Legal 500
Country Comparative Guides 2025

Switzerland
Fintech

Contributor

MLL Legal

Dr. Kilian Schärli

Managing Partner | kilian.schaerli@mll-legal.com

Dr. Reto Luthiger

Partner | reto.luthiger@mll-legal.com

Prof. Dr. Andreas Furrer

Special Counsel | andreas.furrer@mll-legal.com

Andrea Trost

Senior Associate | andrea.trost@mll-legal.com

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

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

Switzerland: Fintech

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

The Swiss Financial Market Supervisory Authority (FINMA) is competent for issuing licenses under the financial market laws (including fintech licenses) and for market supervision in Switzerland. FINMA is also responsible for enforcing the financial market regulations and for investigating related infringements. The basis of the regulatory framework is established by federal laws issued by the Parliament, which are developed or specified in ordinances issued by the Federal Council and, in certain cases, further specified in FINMA ordinances. The regulatory practice of FINMA is reflected in circulars, guidelines and guidances.

For anti-money laundering-only supervision, fintech businesses that are not prudentially licensed (fintech license or other) but that act as financial intermediary must affiliate and be supervised by a private self-regulatory organisation that is recognised and supervised by FINMA.

FINMA has established a "fintech desk", which pre-assesses the regulatory qualification of fintech business models that voluntarily request such a pre-assessment from FINMA. The fintech desk can further be approached when in doubt about the interpretation of a specific regulation.

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

We do not foresee any imminent risks to the growth of the fintech market in Switzerland. On the contrary, the Swiss fintech industry has maintained a rapid rate of innovation. Never before have there been more active companies in the Swiss fintech sector, totalling 483 at the end of 2023 which was an increase of 11% compared to the previous year according to the FinTech Study 2024 of the Lucerne University of Applied Sciences and Arts.

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

Yes, if the fintech company intends to accept public deposits of fiat or cryptocurrencies of more than CHF 1 million the company needs a fintech license. Switzerland introduced the fintech license (or "banking license light") to encourage innovation in the financial sector. The fintech license allows institutions to accept public deposits of up to CHF 100 million in fiat currency or cryptocurrencies theoretically in an unlimited amount but is subject to the discretion of FINMA, as long as they neither pay interest on nor do proprietary trading/investing with such client funds. Fintech licenses are useful for various business models such as crowdlending platforms, trading platforms, payment, account and card services and others. These business models commonly rely on service fees as their revenue source.

Fintech companies that do not accept public deposits but that act as financial intermediaries, e.g. because they provide services related to payment transactions or carry out credit transactions, are still subject to the Anti-Money Laundering Act (AMLA) and need to affiliate with a self-regulatory organisation.

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

The unsupervised and unregulated sandbox can be used by (fintech) companies that accept funds from the public of up to CHF 1 million. As a general rule, only banks with a banking license or fintech companies with a fintech license may accept deposits from the public. The requirements for such a banking or fintech license are onerous, and in particular for the banking license rarely met by start-ups. Therefore, the sandbox was introduced in 2017 in the Banking Act for companies in their initial market testing phase. Fintech start-ups can experiment in the market within the sandbox framework and then grow further with the fintech license or even with a banking license. To be eligible for the sandbox, public deposits must not exceed CHF 1 million in total and no interest must be paid on the deposits. In addition, depositors must be informed before making a deposit that the business is not supervised by FINMA and that the deposit is not covered by the deposit guarantee. The AMLA may still apply and an affiliation with a self-regulatory organisation could be required.

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?

There is no uniform law governing ICOs in Switzerland. Depending on the qualification of the crypto assets, different provisions may apply. There is generally no FINMA authorisation requirement for conducting an ICO, unless a crypto asset is deemed a derivative or if there is a repayment obligation of the issuer. In these cases, authorisation as a securities firm or a banking license may be necessary, with exceptions.

FINMA has issued practical guidance to categorise crypto assets based on the underlying economic function and applies existing financial market regulations to the crypto asset itself, its issuance and transfer. From a regulatory point of view, FINMA differentiates between three different types of crypto assets and refers to these as:

- payment tokens: synonymous with cryptocurrencies, these are tokens intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money, value storage or transfer. Cryptocurrencies give rise to no claims on their issuer. Payment tokens neither qualify as securities nor as financial instruments;
- utility tokens: intended to provide access (digitally) to applications or services through a blockchain-based infrastructure. If a utility token functions solely or partially as an investment in economic terms, FINMA will treat them as securities (ie, in the same way as asset tokens); and
- asset tokens: represent assets such as a debt or equity claim against or in the issuer. These tokens qualify as securities, bonds, derivatives or structured products. FINMA regards asset tokens mainly as securities.

The individual token classifications are not mutually exclusive (eg, both asset and utility tokens can be classified as payment tokens (hybrid tokens)).

An ICO of a payment token triggers, in principle, obligations under the AMLA. The issuer either has to become a member of a self-regulatory organisation or engage a third-party financial intermediary where the payment tokens are issued all at once and not on a continuous basis. However, payment tokens qualify as securities as long as they are not operational on a blockchain.

An ICO of a utility token is not subject to the AMLA if the functionality of the token pertains to access to the blockchain for mainly non-financial purposes.

An ICO of an asset token may lead to the obligatory publication of a prospectus or information sheet under the Financial Services Act (FinSA) unless an exemption applies. Further, a person acquiring the asset tokens from the issuer and publicly offering them in the primary market (underwriting) will require a license as a securities firm.

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 professional purchase and sale of crypto assets against fiat (e.g. Swiss francs) but also between different crypto assets, constitute a currency exchange (a two-party transaction) or money remittance (a three-party transaction) activity subject to the AMLA unless the crypto assets qualify as asset token or pure utility tokens.

The AMLA, and the corresponding ordinance, stipulate the obligations that must be performed by financial intermediaries subject to those laws. Entities that offer currency exchange or money remittance services within the scope of the AMLA and that are not prudentially supervised must join a self-regulatory organisation recognised by FINMA. Self-regulatory organisations impose, based on federal law, their own more specific rules and supervision regarding AML compliance on their members.

Within the scope of the AMLA, the following typical duties apply:

- client identification;
- residence address check;
- verification of beneficial ownership;
- assessing for increased risks, such as high-risk countries (residence, citizenship), high-risk industries, politically exposed persons (PEP);
- the sourcing of funds and wealth;
- documentation duties;
- notification duties;
- the freezing of assets in case of suspicion of money laundering or terrorist financing;
- sanction checks.

The extent of the aforementioned obligation may vary depending on the services or activities and the number of Swiss francs collected or transferred.

In the case of spot money exchange transactions with parties with which *no permanent business relationship* exists, for example, the contracting party must be identified if there is a minimum of CHF 5,000 or CHF 1,000 respectively in transactions with cryptocurrencies (payment tokens) and its beneficial owner must be identified if there is a minimum of CHF 5,000. The changer must take appropriate measures to ensure that the wallet is that of the customer (a two-party transaction) and not that of a third party. Otherwise, it would be a money remittance activity and the identification obligation would apply to zero Swiss francs for outbound transactions and CHF 1,000 for inbound transactions. An intensified duty to monitor transactions with cryptocurrencies exists, whereby the changer must implement suitable technical precautions to prevent any transactions from exceeding the threshold of CHF 1,000 within a period of 30 days.

In cases of money exchange transactions with cryptocurrencies (payment tokens) that entail a *permanent business relationship*, the AMLA duties are fully applicable.

Concerning transactions of payment tokens, financial intermediaries must apply the Travel Rule on every transaction, including transactions to wallets held with unregulated wallet providers (ie, stating the name, address and wallet address of the sending party and the name and wallet address of the receiving party).

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 government's general approach is to create the best possible framework conditions to enable Switzerland to establish itself and evolve as a leading, innovative and sustainable location for cryptocurrency and blockchain companies. Moreover, its goal is to consistently combat abuse, particularly in the fields of money laundering and terrorist financing, and to ensure the integrity and good reputation of Switzerland as a financial center and business location.

Thus, Switzerland with its principle-based laws and regulations and being technology neutral, is very flexible towards new technologies and business models and has established as a key player in the field of crypto assets. Further, the federal and cantonal legislative and governmental bodies are willing to accommodate these innovative approaches. In particular, the Canton of Zug, also known as the "cryptovalley", has attracted numerous international players in the fintech sector due to its business-friendly environment and competitive tax system.

For legal certainty, projects can file a so-called "non-action letter" to obtain confirmation from FINMA that a certain project is not subject to any financial market laws.

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?

To date, cryptocurrency companies and other providers of digital assets services are not subject to tax reporting requirements that are specific to digital assets. Accordingly, they must follow the general rules applicable to all financial assets, subject to certain guidelines that aim at facilitating the qualification of crypto assets from a Swiss tax point of view and the correct reporting by investors of taxable income and taxable wealth that is associated with investments in crypto assets.

The tax year for Swiss resident individuals runs from January 1 to December 31, and every holder of digital assets must be in a position to declare the income generated by such assets during each calendar year and its year-end market value. Capital gains realized by Swiss resident investors on privately held assets, including capital gains on the disposal of cryptocurrency and other digital assets, are not subject to income tax.

First and foremost, Swiss resident issuers of crypto asset are required the determine whether they are subject to a Swiss withholding tax obligation as a result of such asset being assimilated to a bond, a bank deposit, an equity instrument or a share in a collective investment scheme.

Crypto funds that qualify as collective investment schemes and that have been registered for distribution in Switzerland to non-qualified investors are required under the Swiss Collective Investment Schemes Act to report to the Swiss Federal Tax Administration (SFTA) net asset values as at December 31 of each calendar year, as well as income generated during each calendar year, while taking care to segregate the portion of the fund's annual return that stems from capital gains.

Switzerland has undertaken to implement the OECD's Crypto-Asset Reporting Framework (CARF) and will therefore be expanding international automatic exchange

of information in tax matters (AEOI) to crypto assets as from 1 January 2026 under the CARF requirements. Accordingly, Swiss providers of crypto services and specifically crypto banks will be required to document their clients in accordance with the CARF and report non-Swiss resident clients to the Swiss Federal Tax Administration (SFTA). The SFTA will act as the body responsible for forwarding information to the foreign clients' countries of domicile.

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

Although it is undisputed that personal data can be processed in blockchains and other decentralised networks and that numerous data processing operations in blockchains constitute personal data processing under Swiss data protection law, a case-by-case assessment is required. For example, it is disputed whether the public key already qualifies as personal data.

As soon as personal data is processed in the blockchain, the obligations of the Swiss Federal Act on Data Protection (FADP) must be observed. This concerns in particular the data processing principles according to Art. 6 FADP. Data processing must be lawful, it may only be carried out for predetermined purposes (purpose limitation), it must be carried out transparently, i.e. the data subjects must be informed about the processing of their data in the blockchain (transparency requirement and information obligations), the data processing must be proportionate to the purpose of the processing and the processed data must be correct and remain correct over time. One of the most important principles is the requirement for transparency, which is supported in the FADP by a formal duty to provide information. Art. 19 FADP requires that data subjects be informed about the data being processed, the purpose of the data processing and the transfer of data to third parties. This information is regularly provided in the form of a data protection declaration. However, in the context of blockchains, it is necessary to check in each individual case how these data protection declarations are implemented and how they can be brought to the attention of the data subjects.

In addition to the data processing principles and the duty to provide information, there are further obligations in the FADP that may become relevant in connection with blockchains and that blockchain companies must take into account:

- Data Privacy by Design und by Default: The processing of personal data on chain should be minimized. Blockchain companies can avoid storing personal data directly on the blockchain. Instead sensitive personal data may be stored off-chain, but be linked to the blockchain by using cryptographic hashes or pointers (e.g., IPFS) on-chain. Blockchain companies should consider using and implementing privacy-preserving technologies like pseudonymization of data, homomorphic encryption or secure multiparty computation (SMPC). Even if blockchain records are public, personal data should not be easily linkable to specific individuals. It is important to consider data privacy concerns already at the beginning of a blockchain project so that the design and architecture of the blockchain already respect data privacy concerns.
- Cross-Border Data Transfers: If the blockchain involves nodes outside Switzerland, blockchain companies need to ensure that data transfer agreements comply with Swiss data transfer restrictions or use mechanisms like Standard Contractual Clauses (SCCs).
- Data Subject Rights: The FADP contains various rights that data subjects can assert against the controller. These include the right to information about the processing of one's own data, the right to deletion and the right to be forgotten. It is undisputed that the implementation of some of these rights in the blockchain is difficult or technically almost impossible. In particular, the right to be forgotten contradicts the immutability of information in the blockchain. Although there are ways to change data in blockchains and thus individual blocks afterwards, this is not in the sense of the blockchain. Here, too, it is crucial that these aspects are considered at the beginning of a project and incorporated into the decisions on the design and architecture of the blockchain.
- Data Security and Cybersecurity Measures: Where possible, pseudonymisation, anonymisation or encryption of personal data in the blockchain is a security measure. Other security measures include the use of multi-signature wallets for managing sensitive data to prevent unauthorized access as well as regular security audits of on-chain and off-chain components to identify vulnerabilities. For data security and general compliance reasons, blockchain companies should maintain detailed logs of data processing activities, even in decentralized networks, for auditability.
- Regular Compliance Reviews: Blockchain companies should regularly monitor changes to Swiss and international privacy laws to remain compliant. If necessary, companies should adapt the privacy-

related measures.

The aforementioned obligations, including the obligation to comply with the data processing principles, apply to the so-called controller, i.e. the natural or legal person who, alone or together with others, decides on the purpose and means of the data processing. When data is processed in blockchains or by means of blockchains, it is not always easy to determine who the controller is. It is therefore necessary to check in each individual case which player must comply with the obligations of the FADP. It is controversial and depends on the individual case whether, for example, full nodes qualify as controllers. Depending on the circumstances, the designer of the blockchain may also be the controller or co-controller.

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?

In accordance with the Free Movement of Persons Agreement between the European Union (EU) and Switzerland EU/EFTA citizens have the right to enter, remain and take up gainful employment in Switzerland as employees or in self-employed capacity without a visa. Therefore, as there are no immigration obstacles for EU/EFTA nationals, fintech companies already have access to a significant talent pool.

Non-EU/EFTA nationals require a work permit, even for short-term employment. The number of permits issued is limited. Only qualified non-EU/EFTA nationals may work in Switzerland. The future employer must further demonstrate that the employment is in the economic interest of Switzerland and that they were unable to recruit the necessary personnel in Switzerland or from an EU/EFTA member state. Since 1 January 2021, UK nationals are no longer citizens of the EU and are therefore subject to the same rules that apply to third-country nationals, including quotas.

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?

Only companies limited by shares, corporations with unlimited partners or limited liability companies that have their registered office and conduct their business activities in Switzerland can obtain a fintech license from FINMA. A fintech license is subject to simplified regulatory requirements compared to the banking license. Specifically, fintech companies are not subject to banking equity ratio requirements or liquidity requirements. The capital requirements are also less stringent for fintech companies: They must hold a minimum amount of capital of 3% of the public deposits or cryptocurrencies (payment tokens) received, but not less than CHF 300'000.

The requirements for a fintech license include (among others):

- fully paid-up minimum capital of at least 3% of the accepted payment token but not less than CHF 300,000;
- guarantee of irreproachable business activity by qualified participants and members of ultimate strategic and executive management;
- precise factual and geographical description of the business in the articles of association and business rules (business must be compatible with the entity's finances and organisation);
- management of the entity from Switzerland;
- partial separation of ultimate strategic and executive management;
- effective risk management, in particular effective identification, assessment, management and monitoring of the risks associated with its business and effective internal control system, which ensure compliance with legal and internal company regulations;
- appointment of a recognised audit firm for the licensing process; and
- appointment of a recognised regulatory audit firm for ongoing supervision.

The public funds collected by the fintech company must be either kept separate from the company's own funds or recorded in a manner that allows for separate reporting at any time. The latter option requires the fintech company to undergo a regular audit. Further, the anti-money laundering requirements are fully applicable.

FINMA is responsible for granting the fintech license. Upon receiving license applications, FINMA assesses whether the intended business activities require a license and whether the planned business activities are possible under the terms of the fintech license. To simplify the application process, FINMA has published guidelines. It is also possible to present a project to FINMA prior to submitting an application.

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?

Market conditions for fintech companies in Switzerland are generally considered favorable due to its political stability, a strong currency, low inflation, broad access to credit and venture capital, an educated workforce (Switzerland is home to world-class research institutions and universities), years of experience in the banking sector and widespread access to and use of information and communication technology.

Not being part of the EU, Switzerland has its own economic position and in general an affluent population of around 8.85 million. Fintech market entrants should evaluate their ability to cover the German, French and Italian-speaking regions of the country which also have distinct cultural and economic differences.

In terms of competitive landscape there are two crypto banks in Switzerland (Sygnum and AMINA (formerly SEBA)) that have a full banking license and that are at the forefront of crypto and fintech with services and products developed themselves. These crypto banks provide their own infrastructure as outsourcing providers to many existing traditional banks, including many private banks but also an increasing number of Cantonal banks, in particular for custody, brokerage and staking of cryptoassets. Non-crypto fintechs often collaborate intensively with existing banks based on a banking-as-a-service model in order to avoid obtaining a complex and costly banking license.

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 risk of money-laundering remains high for fintech companies and for companies with a crypto-offering. Cryptocurrencies are increasingly used in cyberattacks or to finance illicit activities. Breaches of due diligence obligations under the AMLA can result in serious legal consequences and reputational damage for the fintech in question. Furthermore, sanctions both in general and specifically those related to the war in Ukraine continue to pose operational risks for supervised institutions. On 28 February 2022, the Swiss Federal Council decided to follow the EU's sanctions against Russia by enacting a new Ordinance on Measures in connection with the Situation in Ukraine on 4 March 2022 (Ukraine Ordinance). The Ukraine Ordinance not only encompasses the usual financial sanctions against certain listed individuals, companies and organisations, but also bans on providing certain financial services, including certain services in connection with crypto-based assets to Russian nationals and individuals and businesses based in the Russian Federation. Fintech companies are required to adequately identify, limit and monitor all anti-money laundering and sanction risks and to establish an effective internal control system.

The outsourcing of significant functions to third-party providers poses operational risks for fintech companies. Outsourcing has continued to increase in recent years and financial companies are increasingly dependent on service providers to perform important functions. Interruptions and outages of critical functions and third-party service providers poses a significant risk. Further, cyberattacks are often carried out via third-party providers. Fintech companies are therefore required to identify, monitor, quantify and control the main risks associated with outsourcing. The outsourced function must be integrated into the company's internal control system and a unit within the company should be named as responsible for monitoring and controlling the service provider so that any necessary measures can be taken promptly.

Fintech companies are also a target for cyberattacks. The risk is higher where critical sanctions are outsourced. Fintech companies are therefore advised to avoid weaknesses in the IT infrastructure and to implement adequate security measures and raise awareness.

Furthermore, the use of artificial intelligence (AI) by fintech companies is increasing which not only provides opportunities but also poses risks. In December 2024 FINMA issued its new Guidance on Governance and Risk Management when using Artificial Intelligence in which it identified various risks from the use of AI by supervised institutions, in particular operational risks but also IT, cyber, legal and reputational risks and emphasized the need for supervised entities (including fintechs) to properly identify, calibrate and manage such risks.

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

Yes. The outsourcing of business functions to another

country (including to offshore jurisdictions) is permitted as long as the restructuring or resolving of the outsourcing entity in Switzerland can be assured and it is possible at all times to access information required for this purpose in Switzerland. The outsourcing entity must be able to guarantee that it, its audit form and FINMA can assert and enforce their inspection and audit right.

As a general rule, the outsourcing of business functions does not require the approval of FINMA but the requirements of the FINMA Circular 2018/3 Outsourcing (FINMA Outsourcing Circular), which also applies to holders of the fintech license, and the relevant data protection laws must be complied with. As the outsourcing entity remains responsible for the outsourced functions, it must ensure the proper selection, instruction and control of the third-party provider. This includes conducting a risk analysis that takes account of the main economic and operational considerations as well as associated risks. All outsourcing agreements must clearly set out assigned responsibilities, as well as audit and inspection rights. The outsourcing entity further has an obligation to keep an inventory of all outsourced functions with a proper description of the outsourced functions, the name of the service provider and any subcontractors, the service recipient and the person or department responsible within the outsourcing entity. If a significant function is outsourced, the service provider is subject to information and reporting duties to, and audits by, FINMA.

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?

Under Swiss law, a patent is an intellectual property right for a technical invention. A patent allows fintech companies to prevent others from using their invention for commercial purposes for up to 20 years. The patent owner decides who is allowed to produce, sell or import its invention in those countries in which the patent is valid. The patent owner can also trade the patent, e.g. sell it or license the use of the invention.

An invention uses technology to solve a specific problem. The technical features of an invention have a function through which the problem is solved. The technical character necessary for patenting requires that the laws of nature are used to achieve the objective. The invention can be a product or a process. Fintech innovations are eligible for patent protection if the invention is new, inventive and industrially applicable:

- Fintech inventions must not form part of the state of the art (all knowledge that has been made publicly available anywhere in the world prior to applying for a patent; including printed and online publications, as well as public lectures and exhibitions).
- The invention must not be obvious to a person skilled in the art (a hypothetical person who knows the prior art in his specialist field but is unimaginative).
- The invention must be industrially applicable and practicable, and it must be possible to replicate its implementation.

Whereby program-related technical inventions such as electronic control systems are patentable, computer programs as such cannot be patented in Switzerland. Nonetheless, the source code of computer programs is protected by copyright. However, algorithms which form the basis of software are excluded from protection. Copyright protection automatically applies from the moment a work is created.

Additionally, fintech companies can implement licensing agreements to safeguard their algorithms and software while allowing third parties to use the fintech innovation.

Finally, handling internal know-how as a trade secret can be key for new fintech projects to develop. This can happen by means of contractual confidentiality provisions and internal guidelines to be agreed with employees and business partners.

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

Under Swiss law, a trademark is a protected sign that distinguishes a company's products or services from those of other companies. All graphical representations of a sign can in principle be a trademark within the meaning of the law, for example words, combinations of letters, numbers, graphic images, three-dimensional forms, slogans, combinations of these elements, or even sound trademarks, which are made up of a sequence of notes. A strong trademark can help fintech companies to differentiate their products and services from their competitors. Given that fintech companies are often stewards of important financial assets and documentation, a reputable trademark is likely to be important to customers.

Fintech companies can register their trademarks with the Swiss Federal Institute of Intellectual Property. For broader international protection, registration of the trademark under the Madrid System is recommended.

The international application can also be conducted with the Swiss Federal Institute of Intellectual Property. To effectively maintain the integrity of their trademarks, fintech companies shall further implement regular monitoring mechanisms to promptly identify and address potential trademark infringements.

Unfair competition law adds additional protection in case of products or services being reproduced by third parties in confusion of customers.

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?

While open-source software (OSS) provides numerous advantages to fintech companies, including increased flexibility and cost savings, its utilization requires careful legal consideration. In Switzerland, the source code of computer programs is protected by copyright. Copyright protection grants developers several exclusive rights, such as the ability to control the reproduction, modification, and public availability of the software. While OSS is frequently free of use, fintech companies must nevertheless ensure compliance with the contractual obligations established by the OSS developers. Therefore, numerous legal implications should be carefully assessed, including:

- Licensing: Generally, it is essential to review the conditions of the specific OSS license to fully comprehend the obligations it imposes, even if the software is used for internal purposes within a fintech company. For example, pursuant to the GNU General Public License (GNU GPL), internal distribution of OSS within a company does not constitute distribution that imposes specific obligations. However, when the company provides copies, for instance, to contractors for off-site use, this constitutes distribution, thereby triggering certain obligations. Depending on the terms of the relevant license, the fintech company may, among other obligations, be required to disclose the source code or provide attribution to the original OSS developers.
- Control and ownership: Subject to the terms of the applicable OSS license, incorporating OSS may impose restrictions on the control and ownership of the company's intellectual property rights pertaining to the software (e.g., any modifications made to the software may be required to be made publicly available under the same terms as those specified in the applicable OSS license). Furthermore, the original OSS developer might retain all intellectual property rights, including those related to the source code, as well as any associated patents or trademarks. Additionally, most open-source licenses do not offer patent indemnification, nor do they typically include explicit patent grants or liability protection. While companies may file patents on their contributions to OSS projects as they relate to new inventions, they must ensure compliance with the terms applicable to the open-source project.
- Security and liability: In sectors such as fintech, companies are particularly vulnerable to risks due to the sensitive nature of financial data. Therefore, the use of OSS requires fintech companies to implement robust security strategies to identify and address potential vulnerabilities in the applied OSS. This may include vulnerability scanning and patch management, continuous monitoring and the implementation of security protocols to ensure the integrity of the OSS. Damage resulting from the use of OSS may give rise to legal liability, as most OSS providers do not offer warranty protections. For example, the GNU GPL provides no warranty for its free software. Therefore, modified versions must be marked as such to prevent the erroneous attribution of any issues to the authors of previous versions.

Fintech companies can ensure ongoing compliance with OSS agreements through various means, including the implementation of (i) policies governing, inter alia, the usage, modification and distribution of OSS, (ii) license management to maintain a record of all applied OSS components, (iii) continuous monitoring and compliance management to ensure that the company remains in adherence to the terms of the applicable OSS license(s).

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

Fintech startups must address certain considerations to navigate the complexities of intellectual property ownership and to ensure the protection of their intellectual property during collaborations and partnerships. These considerations include the following:

Firstly, startups should – at the earliest stage possible – implement an intellectual property portfolio management to document the ownership and rights associated with all intellectual property assets. This approach will help mitigate potential conflicts, particularly when engaging in

multiple partnerships or collaborations. Accordingly, when entering into such agreements, the ownership and rights to intellectual property shall be clearly defined, addressing both pre-existing intellectual property rights and those developed during the partnership or collaboration. In particular, the agreement should also include exiting terms that specify the intellectual property rights retained by each party and clarify the management of any proprietary information. Fintech startups should also ensure that their intellectual property protection extends not only to their own territory of operations but also to the jurisdiction the third-party company operates from.

Furthermore, handling the internal know-how as a trade secret can be key for fintech startups and new fintech projects to develop (please refer to question 15 for further details). In addition, non-disclosure agreements (NDAs) provide a mechanism to ensure confidentiality and proper handling of sensitive information.

Finally, once a collaboration or partnership has been established, it is essential to conduct regular audits to ensure ongoing compliance with the agreed terms (e.g., checking of product developments, marketing materials and public disclosures).

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?

The development of a robust and diversified intellectual property portfolio is essential. This will require regular intellectual property audits to ensure that all assets are identified and adequately protected.

As outlined above, fintech companies should focus on protecting their source code for computer programs through copyright. If applicable, early patent filing is essential for fintech companies to gain a competitive advantage. Given the global nature and reach of fintech businesses, using mechanisms such as the Patent Cooperation Treaty (PCT) can facilitate the filing process and extend protection across multiple jurisdictions. In this regard, fintech companies should ensure that the technical aspects of their algorithms and software are thoroughly detailed to ensure clear and precise patent claims. Additionally, trademark protection in particular plays a crucial role in differentiating the products and services of the company from those of its competitors (please refer to questions 15-17 for further details). Finally, fintech companies may register unique creative forms for design protection, encompassing both two-dimensional designs and three-dimensional forms.

Once established, fintech companies should monitor the market for potential infringements and take appropriate measures to enforce their intellectual property rights if required. The enforcement of intellectual property rights may involve issuing cease and desist letters to infringers, demanding the cessation of unauthorised use of protected intellectual property. Should this approach prove ineffective, further legal action may be pursued to safeguard the rights of the intellectual property holder.

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 is no specific legislation on AI in Switzerland. However, in December 2024 FINMA published its Guidance on Governance and Risk Management when using Artificial Intelligence (Guidance 08/2024). In its Guidance 08/2024, FINMA identified model risks, such as incorrectness, bias, lack of stability or explainability as key risks in the use of AI by supervised entities and set out measures to properly identify and manage such risks.

Specifically, FINMA expects supervised entities to define requirements or controls in their internal rules and directives to ensure the required data quality for AI applications. Data must be correct, consistent, complete, representative and up-to-date to avoid bias or unjust discrimination. FINMA further expects supervised institutions to regularly schedule tests (such as back testing, stress testing or adversarial testing) to ensure the data quality and functionality of the AI applications, including checks for accuracy, robustness and (if necessary) bias. For material applications supervised institutions should address the purpose of the application, data selection and preparation, limitations, testing and controls, etc. in the documentation.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

Fintech companies can mitigate the risk of infringement by combining legal protection with operational and technical safeguards:

- Legal protection: Adequate legal protection of proprietary AI models and data sets (e.g., patent and copyright protection) must be assessed on a case-by-case basis (please refer to questions 15-19 for further details on intellectual property protection). In particular, data sets which involve original creation may be granted copyright protection. Furthermore, when developing proprietary AI models, fintech companies must ensure the establishment of precise contractual agreements concerning ownership, including with respect to employees, independent contractors, and external collaborators or partnerships.
- Operational measures: For instance, the establishment of NDAs offers a mechanism to ensure confidentiality and proper handling of sensitive information (please refer to question 18 for further details). Additionally, educating employees on best practices for data security and the protection of proprietary AI models further enhances the overall security framework.
- Technical measures: Potential technical measures include, among others, (i) restricting access to proprietary AI models and data sets exclusively to authorised employees or contractors, (ii) conducting regular audits of such access, as well as (iii) using encryption to protect data.

Prior to using third-party AI tools in the development of proprietary AI models, fintech companies should review the applicable licensing agreements and conduct comprehensive due diligence. This includes determining whether the AI tool incorporates licensed or open-source content, and whether this may lead to unintended copyleft effects. The copyleft effect refers to the obligation of the licensee to distribute the modified, derivative version of an application under the same or a compatible copyleft license (i.e. the source code for the application must be distributed together with the program). The due diligence process shall further determine whether under the terms of the relevant license agreement, the fintech company is obligated to share ownership of any derivative works or whether the third party may assert a claim to the developed AI model. For example, it is useful to obtain confirmation from the third party and/or developer that the training processes of the third-party AI tool did not involve the reproduction of copyrighted works, thereby ensuring compliance with copyright laws. Furthermore, if the AI model is trained using third-party data, the company shall ensure that it holds the necessary rights to use such data and that its utilization complies with data privacy laws and does not infringe upon copyright restrictions.

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 specific laws on AI in Switzerland. The existing financial market laws are technology-neutral and principle-based and their regulatory requirements concerning governance and risk management also apply to the use of AI.

In its Guidance 8/2024 FINMA emphasized the need for supervised entities (including fintech companies) to properly identify, calibrate and manage the risks from their use of AI. FINMA-supervised institutions using AI are required to develop AI risk awareness by specifically addressing AI in their processes, identifying, weighting, assessing and managing the specific AI risks they face and to adapt their current compliance, risk management and internal control system (ICS) to AI.

In this Guidance 8/2024 FINMA has identified the typical risks from the use of AI which are mainly operational risks, in particular model risks (e.g., lack of robustness, correctness and explainability) as well as IT and cyber risks. FINMA further identifies legal and reputational risks as well as challenges in the allocation of responsibilities. Once the risks are identified, they must be weighted to address their materiality. FINMA lists certain factors that lead to a higher materiality or likelihood of materialisation of risks. Amongst them, FINMA refers to the potential impact on compliance, on the balance sheet, the legal and reputational impact, the number of customers affected and their profile (retail or institutional), the importance of the product(s) affected, what the expected consequences of potential failures are, the complexity, predictability and explainability of processes, as well as the possibility to monitor them. Furthermore, the type of data used (unstructured data, integrity, personal data etc.) are to be weighted as well. In a third step, appropriate mechanisms must be defined to identify and assess the specific risks on an ongoing basis. For this purpose, performance indicators, data quality tests and stability and robustness of systems are reviewed, as well as fallback mechanisms, adversarial tests, stress tests and backtests must be implemented on an ongoing basis.

From a governance perspective, the following measures should be implemented to identify, mitigate and control the risks around AI: central management and accountability, independent review by skilled personnel,

third party contractual and liability management, training of employees, definition of models for testing and establishment of a policy and documentation standards.

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

Fintech companies can mitigate legal risks associated with the use of AI by implementing a comprehensive governance structure with clear responsibilities, regular training, and detailed risk assessments. Establishing risk management that addresses the unique challenges of AI is essential for risk mitigation. Key aspects include ensuring data quality, monitoring AI models, maintaining detailed documentation, and conducting regular audits and compliance checks to ensure adherence to regulatory requirements while safeguarding the security and integrity of the AI model.

Third-party providers should be carefully selected and contractually bound to comply with security and quality standards. It is advisable to establish appropriate contractual agreements when using third-party AI tools to clarify liability issues.

Overall, the explainability and traceability of AI models and their results, as well as the flexibility to adapt to new regulatory requirements, are crucial for completing the strategy effectively.

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

The entry into force of the DLT Bill on 1 February 2021 introduced the possibility to issue and transfer ledger-based securities exclusively by a technical transfer on a blockchain or distributed-ledger. In Switzerland, this method is recognised as valid, even without the transfer of a document or paper (as required for traditional certificated securities) and/or a written assignment (as required for traditional simple uncertificated securities) or a booking implemented by a central securities depository (as required for book-entry securities). All rights that can be certificated in securities can now also be structured as ledger-based securities, ie, in principle all contractual rights including receivables and shares in corporations. Therefore, tokenisation has been significantly simplified since the introduction of the DLT Bill.

Additionally, the DLT Bill introduced a new authorisation category for DLT trading facilities. FINMA has clarified that DLT trading facilities may also offer possible settlement services to third parties, extending beyond participants within their own trading facility. In 2023, FINMA received the first formal application for a DLT trading facility license. However, Switzerland is still awaiting the granting of the first DLT trading facility license. It will be interesting to see whether this marks the beginning of a larger trend towards tokenisation and asset tokens (ie, securities), and whether such DLT trading facilities could emerge as strong competitors to traditional trading venues.

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

In Switzerland, investments experienced a decline during 2023 and 2024. Although, investments in Swiss start-ups decreased by 34.8% in 2023 compared to 2022, the invested CHF 2.6 billion is the third best value within the past 10 years.

Fintech funding continued to decline in H1 (first half of) 2024 which mirrors global trends as global fintech funding declined by 32% in H1 2024 compared to H1 2023. Despite the overall decline, notable financing rounds in 2024 include:

- Sygnum Bank: Following the CHF 34.5 million oversubscribed growth round financing in January 2024, more than 20 banks and international financial institutions have joined the Sygnum B2B network platform that enables their end-clients to buy, hold, trade, earn, and transfer cryptocurrencies;
- Wyden: Wyden, a key player in institutional infrastructure for the digital asset trading lifecycle, closed a CHF 14.5 million Series B funding round for its global expansion.

Successful financing rounds are Series B-D rounds rather than Series A rounds.

Contributors

Dr. Kilian Schärli
Managing Partner
kilian.schaerli@mll-legal.com

Dr. Reto Luthiger
Partner
reto.luthiger@mll-legal.com

Prof. Dr. Andreas Furrer
Special Counsel
andreas.furrer@mll-legal.com

Andrea Trost
Senior Associate
andrea.trost@mll-legal.com