envisaged.

Rather, in Japan, the term 'web3.0' has been incorporated into the Basic Policies for Economic Management and Reform from 2022, and its promotion is positioned as a national strategy. In fact, in April 2023, a web3 white paper was submitted by the 'web3 Project Team' of the Liberal Democratic Party ("LDP")'s Digital Society Promotion Headquarters, and the tax reform of crypto assets was specified in the tax reform guidelines, and there is active movement towards the development of a web3 business framework.

More recently, in April 2024, the LDP released a "Web3 White Paper 2024" that included a summary of issues needing immediate resolution for the promotion of Web3, as well as proposals for accompanying legislative revisions.

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

Depending on the nature of the services offered by a fintech company, it may be necessary to obtain a financial license.

For example, if a crypto asset exchange is to be operated for the trading of crypto assets, the business needs to obtain a registration as a CAESP (defined below).

In addition, if a business intends to operate a fund transfer business using electronic money, it falls under the category of fund remittance transactions and requires a banking license or a registration as a fund transfer business operator.

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

To encourage fintech innovation, including the development and usage of blockchain technology, in June 2018 the Japan Economic Revitalisation Bureau established a cross-governmental one-stop desk for a regulatory sandbox scheme in Japan. This scheme, available to foreign as well as to Japanese companies, enables applicants (once approved) to carry out, under certain conditions, a demonstration of their projects even if such activities are not yet covered under current laws and regulations. Blockchain technology, together with AI, IoT and big data, is explicitly mentioned in the basic policy of the regulatory sandbox scheme as a prospective and suitable area for exploration and development.

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?

When tokens issued by way of an initial coin offering ("ICO") or other type of tokens have the characteristics of securities, the Financial Instruments and Exchange Act (the "FIEA") will apply.

In summary, where distributions are made to token holders on the profits of a token issuer's business and calculated based on the ratio of a token holder's token

ownership, the token involved may constitute an electronically recorded transferable rights ("ERTRs") and consequently subject the token issuer to the provisions of the FIEA.

As ERTRs are expected to constitute Paragraph 1 Securities, a broker, an agency or an intermediary selling or purchasing ERTRs or handling a public offering of ERTRs in the course of business will be required to undergo registration as a Type I financial instruments business operator.

In addition, any ERTR issuer that solicits the acquisition of ERTRs (i.e., undertaking a security token offering) will be required to undergo registration as a Type II financial instruments business operator, unless it qualifies as a specially permitted business for qualified institutional investors.

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 Japan, AML rules are regulated by the Act on Prevention of Transfer of Criminal Proceeds (the "APTCP"). The APTCP requires "specified business operators" to conduct KYC and the like. The term "specified business operators" refers to business operators like fintech companies (among others) that are subject to financial regulations.

The APTCP is not directly applicable to unregulated fintech companies that do not fall within the definition of "specified business operators". Accordingly, the AML policies (if any) of such unregulated fintech companies would only be those they have established on their own initiative.

In the meanwhile, as CAESPs are included in "specified business operators", the APTCP will apply to CAESPs and the CAESPs are required to:

a. verify and record the identity of customers when conducting certain transactions (that is, to implement the KYC process);
b. record transactions with customers;
c. report suspicious transactions to the FSA; and
d. take measures to keep information regarding customer verification up to date, provide education and training for employees, and develop other systems necessary for the proper conduct of the processes described in points (a) to (c).

Travel Rule

When a CAESP transfers crypto assets to a customer of another CAESP (including any foreign CAESP) at the request of a customer, the transferring CAESP must notify the receiving CAESP of the identification information, including the name and blockchain address, pertaining to the sender and the receiver (the so-called "Travel Rule"). However, transfers to a CAESP in countries that do not yet have any Travel Rule legislation are not subject to the rule. In addition, when a CAESP transfers crypto assets to an unhosted wallet at the request of a customer, it is not subject to the Travel Rule. Nevertheless, even for transactions that are not subject to Travel Rules, information on the counterparty (such as name, blockchain address, and the like) must be obtained and recorded.

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?

Under the PSA, a person who engages in the purchase and sale of crypto assets as a business is required to be registered as a crypto asset exchange service provider ("CAESP") (Article 63-2 of the PSA). Only CAESPs are permitted to engage in CAES. The PSA requires a person who provides CAES (defined below) to be registered with the JFSA. A person who engages in CAES without registration is punishable by imprisonment for a term not exceeding three years or by a fine not exceeding JPY3 million, or both (Article 107, Item 5 of the PSA).

The term "crypto asset" is defined in the PSA as follows.

- A proprietary value (limited to that recorded on electronic devices or other objects by electronic means and excluding Japanese and other foreign currencies and currency-denominated assets – the same applies in the following bullet point) that:
  - may be used to pay an unspecified person the price of any goods, etc purchased or borrowed or any services provided;
  - may be sold to or purchased from an unspecified person; and
  - may be transferred using an electronic data processing system.
- A proprietary value that:
  - may be exchanged reciprocally for a proprietary value specified in the preceding bullet point with

  - an unspecified person; and
  - may be transferred using an electronic data processing system.

"Currency-denominated assets" means assets denominated in Japanese yen or another foreign currency. Such assets do not fall within the definition of crypto assets. For example, prepaid e-money cards are usually considered currency-denominated assets. If a coin issued by a bank is guaranteed to have a certain value vis-à-vis fiat currency, such a coin is unlikely to be deemed a crypto-asset but would instead be considered a currency-denominated asset.

The term "crypto-asset exchange services" means any of the following acts carried out as a business:

- sale and purchase of crypto-assets or exchange of crypto-assets for other cryptoassets;
- intermediary, brokerage or delegation of such sale, purchase or exchange;
- management of users' money in connection with the acts listed in the two bullet points above; or
- management of cryptoassets for the benefit of another person

Obtaining CAESP registration usually requires a registration review process that takes between 12 to 18 months and involves significant costs in order to establish sufficient internal management systems, including the recruitment of appropriate personnel. As a result, in recent years, many operators seeking to provide crypto asset-related services have been acquiring existing CAESPs in order to save time and costs in obtaining a CAESP registration.

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?

CAESPs who are members of the Japan Virtual and Crypto-assets Exchange Association ("JVCEA"), which is the self-regulatory organization for CAESPs, shall endeavour to deliver to their users an annual report describing the annual trading conditions and realised profits and losses, the state of valuation of deposited assets and valuation profits and losses as at the end of the year and other information (limited to information available to member CAESPs) which contributes to tax payment assistance for users (Article 18 of the JVCEA's self-regulatory rule 'Regulations Concerning Management and Explanation of Users Pertaining to the Crypto Asset Exchange Service').

In this way, CAESPs provide information to their users so that they can voluntarily and correctly file tax returns.

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

Business operators using blockchain technology may be subject to the Act on the Protection of Personal Information (the "APPI") if they handle personal information.

Considering that a public blockchain involves the sharing of a database among unspecified participants, where information on the blockchain will not in principle be deleted or retracted once uploaded on the blockchain, the use of blockchain technology may trigger the application of the APPI. For example, Article 19 of the APPI requires business operators who handle personal information to delete unnecessary personal information once the purpose for which such personal information was required has been achieved. However, a business operator that records the personal information of its users on a blockchain may have difficulty deleting such information, and this could result in a violation of the APPI.

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?

Immigration policies play a crucial role in the ability of fintech companies to set up a business and hire international talent in Japan. While the government of Japan has made strides in easing immigration policies in recent years, certain challenges and regulatory requirements still exist, especially in a highly specialized and competitive sector like fintech.

A foreign person who wishes to start a business in Japan must obtain a "business manager" visa. To obtain a "business manager" visa, it is generally required to (1) secure a physical and separate place of business, and (2) invest at least JPY5 million or employ at least two full-time staff members. However, under the Foreign Entrepreneurship Promotion Program, a foreign person who wishes to start a business in a municipality designated as a national strategic special zone may obtain a "business manager" visa for six months without meeting the above two requirements on the condition

that he/she submits a business plan and other prescribed documents to the relevant municipality and obtains the approval of the relevant municipality. It is also allowed to use a shared office for one year before securing a physical and separate place of business of its own.

The Foreign Entrepreneurship Promotion Program which is implemented in the national strategic special zones only has been recently merged into the Foreign Entrepreneurship Promotion Program, which is now available nationwide. Under the new program, a foreign person who wishes to start a business in Japan may apply for a so-called "startup" visa (*i.e.*, a "designated activities 44" visa) instead of a "business manager" visa, on the condition that he/she submits a startup preparation activity plan and other prescribed documents to a municipality or private sector entity approved by the Minister of Economy, Trade and Industry, and obtains a certificate for the visa application from the relevant municipality or private sector entity. A "startup" visa is effective for up to two years, which needs to be renewed every six months. While a "startup" visa holder must eventually convert their visa to a "business manager" visa, he/she may engage in startup preparation activities in Japan.

When a fintech company hires international talent such as financial experts and IT engineers in Japan, a so-called "working" visa (*i.e.*, an "engineer / specialist in humanities / international services" visa) is normally granted. The requirements for a "working" visa are (1) he/she will receive a salary at least equivalent to that received by a resident of Japan in the same position, and (2) he/she has at least the prescribed level of education or work experience in the field of the relevant technology or knowledge.

The government of Japan also has a "highly skilled professional" visa which is available for international talent who wish to work for a fintech company in Japan. A highly skilled foreign professional may apply for this visa if he/she earns the prescribed level of points in the items such as education, work experience and income. A highly skilled foreign professional who wishes to work for a financial industry may earn special points. A "highly skilled professional" visa holder may receive preferential treatments, such as a five-year period of stay in Japan, permission for his/her spouse to work in Japan, and permission for his/her parents and/or domestic workers to accompany him/her under certain conditions. Once such a visa holder has stayed in Japan for over three years, he/she may be allowed an indefinite period of stay in Japan.

Recently, the government of Japan introduced the "J-Skip" program, which offers further preferential treatment to a "highly skilled professional" visa holder who meets more stringent requirements. The government of Japan also introduced the "J-Find" program under which a foreign person who has graduated from a top-tier university in the last five years, has initial living expenses of JPY200,000, and wishes to engage in a job hunting or startup preparation activities in Japan, may apply for a so-called "future-creation individual" visa (*i.e.*, a "designated activities 51" visa). A "future-creation individual" visa holder may stay in Japan for up to two years.

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?

Like most other jurisdictions, Japan has stringent and complex financial regulations. When a foreign fintech company enters the Japan market, it is important to define its business model and to figure out, with the assistance of local legal counsel, whether it is required to obtain a license under the applicable laws and regulations of Japan at the initial stage. If a fintech company's business model falls under a regulated activity which requires a license, it is advisable to hire a local compliance officer who is familiar with the relevant laws and regulations and business sector. It is often the case that such a local compliance officer plays a leading role during the license application procedures. The following are examples of the major laws that may require a license for fintech companies acting in Japan or dealing with Japanese customers from overseas:

(1) The Financial Instruments and Exchange Act is applicable to those who engage in a financial instruments business such as an offering of securities or derivatives, investment advisory service, and discretionary investment management service;

(2) The Banking Act is applicable to those who engage in a banking business;

(3) The Trust Business Act is applicable to those who engages in a trust business;

(4) The Insurance Business Act is applicable to those who engage in an insurance business;

(5) The Payment Services Act is applicable to those who deal with payment tools such as prepaid payment instruments, crypto assets and stable coins, or who

engage in a money transfer business (but not in a banking business); and

(6) The Money Lending Business Act is applicable to those who engage in a money lending business (but not in a banking business).

A fintech company should also bear in mind that other laws and regulations will be also applicable to it when engaging in the fintech business in Japan. It is also important to hire a local compliance officer and, especially when facing with new issues, to consult with a local legal counsel to ensure adherence to all applicable laws and regulations. The following are examples of the major laws that may be relevant to fintech companies acting in Japan or dealing with Japanese customers from overseas:

(1) The Act on the Prevention of Transfer of Criminal Proceeds and Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism, issued by the Financial Services Agency, requires them to conduct AML/CFT measures such as KYC checks, transaction monitoring and record-keeping;

(2) Consumer protection laws such as the Consumer Contract Act should be also considered by those who deal with individual customers in Japan. In addition, if they offer their services via Internet, they must display certain notices on their website under the Specified Commercial Transaction Act;

(3) The Act on the Protection of Personal Information may be applicable to those who deal with personal information and personal data in their business; and

(4) The Guidelines for Cybersecurity in the Financial Sector, issued by the Financial Services Agency, require them to put in place a cybersecurity management system which performs risk assessment, identification of cybersecurity risks, cyberattack protection, cyberattack detection, cyber incident response and recovery, and third-party risk management.

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?

When a foreign fintech company enters the Japanese market, it is important to define its business model and try to have a clear picture of the target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions based on the chosen business model. It is advisable to conduct market research to understand the specific financial needs of different demographic groups and to analyze whether the business model is unique, well-differentiated from the competitors' products or services, and acceptable for Japanese customers in the competitive landscape. If the business model is complementary and helpful for the local financial institutions' business model, it is worth trying to establish partnerships with them.

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?

It is important to hire a local compliance officer, to consult with a local legal counsel, and to hire enough local staff to effectively mitigate these risks and to ensure both a smooth transition and sustainable growth. While we cannot identify any typical financial or operational risks associated with entering the market in Japan specifically, it is advisable to be mindful of such risks as cultural gap or reputation risk in the context of consumer behaviors and employment, currency exchange risk in light of the recent low interest rate and yen-depreciated environment, and increasing cybersecurity risks and personal data leakage risks.

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

Yes, Japan allows certain business functions to be outsourced to offshore locations generally, while certain regulated business functions may be outsourced only to a service provider which has a necessary license. Even in such cases, it is generally expected to monitor the service provider to ensure the appropriate performance of such outsourced business functions and compliance with the applicable laws and regulations. It is expected that the business will carefully consider what functions are to be outsourced depending on the nature of such outsourced functions. For example, it may be difficult to outsource customer support or call center services to an offshore location because these may require superior communication skills in Japanese. It is also advisable to be mindful of regulatory or operational risks, such as personal data security and cybersecurity risks, when

outsourcing the business functions handling personal data or using Internet.

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 Japan, fintech companies can protect proprietary algorithms and software through a combination of trade secrets, copyright protections, and patent eligibility, depending on the nature of the innovation. Trade secret protection is particularly significant and is governed by the Unfair Competition Prevention Act (UCPA). For algorithms or software to qualify as trade secrets, they must be kept confidential, provide commercial value, and remain undisclosed to the public. Companies can achieve this by implementing robust confidentiality measures, such as restricting access to sensitive information, enforcing non-disclosure agreements with employees and partners, and employing technical safeguards like encryption and secure storage.

Copyright protection under the Copyright Act also offers an important safeguard for software. Source code is automatically protected as a “program work,” preventing unauthorized reproduction or distribution. While registration is not a requirement for protection, fintech companies are encouraged to register their copyrights with the Agency for Cultural Affairs. Registration provides evidence of ownership and facilitates enforcement in cases of disputes or infringement.

Patent protection offers another avenue for protecting fintech innovations, particularly for software and algorithms with novel technical features. Under the Patent Act, software-related inventions are patentable in Japan if they solve a technical problem using technical means, are new and inventive, and have industrial applicability. For example, an algorithm that improves the efficiency of financial transactions or enhances cybersecurity could qualify for a patent. However, patenting requires public disclosure of the invention, so fintech companies should carefully evaluate whether the benefits of exclusivity outweigh the potential risks of revealing proprietary information.

A comprehensive protection strategy combines trade secrets to safeguard confidential know-how, copyright to protect source code, and patents to secure novel technical features. This multi-layered approach ensures that proprietary algorithms and software are well-protected against unauthorized use, misappropriation, or infringement while preserving the company's competitive advantage.

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

In Japan, a fintech company can effectively safeguard its trademarks and service marks to protect its brand identity by focusing on trademark registration, proper usage, and active enforcement of its rights. Trademark protection in Japan is governed by the Trademark Act, which provides exclusive rights to the owner of a registered mark for specific goods or services.

The first and most critical step is to register the trademark or service mark with the Japan Patent Office (JPO). Registration provides the company with exclusive rights to use the mark in connection with the goods or services it covers, as well as the ability to take legal action against unauthorized use by third parties. To ensure comprehensive protection, the company should carefully determine the appropriate classes of goods and services that align with its current business offerings and potential future expansions. Before filing, it is important to conduct a thorough trademark search to confirm that the proposed mark does not conflict with existing registrations, which could lead to refusal or legal disputes.

Once a trademark is registered, consistent and proper use of the mark is vital to maintain its validity and distinctiveness. A fintech company should develop internal guidelines for using the trademark across marketing materials, websites, and products to ensure it is used in a consistent manner that aligns with the registered form. This consistency strengthens the trademark's distinctiveness and prevents its dilution.

To safeguard its brand identity, a fintech company must also actively monitor the market for unauthorized or infringing uses of its trademarks. This can involve regularly reviewing trademark filings by other entities and monitoring online platforms and marketplaces. If an infringement is detected, the company can take action by sending a cease-and-desist letter or filing a lawsuit under the Trademark Act to seek remedies, including injunctive relief and damages.

In addition to these legal measures, fintech companies should build their brand reputation by associating the trademark with high-quality services, as a strong reputation further deters infringement. By registering trademarks, maintaining proper usage, and enforcing their rights, fintech companies in Japan can effectively

protect their brand identity and maintain a competitive edge in the market.

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 Japan, the use of open-source software (OSS) in fintech products carries both significant benefits and legal implications, as non-compliance with open-source licensing agreements can lead to serious legal consequences, including claims of copyright infringement under the Copyright Act. To minimize risks, fintech companies must carefully understand and comply with the terms of the licenses governing the OSS they use.

Open-source software is typically licensed under specific agreements, such as the GNU General Public License (GPL), Apache License, or MIT License. These licenses dictate how the software can be used, modified, and distributed. Some licenses, particularly those with “copyleft” provisions (e.g., GPL), require companies to disclose the source code of derivative works if the OSS is incorporated into their proprietary software. This obligation can conflict with the business models of fintech companies that rely on keeping their proprietary software confidential. Non-compliance with such provisions can result in legal action, including demands to cease distribution, release source code, or pay damages.

To ensure compliance with open-source licensing agreements, fintech companies should establish clear internal policies for OSS usage. This includes maintaining an inventory of all open-source components used in their products, along with their corresponding licenses and versions. Companies should conduct regular audits of their software to ensure that licensing terms are being adhered to, particularly when updating OSS components or integrating them into proprietary systems.

When selecting OSS, fintech companies should prioritize licenses that align with their business model. For example, permissive licenses such as the MIT or Apache License, which have fewer restrictions on commercialization, may be more suitable than copyleft licenses for certain projects. Additionally, companies should implement governance procedures to review and approve OSS usage, ensuring that legal and technical teams are involved in assessing compliance risks.

When distributing fintech products that include OSS, companies should comply with license requirements, such as providing attribution, including license texts, and disclosing source code if required. Failing to meet these obligations not only risks legal consequences but can also damage the company's reputation within the open-source community.

By understanding the legal implications of OSS and taking proactive measures to ensure compliance, fintech companies in Japan can harness the benefits of open-source technologies while minimizing legal risks and maintaining the integrity of their intellectual property.

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

In Japan, fintech startups must navigate the complexities of intellectual property (IP) ownership when collaborating with third-party developers or entering into partnerships by proactively addressing ownership, usage rights, and confidentiality through well-drafted contracts and clear communication. Failure to do so can lead to disputes, loss of proprietary rights, or unintended sharing of sensitive innovations.

The first and most critical step is to establish a clear, written agreement at the outset of any collaboration. This agreement should explicitly define the ownership of IP created during the partnership or development project. Fintech startups typically have two primary options: either retain sole ownership of all newly created IP or agree to joint ownership with the partner. Joint ownership, while sometimes unavoidable, can create legal and operational challenges, such as the need for mutual consent to license or enforce the IP. To avoid such complexities, startups are advised to include clauses assigning ownership of all developed IP to a single party, typically the startup itself, unless there are compelling reasons to share ownership.

In cases where third-party developers are engaged, startups should include **"work-for-hire" provisions** or IP assignment clauses in the contract. These provisions ensure that any IP created by the developer automatically belongs to the fintech startup, rather than the developer. If pre-existing IP owned by the developer is incorporated into the project, the agreement should grant the startup a perpetual, royalty-free license to use that IP in connection with the product.

To safeguard proprietary innovations and sensitive business information, confidentiality clauses are

essential. These clauses should obligate all parties to keep proprietary information secure and restrict its use solely to the scope of the collaboration. Non-compete clauses can further protect startups by preventing partners or developers from using shared IP to create competing products.

Startups should also address licensing rights within the agreement, especially if the collaboration involves joint development of software or technology. The contract should specify whether each party has the right to independently use, license, or commercialize the jointly developed IP and under what conditions.

Regular communication and thorough documentation throughout the project are equally important. Detailed records of contributions by each party, including versions of code, designs, or other deliverables, can help resolve disputes over IP ownership. Startups should also consider maintaining a secure repository for source code and other project materials, with controlled access granted only to authorized personnel.

Finally, fintech startups may benefit from legal reviews of all collaboration agreements by IP attorneys to ensure compliance with Japanese laws and to safeguard the startup's rights. By taking these proactive steps, startups can mitigate the risks of IP disputes and protect their innovative technologies in collaborative settings.

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?

In Japan, fintech companies can take several proactive and reactive steps to prevent and address potential intellectual property (IP) infringements, such as the unauthorized use of their technology or brand by competitors. A comprehensive approach that combines preventative measures, monitoring, and enforcement mechanisms is essential to safeguard IP assets effectively.

The first step is to secure formal IP rights by registering trademarks, patents, and copyrights with the appropriate authorities. For trademarks, registration with the Japan Patent Office (JPO) grants exclusive rights to use the mark in connection with specified goods or services. Patents provide robust protection for novel, inventive, and industrially applicable technologies, while copyrights automatically protect original software code and other creative works but benefit from registration for ease of enforcement. These registrations not only deter infringement but also provide the legal basis for pursuing remedies if unauthorized use occurs.

Prevention also involves implementing robust internal measures to protect trade secrets and proprietary information. Under the Unfair Competition Prevention Act (UCPA), trade secrets, including algorithms, software, and business strategies, are protected if they are kept confidential, provide business value, and are not publicly known. Companies should establish strict confidentiality agreements with employees, contractors, and partners, limit access to sensitive information, and implement technical safeguards such as encryption and access control systems.

Monitoring the market for potential infringements is another crucial step. Companies should regularly review trademark filings, online marketplaces, and competitor activities for unauthorized use of their IP. Technology tools such as automated web crawlers or trademark monitoring services can help identify potential violations more efficiently.

When infringement is detected, fintech companies should act swiftly and decisively. The first course of action is typically to issue a cease-and-desist letter to the infringer, clearly outlining the infringement and demanding that it stop immediately. This approach often resolves the issue without the need for litigation. If the infringement persists or is particularly egregious, the company can pursue legal remedies, such as filing a lawsuit under the relevant laws, including the Trademark Act, Patent Act, Copyright Act, or UCPA. Remedies may include injunctive relief to stop the infringing activity, monetary damages, and, in some cases, criminal penalties.

Additionally, fintech companies can mitigate the risk of IP theft by educating their employees and partners about IP rights and the importance of compliance. Regular training and clear internal policies can help create a culture of IP awareness and respect within the organization.

Finally, establishing relationships with IP attorneys and leveraging legal expertise early can help fintech companies strengthen their IP strategies and respond effectively to infringements. By taking these steps, fintech companies operating in Japan can protect their technological and brand assets while minimizing the risk of unauthorized use by competitors.

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?

As of January 2025, in Japan, there are no comprehensive laws regulating the use of AI by financial institutions or credit rating agencies. Therefore, whether the inappropriate use of AI constitutes a legal obligation violation boils down to whether it violates abstract obligations such as the soundness and proper operation of bank business. At present, there are no legally binding laws, supervisory guidelines, or standards that provide specific criteria for this. Consequently, there are no established methodologies or standards for demonstrating compliance.

However, the Japanese government, through the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications, published non-binding "AI Guidelines for Business Ver 1.0" on April 19, 2024 (available only in Japanese language).

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?

As of January 2025, there is no established theory in Japan regarding AI models and intellectual property rights, the protection of AI technologies and data sets, or the implications of using third-party AI tools.

The Japanese government's "Study Group on Intellectual Property in the AI Era" has been discussing the rights that generative AI might infringe upon, focusing on copyright law, design rights, trademark rights, and the Unfair Competition Prevention Act (including trade secrets). In May 2024, the "Interim Report on Intellectual Property in the AI Era" was published (available only in Japanese language). This report includes discussions on the handling of inventions utilizing AI, addressing issues such as the recognition of inventors and the assessment of inventiveness.

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?

Please refer to the answer to question 20.

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

Since there are no specific regulations unique to AI technology, it is important to comply with traditional regulations, specifically financial regulatory laws such as the Banking Act and the Financial Instruments and Exchange Act, as well as related IP and information laws such as the Copyright Act, the Unfair Competition Prevention Act, and the Personal Information Protection Act. Additionally, it may be crucial to actively provide information to relevant stakeholders and society at large, within a reasonable scope and considering privacy and trade secrets, to build trust based on the characteristics and uses of the adopted technology.

The examination of legal regulations and frameworks related to AI technology in Japan has just begun. Therefore, it is challenging to formulate definitive risk management strategies based on existing regulations. It is necessary to keep an eye on updates to the AI Guidelines for Business and other developments from the government and related committees, as well as the regulatory trends in other countries.

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

Most fintech start-ups in Japan seek collaboration with traditional financial institutions. Traditional financial institutions have already invested in fintech start-ups including blockchain tech companies. Accordingly, we seldom see disruption by fintech businesses. This trend is expected to continue.

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

The fintech landscape in Japan appears to be vibrant, especially with digital payments, blockchain/cryptocurrency, and other services like RegTech and InsurTech leading the investment trends. Startups at various funding stages, from Seed to Series B, appear to be attracting investment, with a notable

emphasis on early-stage funding, as investors seek to support companies in establishing a market fit and scaling operations. The areas seeing the most significant investment are often those that are leveraging cutting-edge technology like AI, blockchain, and automation and that disrupt traditional financial services.

Contributors

Ken Kawai
Partner
ken.kawai@amt-law.com

Akihito Miyake
Partner
akihito.miyake@amt-law.com

Kei Sasaki
Partner
kei.sasaki@amt-law.com

Takeshi Nagase
Partner
takeshi.nagase@amt-law.com

Kensuke Inoue
Partner
kensuke.inoue@amt-law.com