

# Legal 500

## Country Comparative Guides 2026

### Switzerland

#### Fintech

#### Contributor

MLL Legal



#### Dr. Kilian Schärli

Managing Partner | [kilian.schaerli@mll-legal.com](mailto:kilian.schaerli@mll-legal.com)

#### Dr. Reto Luthiger

EMBA, Partner and Vice-Chair | [reto.luthiger@mll-legal.com](mailto:reto.luthiger@mll-legal.com)

#### Andrea Trost

LL.M., Salaried Counsel | [andrea.trost@mll-legal.com](mailto:andrea.trost@mll-legal.com)

#### Franziska Gall

LL.M., Associate | [franziska.gall@mll-legal.com](mailto:franziska.gall@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](https://legal500.com/guides)

## Switzerland: Fintech

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

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 financial market regulations and for investigating related infringements. The basis of the regulatory framework is established by federal laws issued by 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 guidance.

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 (SRO) 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.

Since 2015, the legislator has focused on adapting the legal and regulatory framework to the needs of the fintech sector. In 2016, FINMA issued a circular allowing financial intermediaries to onboard clients by conducting video identification or an online identification which made client onboarding for anti-money laundering purposes economically more attractive. In 2017, the Federal Council extended the holding duration for settlement accounts from 7 to 60 days. The settlement account exemption allows asset managers, securities firms, dealers of precious metals and similar entities to accept and hold funds in customer accounts that exclusively serve the purpose of settling customer transactions without triggering the need for a banking license, provided that the funds are not-interest bearing and

forwarded within 60 days. FINMA clarified that the settlement account exemption does not apply to cryptocurrency traders that undertake a similar activity as FX traders by maintaining accounts for their clients for investments in different currencies. In 2017, a sandbox regime was introduced in the Banking Act that allows companies to accept public deposits of up to CHF 1 million without requiring a banking license subject to certain conditions. In addition to the sandbox regime, a new fintech license was introduced in 2019. The fintech license authorises its holders to accept public deposits of up to CHF 100 million in fiat currency without engaging in any lending activities (i.e., without investing or paying interest on them). The fintech license thus falls between the sandbox and a full banking license. In 2021, the scope of application of the fintech license was extended to certain deposit-taking activities of crypto-based assets (cryptocurrencies) theoretically in an unlimited amount but subject to the discretion of FINMA and as long as neither interest is paid on them and no proprietary trading/investing of such client funds occurs. A fintech license is subject to simplified regulatory requirements compared to the banking license. The existing fintech license has helped enable innovation, and ongoing reforms aim to introduce more tailored regimes for payment services and crypto-asset activities, including stablecoins and custody. Overall, the framework is being refined to close regulatory gaps, improve consumer protection, and ensure consistent oversight as financial services converge.

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

Regulatory fragmentation poses a key risk for fintech innovation. Major jurisdictions such as the EU, UK, and US have now brought stablecoins and crypto asset services under strict regulatory oversight. In order to align more closely with global standards, notably those of the Financial Stability Board and the EU's MiCA regulation, and to remain competitive and credible, the Swiss Federal Council opened in October 2025 a consultation process for two new license categories: the payment instrument institution and the crypto institution.

The new regime aims to enhance Switzerland's regulatory framework for fintech businesses, the issuance of stablecoins and the provision of crypto asset services.

Regulatory fragmentation with the EU poses additional challenges. The EU's MiCA, which entered into force in stages during 2024–2025, and the Digital Operational Resilience Act (DORA), applicable since January 2025, do not apply directly in Switzerland. As a non-EU state, Switzerland does not benefit from passporting rights, meaning Swiss fintechs must take advantage of the very limited cross-border opportunities, but more often establish locally licensed EU entities or obtain direct authorisation in EU member states to serve EU clients or operate EU subsidiaries. For Swiss fintechs with EU operations or significant EU client bases, practical alignment with MiCA's requirements for crypto-asset service providers and DORA's operational resilience standards (including ICT risk management, incident reporting, and third-party oversight) has become necessary, alongside compliance with Switzerland's own framework under FINMA Circular 2023/1 (discussed in Question 10).

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 Anti-Money Laundering Act (AMLA) can result in serious legal consequences and reputational damage for the fintech in question.

Furthermore, the use of AI by fintech companies has increased, 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.

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

FINMA applies a technology neutral and "same risk, same rules" approach – activities replicating regulated functions (custody, lending) fall under existing laws regardless of the technology used. Therefore, fintechs

combining multiple functions are subject to cumulative regulatory requirements, amongst others triggering banking, securities, portfolio management, custody, and AML rules simultaneously.

If a fintech company intends to accept public deposits exceeding CHF 1 million, it must either obtain a fintech license (for deposits up to CHF 100 million in fiat currency, with certain conditions for cryptocurrencies) or a full banking 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 AMLA and need to affiliate with an SRO.

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

Switzerland is not adopting a single omnibus license that covers all fintech activities under one umbrella. Instead, the Swiss Federal Council has proposed a targeted reform of the Financial Institutions Act (FinIA), which introduces two new specialised license categories rather than a unified regime: The payment instrument institution license and the crypto institution license.

The payment instrument license will replace the existing fintech license allowing institutions to accept customer funds without engaging in lending or interest payments. The CHF 100 million limit is abolished, enabling institutions to grow and take advantage of economies of scale. In case of bankruptcy, customer funds are segregated and not part of the bankruptcy estate, a significant improvement over the previous regime. Furthermore, only licensed payment instrument

institutions will be permitted to issue a special type of stablecoin (i.e. crypto-based assets that are issued in Switzerland and aimed to maintain a stable value in relation to a single Fiat currency), which must be fully backed, segregated from the issuer's assets, and redeemable at par value.

The crypto institution license covers entities providing custody, trading, and certain other services involving payment tokens (such as Bitcoin and non-Swiss stablecoins), excluding utility tokens, asset tokens and stablecoins issued by payment instrument institutions. Licensing and activity requirements are modelled on those for securities firms but are less extensive, reflecting the different risk profile of crypto asset services. Rules on custody are based on existing provisions in the Banking Act. Licensed banks and securities firms do not require an additional license as crypto institutions.

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

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. By 2025, this framework has become a core innovation tool, widely used by fintech and blockchain start-ups for early-stage testing without triggering full regulatory burdens 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 an SRO could be required.

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

### finance models?

In Switzerland, FINMA is progressively modernising its supervisory approach to keep pace with cross border fintech activity, embedded finance models, and increasing technology driven complexity in financial services:

- Increased use of data and technology in supervision: FINMA is adopting technology-supported, data-driven supervision (SupTech) tools to improve the efficiency and effectiveness of oversight, including automated analysis of large datasets and non-traditional sources. These tools help FINMA detect risks earlier and more comprehensively, even as fintechs operate across multiple service lines and jurisdictions.
- Digital reporting and electronic processes: FINMA increasingly relies on standardised, digital reporting and communication channels. Licensed fintechs and other supervised entities are expected to submit filings, notifications, data collections and licence applications electronically via FINMA's Erhebungs- und Gesuchsplattform (EHP). Submitted data is subject to automated validation and plausibility checks, improving data quality and enabling more timely supervisory responses. Indirect supervision via external audit firms is also supported by structured, electronic submission of audit findings and risk assessments, contributing to more consistent and scalable oversight across a diverse fintech population.
- Risk- and principles-based supervision: FINMA's supervisory approach remains firmly risk oriented and principles based. Fintech and embedded finance models are assessed based on their actual activities, risk exposures, and economic substance rather than formal labels or specific technologies. This allows FINMA to supervise hybrid and cross border models – such as those combining payments, lending, digital assets, wealth management, or platform based distribution – within the existing regulatory framework, while remaining adaptable as business models and delivery channels converge.
- Early steps toward advanced tech use: While still in the early stages of systematic AI integration into supervision, FINMA has begun piloting AI capabilities to support data processing and analysis and is developing

internal competencies to scale  
RegTech/SupTech use in core oversight  
functions.

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

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, enabling tokenization of rights and claims. 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.

For stablecoins, FINMA follows the rules based on the stablecoin supplement to the ICO Guidelines, which takes the same approach as blockchain-based tokens by mainly focusing on the economic function and the purpose of the token (substance over form). Depending on the case, FINMA will follow the "same risks, same rules" principle and the relevant features of each case. Since stablecoins can be variable in substance, the requirements under supervisory law may differ depending on which assets (eg, currencies, commodities, securities and real estate) the stablecoin is backed by or pegged to and the legal rights of its holders. FINMA has published an overview table in the ICO Guidelines supplement with the regulatory qualification depending on the underlying assets or features of the stablecoin. Regulations of banking, fund management, financial infrastructure, anti-money laundering and securities trading can all become relevant. Under the new proposed licensing regime (see question 3 above) only licensed payment instrument institutions will be permitted to issue a special type of stablecoin (i.e., crypto-based assets that are issued in Switzerland and aimed to maintain a stable value in relation to a single fiat currency), which must be fully backed, segregated from the issuer's assets, and redeemable at par value. The payment instrument

institution must further publish a whitepaper.

FINMA applies the "same business, same risks, same rules" approach also to DeFi projects. Projects claiming decentralisation but that are controlled by identifiable entities therefore trigger financial markets laws where there are similarities with traditional financial market applications. In this regard, FINMA has identified possible regulatory anchor points which speak against the true decentralization of a DeFi project and which may trigger licensing requirements under the applicable financial market laws:

- person or group that controls the further development of the protocol smart contracts (e.g., in the form of an admin key for the smart contract);
- person or group that owns the majority of the governance tokens of a project to be able to determine the further development of the protocol smart contracts;
- the functioning of the smart contract depends substantially on the input of a person or group (e.g., control of oracles that provide data);
- access to the DeFi application is only possible via certain persons (e.g., through whitelisting);
- person that generates revenue with the DeFi application;
- person that has a permanent business relationship with end users of the protocol.

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

The AMLA, and the corresponding ordinance, stipulate the obligations that must be performed by virtual asset service providers. Virtual asset service providers that are not prudentially supervised must join an SRO recognised by FINMA. SROs 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) and respective enhanced due diligence

(EDD) procedures;

- 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 obligations may vary depending on the services or activities and the number of Swiss francs collected or transferred.

Concerning transactions of payment tokens, virtual asset service providers must apply the travel rule on every transaction, including transactions to wallets held with unregulated wallet providers (i.e., stating the name, address and wallet address of the sending party and the name and wallet address of the receiving party).

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

Under the proposed payment instrument license regime client funds must be fully segregated from the institution's own assets and are protected from the bankruptcy estate in case of insolvency. All client funds (including those backing stablecoins) must be held in highly liquid, high-quality assets with short maturities, or as sight deposits at a bank, another payment institution, or (if allowed) at the Swiss National Bank. Assets must be diversified to limit credit, liquidity, and market risks.

Assets must be held in the same currency as the stablecoin's redemption claim to avoid FX risk.

Stablecoin holders have a legal right to redemption at par value at any time, with no lock-up or notice period, except for AML or sanctions compliance. The redemption must be processed promptly.

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

FINMA is highly focused on data privacy, cybersecurity, and operational resilience for fintechs. Its Circular 2023/1 "Operational risks and resilience – banks" requires banks and financial institutions (including fintech companies) to strengthen operational risk management and resilience, with a strong focus on ICT, cyber, and data risks. Institutions must identify critical functions, set disruption tolerances, regularly test business continuity and cyber defences, and report major incidents promptly. The rules

are risk-based and proportional, aiming to ensure robust governance, continuity, and protection against evolving threats. Enforcement trends show more frequent supervisory reviews, mandatory incident reporting, and a clear expectation that fintechs continuously adapt to evolving cyber and operational risks. Finally, FINMA expects also full compliance with the Federal Act on Data Protection (FADP).

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

Cryptocurrency and blockchain companies should implement robust transaction monitoring systems to detect suspicious patterns, use blockchain analytics tools to identify high-risk wallets, and apply strong KYC/AML procedures to prevent fraudulent activity. Regular staff training, clear internal controls, and prompt reporting of suspicious transactions are essential. To prepare for regulatory audits and enforcement, firms should maintain thorough documentation of compliance processes, keep audit trails of all transactions, and conduct regular internal reviews.

Engaging with legal and compliance experts, staying updated on regulatory changes, and proactively cooperating with authorities will help ensure readiness for inquiries and minimize enforcement risks.

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

Swiss fintechs are adapting to changing global immigration frameworks by leveraging Switzerland's relatively stable and efficient work permit system, which is being further streamlined in 2025 to speed up processing and reduce red tape for employers. Under Switzerland's dual regime, EU/EFTA nationals benefit from the Free Movement of Persons Agreement, allowing them to enter, reside, and work in Switzerland as employees or in a self-employed capacity without a visa, giving fintechs immediate access to a large and highly skilled talent pool. While quotas and stricter requirements continue to apply to third-country nationals, recent reforms are intended to make it easier for companies to recruit and onboard international tech and compliance

specialists. At the same time, Swiss fintechs are monitoring digital nomad visa developments in the EU and Asia, but Switzerland's policy focus remains on simplifying domestic procedures, maintaining competitive quotas, and supporting integration of foreign hires. Overall, this enables Swiss fintechs to remain attractive to global talent – particularly from the EU – while encouraging proactive human resources planning and compliance as immigration rules evolve.

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

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.

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

In Switzerland, immigration and workforce-mobility rules have a major practical impact on fintechs' ability to deploy and relocate talent, particularly for cross-border expansion. EU/EFTA nationals enjoy relatively flexible access – they can live and work in Switzerland with a residence permit (L or B) after registering locally if staying longer than about 90 days. Non-EU/EFTA nationals must secure a work permit plus residence permit before working in Switzerland. These are issued in limited numbers under annual quotas, and companies must file applications early to secure slots. The Swiss Intra-Company Transfer (ICT) Permit lets multinational companies move senior managers or specialists relocate

to Swiss branches, subsidiaries or affiliates without local labour market testing, which is crucial for key fintech roles (e.g., product leads, compliance heads). This permit is typically for temporary assignments and requires the employee to have worked with the company already and meet salary/qualification criteria. Switzerland has no dedicated “digital nomad” or remote-work visa. Foreign employees physically working in Switzerland – even for a foreign fintech – generally need a work/residence permit if their activity could impact the Swiss labour market or economy. Fintechs operating in or expanding to Switzerland should plan work-permit applications early and closely monitor annual quota availability, as timing constraints can be a key bottleneck. Where possible, firms with a Swiss presence should rely on intra-company transfer permits to relocate senior managers or specialists without full labour-market testing. Companies without a local entity can mitigate hiring friction by partnering with Employer-of-Record providers or establishing a Swiss branch to sponsor permits and manage tax and social-security compliance. Clear internal policies on remote work are also essential, as performing work from Switzerland can trigger immigration, tax, and social-security obligations even for foreign employers. Overall, Switzerland's system supports structured and compliant mobility, but quota limits and the lack of dedicated remote-work visas mean proactive planning is critical to avoid delays or talent gaps.

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

In Switzerland, immigration rules and visa limitations play a material role in shaping both the speed and strategy of fintech market entry, particularly for firms launching in multiple jurisdictions. Under the Free Movement of Persons Agreement, EU/EFTA nationals can enter, reside, and work in Switzerland without a visa, either as employees or self-employed, giving fintechs relatively frictionless access to a large regional talent pool and enabling faster initial market entry. By contrast, non-EU/EFTA nationals (including UK nationals since 1 January 2021) require a work permit even for short-term assignments, are subject to annual quotas, and must meet strict criteria: they must be highly qualified, the role must be in Switzerland's economic interest, and employers must demonstrate that no suitable candidate could be found in Switzerland or the EU/EFTA. These constraints can slow hiring and deployment of key staff, affecting timelines for regulatory set-up, product launches, and scaling. As a result, fintechs often sequence market entry to prioritise jurisdictions with

easier mobility, rely more heavily on EU-based teams or regional hubs, and align hiring and entity-structuring decisions early with immigration timelines – making workforce mobility a core strategic consideration rather than a back-office issue.

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

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.

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.

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

Under Swiss law, a trademark is a protected sign that distinguishes a company's products or services from those of other companies. Graphical representations of a sign can include words, combinations of letters or numbers, images, three-dimensional forms, slogans, combinations of these elements, or even sound trademarks. For fintechs, a strong trademark is critical not only for brand differentiation but also for customer trust, given the sensitive financial assets and personal data they manage.

Fintech companies can register their trademarks with the Swiss Federal Institute of Intellectual Property, and for broader international protection, registration under the Madrid System is recommended. International applications can also be processed via the IPI, providing a streamlined route to safeguard brands globally.

To protect against AI-generated impersonation, deepfakes, and synthetic media fraud, Swiss fintechs should adopt a multi-layered brand protection strategy that combines proactive monitoring of digital channels and AI content platforms, enforcement of unfair competition law against confusing imitation, and contractual and technological safeguards such as non-disclosure agreements (NDAs), licensing agreements, watermarking, and cryptographic authentication. Rapid takedown procedures and collaboration with online platforms and regulators, along with internal training to recognize phishing or synthetic-media threats, further strengthen defenses. By integrating trademark registration, international protection, legal enforcement, and digital safeguards, fintechs can maintain brand integrity, protect their reputation, and preserve customer trust in an era of increasingly sophisticated digital impersonation.

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

Fintechs 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, fintechs 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 terms that specify the intellectual property rights retained by each party and clarify the management of any proprietary information. Fintechs 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 16 for further details). In addition, 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 fintechs take to detect, prevent, and respond to competitors or third parties who might copy or misuse their technology, algorithms, or branding, and how do enforcement strategies differ across jurisdictions?**

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.

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. 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. How are jurisdictions addressing cross-border IP enforcement for fintech products**

### **involving distributed infrastructure and decentralized code bases?**

In Switzerland, cross-border IP enforcement for fintech products with distributed infrastructure is addressed through a combination of traditional IP frameworks, evolving regulatory approaches and private international law principles.

Swiss courts and authorities recognize that software, smart contracts, and AI models may be protected as copyrighted works or trade secrets (see question 16), but enforcement can be complex when such fintech products are hosted or executed across multiple jurisdictions.

To address this, fintechs often rely on contractual agreements, licensing terms, and technological safeguards to define usage rights and establish jurisdiction for disputes. Regulators and courts generally take a technology-neutral approach, focusing on the protection of proprietary rights rather than the underlying infrastructure, requiring firms to combine robust contracts, operational controls, and technical measures to protect decentralized fintech products globally.

Furthermore, effective enforcement mechanisms are based on comprehensive and systematic monitoring. Therefore, once established, fintech companies should monitor the market for potential infringements.

However, effective protection of fintech innovations with distributed infrastructure typically requires coordinated multi-jurisdictional strategies.

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

In Switzerland, fintechs licensing or selling software, smart contracts, or AI models should adopt a multi-layered IP protection strategy that combines legal, operational, and technical safeguards to maintain control and ensure compliance with domestic and international laws.

From a legal perspective, firms should clearly define ownership, licensing scope, and permitted uses in contracts, specifying whether rights are exclusive, non-exclusive, transferable, or sublicensable. Proprietary software, AI models, and datasets can be protected through copyright, trade secrets, and patents where applicable. Fintechs must also establish precise contractual agreements regarding ownership with

employees, independent contractors, and external collaborators. Operational measures include NDAs to ensure confidentiality, employee training on best practices for data security, and clear policies for handling proprietary AI models. Technical safeguards may involve restricting access to authorized personnel, conducting regular access audits, using encryption to protect data, and implementing monitoring systems to detect misuse. Combined, these measures help fintechs mitigate infringement risk, preserve enforceable rights, and ensure compliance across multiple jurisdictions.

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

In Switzerland, fintechs using AI in underwriting, robo-advisory, or fraud protection are primarily governed by existing financial, consumer protection, and data laws, with FINMA Guidance 08/2024 providing detailed expectations for AI governance. FINMA emphasizes that supervised entities must identify, assess, and manage the risks arising from AI, including operational risks such as model robustness, correctness, and explainability, IT and cyber risks, as well as legal and reputational risks.

Institutions are expected to adapt their compliance, risk management, and internal control systems to account for AI-specific risks, weighting factors such as potential impact on the balance sheet, customer base, product importance, process complexity, and data quality.

FINMA requires fintechs to implement ongoing risk monitoring and mitigation mechanisms, including performance indicators, stress tests, backtests, data quality checks, fallback mechanisms, and adversarial testing. From a governance perspective, firms should establish central accountability, independent review, third-party oversight, employee training, model testing frameworks, and robust documentation standards. Combined with strong model validation, human oversight, explainability, and auditability, these measures ensure AI-driven decision-making in finance is safe, fair, transparent, and compliant, aligning with both Swiss regulations and emerging international frameworks like the EU AI Act and U.S. GENIUS Act.

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

In Switzerland, AI-driven investment and credit-decisioning tools are subject to existing fiduciary, fair-lending, and disclosure obligations, with regulators emphasizing transparency, accountability, and robust risk management. FINMA expects financial institutions to demonstrate adequate governance, model validation, and human oversight when using AI for credit scoring, investment advice, or risk assessments, ensuring decisions are explainable, non-discriminatory, and aligned with consumer protection requirements. Clear disclosure of automated decision-making processes and limitations is required, and firms must monitor AI outputs to prevent bias or unfair treatment.

FINMA's Guidance 08/2024 further details governance and risk management expectations for AI in finance, covering operational risks – including model risks such as lack of robustness, correctness, explainability, or bias – data-related risks like quality, security, and availability, IT and cyber risks, increasing third-party dependencies, and legal or reputational risks.

Looking ahead, the Swiss Federal Council plans to adopt sector-specific amendments to existing legislation rather than a comprehensive AI law. A draft incorporating the EU AI Convention is expected to be submitted for public

consultation by the end of 2026. Overall, Swiss regulators take a technology-neutral, outcome-focused approach, requiring firms to integrate strong governance, documentation, and auditability to meet fiduciary and consumer protection standards.

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

In Switzerland, as fintechs increasingly use AI, automation, and complex models, several emerging liability theories could expose them to enforcement actions or civil litigation over the next 12 months. Negligent model governance may arise if AI models or automated decision systems – such as those for credit scoring, compliance screening, or pricing – produce biased, inaccurate, or harmful outcomes due to poor governance, documentation, or testing. Similarly, a failure to supervise AI or automated systems could create liability if insufficient human oversight leads to consumer harm, discriminatory results, operational losses, or regulatory non-compliance.

Other emerging risks include data privacy and cybersecurity breaches, particularly where AI training pipelines or automated systems mishandle customer data, triggering claims under Swiss data protection law and contractual obligations. Algorithmic discrimination or unfair terms is another concern, as automated pricing, risk assessments, or contract generation that produce discriminatory or unfair outcomes could prompt civil suits or regulatory scrutiny under Swiss consumer and financial services laws.

To build a defensible risk management framework, Swiss fintechs should implement robust model governance with policies for development, validation, documentation, change control, and periodic review, alongside human-in-the-loop controls for oversight of critical decisions. Maintaining explainability, traceability, and thorough documentation of data sources, design choices, testing results, and risk assessments is essential for regulatory transparency and adapting to evolving requirements. Firms should conduct stress testing, monitoring, bias detection, scenario analysis, and independent audits, while enforcing strict data protection and cybersecurity measures. Third-party AI providers should be carefully selected, contractually bound to security and quality standards, and liability clarified. Combined with regular

training, risk assessments, and compliance checks, this integrated approach allows fintechs to mitigate legal risks, reduce liability, and demonstrate responsible, defensible use of AI and automated system.

#### **25. What notable examples of fintech-driven disruption or embedded finance adoption have reshaped your jurisdiction's financial landscape in the past year?**

Switzerland's financial landscape has undergone significant transformation over the past year, driven by key fintech developments and the growing adoption of embedded finance in non-financial apps and platforms.

Retail clients now benefit from multibanking, with SIX launching its bLink open-banking platform in November 2025; eight banks and two third-party providers participated initially, and more than 30 banks now offer the required data interfaces, allowing customers to consolidate accounts across banks within a single app or integrate them into third-party services. On the capital markets side, BX Digital, a sister company of BX Swiss and part of the Boerse Stuttgart Group, received Switzerland's first DLT trading venue license from FINMA in March 2025, paving the way for tokenised securities trading for supervised participants. Meanwhile, digital-native banks like Alpian continue to grow, blending AI, cloud-native infrastructure, and embedded payments, while payment platforms such as TWINT and Payrex expand cashless and embedded payment options for consumers and SMEs. Together, these developments illustrate how embedded finance, digital banking, and blockchain-based innovation are reshaping Switzerland's financial ecosystem.

#### **26. Looking ahead, which regulatory reforms or global coordination efforts—such as cross-border licensing passporting or stablecoin reserve interoperability—hold the greatest potential to accelerate fintech innovation?**

Regarding Swiss regulatory reforms, on 22 October 2025, the Swiss Federal Council opened the consultation process for a major amendment to the Financial Institutions Act, aiming to enhance Switzerland's regulatory framework for fintech businesses, the issuance of stablecoins and the provision of crypto asset services. This move is designed to strengthen Switzerland's position as a leading hub for fintech and blockchain innovation, while ensuring robust standards for financial stability, integrity, and investor protection.

The consultation will run until 6 February 2026.

The rapid evolution of digital finance has exposed gaps in Switzerland's existing regulatory regime. Until now, stablecoins – tokens pegged to the value of one or more underlying assets – have been assessed under existing financial market laws, often resulting in either over-regulation (e.g., requiring a full banking license) or regulatory blind spots. Meanwhile, the fintech license introduced in 2018, though innovative, has shown weaknesses, particularly regarding customer protection in bankruptcy scenarios and growth limitations due to a CHF 100 million deposit cap.

Internationally, major jurisdictions such as the EU, UK, and US have brought stablecoins and crypto asset services under strict regulatory oversight. To remain competitive and credible, Switzerland is now proposing a bespoke regime that aligns with global standards, notably those of the Financial Stability Board and the EU's MiCA regulation.

Against this backdrop, the Federal Council is proposing

two new license categories: Firstly, the new category payment instrument institution will replace the existing fintech license, allowing institutions to accept customer funds without engaging in lending or interest payments. Secondly, the new license crypto institutions covers entities providing custody, trading, and certain other services involving payment tokens (such as Bitcoin and non-Swiss stablecoins), excluding utility tokens, asset tokens and stablecoins issued by payment instrument institutions.

Switzerland's proposed reform marks a decisive step toward a modern, innovation-friendly, and robust regulatory environment for fintech businesses, stablecoins and crypto assets service providers. In particular, the new categories offer a clearer, more attractive path to market for fintechs and start-ups, with improved legal certainty, customer confidence and growth potential. By introducing dedicated license categories, enhancing customer protection, and aligning with international standards, the country is poised to remain at the forefront of digital finance and innovation – balancing opportunity with responsibility.

## Contributors

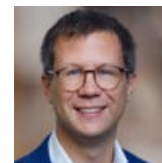
**Dr. Kilian Schärli**  
Managing Partner

[kilian.schaerli@mll-legal.com](mailto:kilian.schaerli@mll-legal.com)



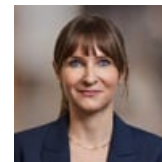
**Dr. Reto Luthiger**  
EMBA, Partner and Vice-Chair

[reto.luthiger@mll-legal.com](mailto:reto.luthiger@mll-legal.com)



**Andrea Trost**  
LL.M., Salaried Counsel

[andrea.trost@mll-legal.com](mailto:andrea.trost@mll-legal.com)



**Franziska Gall**  
LL.M., Associate

[franziska.gall@mll-legal.com](mailto:franziska.gall@mll-legal.com)

