Legal 500
Country Comparative Guides 2026

United States
Fintech

Contributor

Orrick, Herrington & Sutcliffe LLP

Lisa M. Lanham

Partner, Head of Fintech Licensing | llanham@orrick.com

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

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

United States: 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?

U.S. fintech oversight, a sweeping area of law that covers everything from digital lending platforms and robo-advisors to payment apps and embedded banking products, is a fragmented field across federal and state regulators whose place in the legal world is based principally on activity rather than business model. Key federal regulators include the Consumer Financial Protection Bureau ("CFPB") (i.e., for consumer financial products), the Office of the Comptroller of the Currency ("OCC") (i.e., national banks and certain fintech-bank partnerships), the Board of Governors of the Federal Reserve System ("Federal Reserve") (i.e., bank holding companies and payment systems), the Federal Deposit Insurance Corporation ("FDIC") (i.e., deposit insurance and bank supervision), the U.S. Securities and Exchange Commission ("SEC") (i.e., securities and certain digital assets), the U.S. Commodity Futures Trading Commission ("CFTC") (i.e., derivatives and commodities), and the Financial Crimes Enforcement Network ("FinCEN") (i.e., Bank Secrecy Act/anti-money laundering ("BSA/AML") compliance). State regulators, including state banking departments and money transmitter authorities coordinated through the Conference of State Bank Supervisors ("CSBS"), supervise nonbank lenders and payments companies.

Importantly, fintechs must consider both consumer-purpose (B2C) and commercial-purpose (B2B) regulatory frameworks. While B2B transactions are generally less regulated at both the federal and state level, they are certainly not immune to regulation. Regulatory classification of a particular transaction generally depends on the nature of the borrower, collateral, and transaction characteristics rather than stated purpose of said transaction. For example, loans made to borrowers for commercial real estate investment secured by an interest in real property improved by one-to-four family dwelling units, which property is to be owner-occupied or made to a natural person, may be treated as a residential mortgage loans subject to TILA, RESPA, and state mortgage lending laws, irrespective of the borrower's stated business or commercial purpose in acquiring the real estate.

Regulatory boundaries are increasingly strained as fintechs blend payments, lending, wealth management, and digital assets into unified platforms. Through enforcement, the SEC has asserted jurisdiction over crypto tokens as securities, while the CFTC pursues digital asset derivatives matters. Bank-fintech partnerships face heightened scrutiny from the FDIC, OCC, and Federal Reserve, particularly following enforcement actions related to third-party risk management and "rent-a-bank" arrangements where banks are alleged to allowed non-bank lenders to act under cover of the banks' charters in order to bypass state interest rate caps.

As embedded finance and stablecoin models proliferate, jurisdictional overlap continues driving interagency coordination and policy debate.

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?

Four areas present the greatest headwinds: digital asset classification uncertainty, artificial intelligence (AI) governance expectations, bank-fintech partnership scrutiny, and evolving licensing frameworks for emerging product categories.

First, digital asset regulation remains unsettled. While courts have weighed in on token classifications under SEC enforcement actions, and despite a legislative framework for payment stablecoins, comprehensive federal crypto legislation has not materialized. Ongoing SEC and CFTC jurisdictional debates, lacking definitive solutions, and FinCEN AML obligations increase compliance costs without providing clear pathways forward.

Second, AI oversight is accelerating. The CFPB, FTC, and banking agencies have made clear that existing laws, including the Equal Credit Opportunity Act (ECOA), Fair Housing Act (FHA), Fair Credit Reporting Act (FCRA), and prohibitions on unfair, deceptive, or abusive acts or practices (UDAAPs), apply fully to AI-driven underwriting

 © 2026 Legalease Ltd

and automated decisioning. Regulators warn against "black box" models that cannot provide compliant adverse action explanations. State laws, including Colorado's AI Act (effective 2026), impose additional risk management and transparency requirements.

Third, supervisory pressure on bank-fintech partnerships has intensified, particularly following the Madden v. Midland Funding Second Circuit decision, which created uncertainty around whether interest rate exportation survives loan sale or assignment. This "valid-when-made" doctrine uncertainty has driven states to enact protective legislation, but challenges to bank partnership models through litigation and enforcement continue.

Fourth, emerging product categories face rapidly evolving state licensing frameworks. Earned Wage Access (EWA) products and payroll-linked financial services are drawing heightened regulatory scrutiny, with states enacting new licensing requirements and regulators issuing guidance on whether these products constitute credit subject to the federal TILA and state lending laws. Each legislative session brings new compliance obligations.

Together, regulatory uncertainty, examination intensity, a patchwork of state requirements, and regulation-through-enforcement all increase capital costs and extend product launch timelines.

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)?

Yes. Fintech licensing depends on activity, not technology. Most fintech business models require state and/or federal licensing across multiple jurisdictions.

Consumer lending typically requires state lending licenses in each jurisdiction where borrowers reside. Activities like originating, servicing, or purchasing loans trigger licensing under state lending laws and usury statutes. Federal consumer protection laws, including TILA, ECOA, and FCRA, also apply. Private student lending and refinancing products are subject to these same frameworks (and sometimes additional laws specific to post-secondary education financing products), with additional considerations around ability-to-repay standards, qualified education loan disclosures under TILA, and state-specific student loan servicer licensing requirements that have proliferated in recent years.

Commercial lending, while generally less regulated, is not wholly unregulated. Fintechs must carefully analyze transaction characteristics to determine applicable regulatory frameworks. For example, loans for business, commercial, or investment purposes that are secured by an interest in real property improved by one-to-four family dwelling units may trigger mortgage lending licensing and federal consumer protection laws if the property will be owner-occupied or the loan is made to a natural person, regardless of stated business purpose of the parties to the transaction. Small business lending may trigger state licensing depending on loan size, borrower type, and jurisdiction-specific definitions. Additionally, Section 1071 of the Dodd-Frank Act calls for covered financial institutions to collect and report demographic and other data on credit applications by women-owned, minority-owned, and small businesses, with forthcoming final rules creating new compliance obligations for small business lenders. Alternative credit products, including merchant cash advances and revenue-based financing, may trigger lending licensing depending on structure and characterization under state law.

Payments activity commonly triggers state money transmitter licensing. Forty-nine states and the District of Columbia require licenses for receiving and transmitting money or issuing stored value. Federal-level FinCEN registration as a money services business (MSB) is required under the BSA.

Payroll processing and EWA are drawing increased regulatory attention. Several states have enacted or proposed EWA-specific licensing frameworks, while regulators debate whether EWA products constitute credit subject to lending laws. Some states treat tips and fee-based EWA differently from interest-bearing or recourse-based products. Payroll processing may trigger money transmission licensing depending on how funds flow and whether the provider takes custody of employer funds.

Digital asset custody or exchange activities may trigger MSB registration, state money transmission licensing, or specialized charters like New York's BitLicense or limited-purpose trust charter under New York Department of Financial Services (NYDFS) regulations. Broker-dealer registration may be required if digital assets are deemed securities.

Investment advisory services trigger SEC or state investment adviser registration depending on assets under management. Robo-advisers must comply with the Investment Advisers Act and related SEC guidance.

Most significantly, state licenses generally apply to each

 © 2026 Legalease Ltd

individual legal entity conducting the regulated activity. Licenses cannot typically be shared across entities under common ownership or control, absent express statutory exemptions. Fintechs must carefully structure their corporate organization and ensure each entity performing licensed activities holds the appropriate authorization.

In sum, licensing requirements hinge on (a) what the fintech does, (b) how it does it, (c) whom it serves, (d) which legal entity performs the activity, and (e) the characteristics of the borrower, collateral, and transaction, not merely the stated purpose. The regulatory characterization of products, particularly those straddling consumer and commercial classifications, remains subject to state-by-state interpretation and enforcement.

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?

No. Unlike the EU's Markets in Crypto-Assets Regulation (MiCA) or Digital Operational Resilience Act (DORA) frameworks, the United States does not have a unified omnibus fintech license. Regulatory authority remains functionally segmented across federal and state authorities.

However, some developments reflect incremental harmonization. The CSBS expanded the Nationwide Multistate Licensing System and Registry (NMLS) to streamline multi-state licensing and supervision for money transmitters and lenders. The Money Transmission Modernization Act (MTMA) model law, adopted in many states, aims to harmonize money transmission standards, though adoption is not universal and many states made significant customizations that hamper the uniformity the model law intended to create.

The OCC previously proposed a Special Purpose National Bank (SPNB) charter for fintech companies, which faced litigation and has not been widely used. Industrial Loan Company (ILC) charters remain available but politically sensitive.

The GENIUS Act was an important step toward introducing stablecoins into the U.S. financial system but significant questions remain, including as various federal and state regulatory agencies craft rules to implement the GENIUS Act's permitted payment stablecoin issuer framework.

The United States remains a multi-license jurisdiction rather than a single-passport model. Fintechs operating nationally must navigate overlapping state and federal requirements simultaneously.

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?

Regulatory sandboxes have had mixed results. The CFPB previously operated a Compliance Assistance Sandbox and no-action letter policy, though its approach has evolved across administrations. The OCC maintains an Office of Innovation. Several states, including Arizona, Utah, and Wyoming, have established fintech sandboxes permitting limited testing under regulatory supervision.

While these programs provide structured regulator engagement, measurable impact on capital formation and time-to-market has been modest. Participation volumes remain limited, and most fintechs still must secure full licensure for scaled operations.

Industry participants report that sandboxes primarily provide regulatory clarity rather than long term licensing solutions. They are most useful for early product testing, but do not eliminate multi-jurisdictional compliance requirements.

By 2025, innovation offices are institutionalized, functioning as engagement mechanisms rather than alternative licensing regimes. Fintechs should view them as dialogue channels, not regulatory shortcuts.

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?

U.S. regulators increasingly leverage technology-enabled supervision while simultaneously expanding enforcement actions that may give insight to regulatory boundaries. The CFPB and federal banking agencies use data analytics in supervision and enforcement, particularly for fair lending and UDAAP monitoring. The CFPB has emphasized its authority over nonbank "larger participants" in key consumer financial markets including

 © 2026 Legalease Ltd

student loan servicing, auto lending, debt collection, consumer reporting, and international remittance payments.

Interagency third-party risk management guidance (issued on or about 2023) formalized supervisory expectations for bank-fintech partnerships, requiring enhanced oversight, data-sharing, and monitoring of embedded finance arrangements. This reflects lessons from enforcement actions involving program managers and sponsor banks.

Regulation through enforcement has become a defining supervisory approach, particularly in alternative credit and bank partnership models. Following Madden v. Midland Funding, which questioned whether interest rate exportation survives loan assignment, both federal banking agencies and state attorneys general have increased scrutiny of "true lender" arrangements. States have enacted varied responses. Some adopted protective legislation confirming valid-when-made doctrine, while others pursued aggressive enforcement against perceived rent-a-bank structures. Courts remain divided, creating jurisdictional uncertainty for fintechs relying on bank partnership models.

The CFPB has also used enforcement actions to establish regulatory expectations for emerging products like EWA and payroll-linked financial services, issuing interpretive guidance and consent orders that treat into substance reserved for notice-and-comment rulemaking. This approach forces market participants to assess compliance obligations through settlement precedent rather than clear advance guidance.

Embedded finance models present particular structural complexity. Because state licenses apply to individual legal entities and generally cannot be shared across corporate groups, regulators scrutinize which entity in the fintech's structure is actually performing regulated activities. Program managers, white-label service providers, and sponsor banks must each maintain appropriate licenses for their respective activities.

State regulators, coordinated through CSBS, expanded information-sharing agreements and multi-state examinations for money transmitters. API-based reporting and standardized data calls are becoming more common, particularly for BSA/AML compliance and suspicious activity monitoring.

Supervisory models are shifting toward data-driven, coordinated oversight combined with aggressive enforcement to define regulatory boundaries, particularly where fintechs operate across state lines, rely on bank sponsorship structures, or offer products in regulatory gray areas.

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?

Tokenization, decentralized finance (DeFi), and stablecoins are regulated by function, not technology. The SEC evaluates tokenized assets and certain DeFi arrangements under the Howey test, focusing on economic reality over labels. Where tokens resemble investment contracts, trading platforms and intermediaries face broker-dealer or exchange registration exposure. The CFTC asserts jurisdiction where digital assets function as commodities or involve derivatives.

From a banking perspective, the OCC and Federal Reserve permit banks to engage in certain digital asset activities, including custody, stablecoin reserve management, and tokenized deposits, provided safety and soundness expectations are met and supervisory non-objection is obtained.

Stablecoins, more recently, seem to draw the most attention. New York's NYDFS regime imposes reserve segregation, attestation, and redemption requirements. Other states are advancing stablecoin-specific frameworks. Congress continues debating federal legislation that would impose standardized reserve, custody, disclosure, and jurisdictional rules.

Firms must map activities across securities, commodities, banking, and money transmission frameworks simultaneously.

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?

Most custodial crypto businesses are treated as MSBs under FinCEN regulations, requiring BSA compliance, including registration, written AML programs, suspicious activity reporting (SAR), customer identification procedures, and Travel Rule compliance for qualifying transfers.

 © 2026 Legalease Ltd

The Travel Rule requires covered institutions to transmit originator and beneficiary information for transactions above applicable thresholds, driving adoption of industry messaging standards among exchanges and custodians.

For non-custodial or self-hosted wallet models, FinCEN guidance clarifies that software developers who merely provide unhosted wallet code are generally not MSBs. However, once a business exercises control over customer funds or facilitates transmission as an intermediary, it may fall within money transmitter definitions. Regulators focus on control and custody, not branding.

Enforcement activity underscores that regulators look beyond decentralization claims if there is meaningful operational control, fee extraction, or governance concentration. Companies operating near that boundary need careful structuring and independent compliance assessments.

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

Currently, comprehensive federal stablecoin regulation does not exist although some steps have been taken with the passage of the GENIUS Act and continued discussion on the CLARITY Act. New York remains the most developed state regime, requiring issuers under NYDFS oversight to maintain 1:1 reserves in high-quality liquid assets, segregate reserves from operating funds, and provide regular third-party attestations. Monthly public reporting has become a market standard among credible issuers seeking institutional adoption, but this is driven by competitive pressure rather than federal mandate.

Bank regulators have indicated that where insured depository institutions hold stablecoin reserves or issue tokenized deposits, traditional liquidity, capital, and risk management expectations apply. However, these statements reflect supervisory guidance rather than codified rules.

Congressional proposals have typically contemplated requiring reserves of cash and short-duration Treasuries, prohibiting rehypothecation, mandating prompt redemption at par, and subjecting issuers to federal or state supervisory oversight. The GENIUS Act regulates “payment stablecoins," which are any digital asset that is not itself a national currency that “is or is designed to be used as a means of payment or settlement" and that the issuer of which “is obligated to convert, redeem, or repurchase for a fixed amount of monetary value" and “represents that such issuer will maintain, or create the reasonable expectation that it will maintain, a stable value relative to the value of a fixed amount of monetary value." Accordingly, permitted payment stablecoin issuers must maintain 1:1 reserves of appropriate categories of highly stable assets and publish monthly online the amount and composition of those reserves. Further details are expected through forthcoming regulation.

Custodians holding digital assets face enhanced safeguarding expectations following high-profile insolvencies, with regulators emphasizing segregation, bankruptcy remoteness, and clear customer disclosures. However, specific prudential requirements remain fragmented across state money transmission laws and federal guidance rather than unified standards.

The direction is clear in that there is a pressure toward bank-like discipline; however, the framework remains incomplete.

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?

Cybersecurity and operational resilience are core regulatory priorities. The FTC, CFPB, SEC, state and federal banking agencies, and state attorneys general actively enforce data security obligations under consumer protection and privacy statutes. For broker-dealers and investment advisers, SEC cybersecurity risk management rules impose formalized governance, disclosure, and incident reporting requirements. Fintechs and other providers of consumer financial products and services must adhere to comparable FTC standards.

At the state level, fintechs must comply with data security frameworks like the NYDFS Cybersecurity Regulation. All states maintain breach notification statutes, with increasingly coordinated enforcement following data incidents.

Banking regulators have intensified scrutiny of third-party risk management, particularly in embedded finance models where fintechs rely on sponsor banks and cloud service providers. Recent supervisory actions highlight deficiencies in vendor oversight, access controls, and transaction monitoring integration.

Regulators expect board-level visibility into cyber and operational risk. Incident response plans must be tested, vendor contracts must clearly allocate security

 © 2026 Legalease Ltd

responsibilities, and business continuity planning must contemplate cloud and API dependencies.

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?

Fraud detection requires layered controls: blockchain analytics tools, sanctions screening (including Office of Foreign Assets Control (OFAC) list monitoring), behavioral analytics, velocity checks, and enhanced due diligence for high-risk counterparties.

Strong know-your-customer (KYC) procedures remain foundational. Clear escalation protocols, documented suspicious activity report (SAR) decisioning, and independent model validation are critical. Where AI is deployed for fraud detection, regulators expect meaningful human oversight and intervention capabilities. Automated systems must include mechanisms for human review of alerts, override capabilities for false positives, and documented escalation procedures when fraud patterns emerge. The model cannot function as a pure "black box." Compliance teams must understand why the system flags particular transactions and be able to explain decisioning to regulators.

Regulators expect institutions to demonstrate not just that monitoring tools exist, but that alerts are reviewed, trends are analyzed, and remediation is tracked. This requires periodic tuning of AI models to reduce false positives without creating gaps in coverage, regular testing against known fraud typologies, and documentation showing that human analysts remain engaged in the fraud detection process.

Preparation for regulatory audits begins before an inquiry. Companies should maintain updated AML and compliance manuals, board reporting minutes reflecting oversight, documented risk assessments, penetration testing results, and vendor management files. Independent compliance testing, particularly of BSA/AML and sanctions programs, significantly reduces enforcement exposure.

Crisis planning matters. Firms should have documented response plans for subpoenas, regulatory exams, and asset freezes.

Companies that approach compliance as infrastructure, not overhead, are better positioned to attract institutional partners and withstand supervisory scrutiny.

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?

U.S. immigration policy shifts are directly impacting fintech talent strategies. In early 2025, the second Trump administration implemented stricter H-1B visa policies, including increased minimum salary thresholds, heightened scrutiny of specialty occupation classifications, and elevated filing fees. The United States Immigration and Customs Enforcement (ICE) has intensified worksite enforcement and compliance audits, creating uncertainty for employers sponsoring foreign workers.

These changes particularly affect fintechs, which rely on specialized talent for engineers, data scientists, compliance architects, and quantitative analysts, often sourced globally. The H-1B lottery remains unpredictable, and processing delays now extend product development and regulatory timelines.

Additionally, fintechs must navigate state-level restrictions on offshore outsourcing for certain regulated activities. Many states prohibit or restrict outsourcing of debt collection and loan servicing to offshore locations, for example, requiring these functions to be performed by licensed entities within the United States. This limits fintechs' ability to leverage global talent for key operational functions and increases the importance of securing appropriate work authorization for foreign nationals performing these activities domestically.

Fintechs are responding by:

• **Diversifying visa pathways:** Using O-1 visas for extraordinary ability, L-1 transfers for intracompany mobility, and E-3 or TN categories where applicable.

• **Advancing immigration planning:** Initiating visa processes 12-18 months before anticipated need.

• **Structuring operations to comply with state outsourcing restrictions:** Keeping regulated activities onshore while potentially locating non-regulated functions offshore.

• **Monitoring ICE enforcement:** Conducting internal I-9 audits and ensuring worksite verification compliance.

Immigration strategy is now integrated into workforce

 © 2026 Legalease Ltd

planning and regulatory compliance, not treated as a back-office function.

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?

Geopolitical tensions and sanctions regimes are front-and-center operational risks for cross-border fintechs. OFAC has expanded enforcement to include virtual currency addresses, DeFi platforms, and non-custodial intermediaries facilitating transactions with blocked entities.

Regulatory fragmentation complicates compliance. Fintechs must align U.S. OFAC sanctions with evolving international frameworks while navigating country-specific AML and counter-terrorism financing laws. Regulators have levied penalties for inadequate screening of crypto transactions and failing to block transactions tied to sanctioned entities.

Cross-border data governance adds complexity. Data localization requirements and privacy laws vary significantly, affecting fintechs' ability to centralize compliance infrastructure.

To manage these risks, fintechs invest in sanctions screening integrations, blockchain analytics tools, and cross-border legal counsel. Compliance protocols must adapt to evolving geopolitical sanctions rather than relying on static rule sets.

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?

Workforce mobility policies directly influence fintechs' ability to deploy talent where needed, such as for engineers, product leads, compliance officers, and regulatory specialists in markets where products are live or imminent. In the U.S., visa delays and country-specific caps mean fintechs must start immigration processes earlier than anticipated or consider remote deployment from jurisdictions with less restrictive work-permit regimes. Practical strategies include: **Advance planning:** Initiating immigration processes well before market entry targets. **Alternative visa classifications:** Using intra-company transfers (L-1), specialized professional visas, or investor-founder visas. **Hybrid workforce policies:** Leveraging remote work for initial deployment while securing local work authorization. **Compliance frameworks:** Ensuring cross-border remote work aligns with employment, data privacy, and tax laws in each jurisdiction. These steps mitigate delays and ensure critical operational talent is positioned when companies scale into new markets.

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

Immigration constraints present strategic hurdles in how quickly fintechs enter and scale in new markets. If a company cannot physically place a regulatory lead or compliance architect in a jurisdiction at product launch, regulators and partners may view this as a risk factor, which can affect licensing timelines, regulator engagement, and investor confidence.

Immigration rules also influence market prioritization. Regions with flexible pathways for tech and investment immigration become more attractive launch pads. Restrictive work permit regimes necessitate heavier reliance on local hires or outsourcing partnerships, potentially affecting control and culture.

Fintechs should build immigration considerations into market entry playbooks, align talent strategy with regulatory milestones, and engage early with immigration counsel and local employment specialists to minimize delays.

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?

Proprietary value typically sits in algorithms, underwriting logic, fraud models, and smart-contract architecture. These assets are protected through trade secret law (federal Defend Trade Secrets Act and state Uniform Trade Secrets Act regimes), copyright, carefully structured licensing, and patents.

Fintechs should treat core algorithms as trade secrets unless patent protection offers a clear and competitive advantage. This requires strict access controls, documented confidentiality protocols, employee invention assignment agreements, and segmented code repositories. Courts scrutinize whether “reasonable

 © 2026 Legalease Ltd

measures" were taken to preserve secrecy.

Smart contracts introduce complexity because deployment on public blockchains can expose logic. Companies often separate proprietary logic from on-chain execution layers or rely on audited but modular code structures protecting key components off-chain.

Open-source use must be actively managed. Fintechs should maintain formal open-source policies, track dependencies through software composition analysis tools, and avoid inadvertently incorporating copyleft licenses requiring public disclosure of proprietary code.

AI adds another layer. Emerging AI transparency rules in lending and automated decisioning mean firms must balance explainability obligations under consumer protection laws with protection of model intellectual property (IP). This requires disciplined documentation without over-disclosure of proprietary methodologies.

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

Traditional trademark tools, such as federal registration with the U.S. Patent and Trademark Office (USPTO), remain foundational but insufficient alone.

Fintechs increasingly face phishing schemes, deepfake executive impersonations, and cloned websites mimicking digital onboarding flows. Enforcement requires combined IP and cybersecurity strategies: proactive domain name monitoring, rapid Uniform Domain-Name Dispute-Resolution Policy (UDRP) proceedings for domain recovery, social media takedown protocols, and coordinated response plans with hosting providers and app stores.

From a regulatory perspective, consumer protection authorities expect financial institutions to safeguard users against impersonation fraud. Failure to act quickly can expose companies to UDAAP scrutiny if customers are harmed.

Practical steps include:

- Securing defensive domain registrations;
- Implementing brand-monitoring services;
- Developing rapid-response escalation pathways; and
- Coordinating with fraud teams to detect synthetic media threats.

AI-generated impersonation is increasingly treated as a financial crime risk with regulatory implications.

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?

Disputes over code ownership typically stem from poorly drafted agreements. Copyright initially vests in the author unless the work qualifies as “work made for hire” or is expressly assigned. Fintechs must ensure all employees and contractors sign robust invention assignment and confidentiality agreements.

When collaborating with outside developers, clarity around ownership, licensing rights, and derivative works is critical. Master services agreements should specify that custom-developed work product is assigned to the fintech, while background IP remains with the original owner under defined license.

Open-source contributions require additional governance. If employees contribute company-developed improvements to open-source projects, companies should understand whether this impacts proprietary control.

Joint development arrangements are particularly risky. Without clear allocation of foreground IP, parties may unintentionally create jointly owned assets, which under U.S. law can be exploited independently absent contractual restriction.

The most effective strategy typically includes disciplined IP mapping before collaboration begins, identifying background technology, defining ownership of enhancements, and documenting usage rights precisely.

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?

Fintechs should treat IP enforcement as ongoing compliance, not reactive litigation. Monitoring tools detect unauthorized app clones, code scraping, brand misuse, and domain impersonation. For algorithms, forensic analysis and employee exit controls mitigate

 © 2026 Legalease Ltd

insider risk.

When misuse is identified, response options range from cease-and-desist letters and Digital Millennium Copyright Act (DMCA) takedown notices to civil litigation under copyright, trademark, trade secret, or unfair competition laws. The Defend Trade Secrets Act provides federal cause of action, including potential injunctive relief and, in extraordinary cases, ex parte seizure.

From a business perspective, companies should document development timelines and maintain code version histories. These records are invaluable in proving ownership and misappropriation. Stronger documentation provides more leverage in negotiations or court.

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

Distributed infrastructure complicates traditional IP enforcement because infringing activity may not be confined to a single jurisdiction. Smart contracts may be deployed globally, nodes dispersed, and developers operating pseudonymously.

Jurisdictions apply territorial IP laws, but enforcement increasingly focuses on identifiable intermediaries: platform operators, domain registrars, centralized exchanges, or hosting providers. Courts may assert jurisdiction where infringing effects are felt or where commercial activity is directed.

For decentralized projects, governance tokens and decentralized autonomous organization (DAO) structures add complexity. Regulators and courts have shown willingness to look through formal decentralization if identifiable actors exercise meaningful control.

International treaties provide baseline recognition of copyrights and trademarks, but enforcement requires local action. Fintechs operating globally should prioritize registering key IP in major markets and structuring product launches through identifiable entities rather than purely decentralized deployments.

Decentralization does not eliminate enforcement exposure; it shifts where and how it is applied.

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?

Well-drafted license agreements should clearly define scope (e.g., use, territory, duration), prohibit reverse engineering where permitted, restrict sublicensing, and address data ownership.

For AI models, companies should specify training data rights, output ownership, and compliance obligations with applicable privacy and consumer protection laws. Export control laws may apply to certain encryption technologies or advanced software.

Cross-border licensing raises additional issues, including local consumer protection laws, mandatory warranty rules, data localization requirements, and technology transfer regulations. Governing law and dispute resolution clauses should be chosen strategically, often favoring arbitration for international deals.

Fintechs should avoid outright IP transfers unless strategically necessary. Structured licenses paired with audit rights and termination triggers for misuse preserve leverage and regulatory flexibility.

IP strategy should align with regulatory compliance, cybersecurity safeguards, and long-term enterprise value.

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?

For U.S. fintechs, AI does not change the law, but it changes how existing laws apply. In underwriting, robo-advisory, and fraud detection, regulators emphasize that ECOA, FHA, FCRA, the Investment Advisers Act, and UDAAP apply fully to AI-driven systems.

In credit underwriting, if AI models influence approval, pricing, or adverse action decisions, lenders must provide compliant adverse action notices with specific and accurate reasons under ECOA and FCRA. "Black box" models that cannot generate explainable outputs create regulatory risk. The CFPB and state banking agencies clarify that use of complex models does not excuse noncompliance. State fair lending laws and state consumer protection statutes impose parallel or additional obligations, often with private rights of action.

Importantly, fintechs offering both consumer and

 © 2026 Legalease Ltd

commercial lending products must carefully analyze which transactions trigger consumer protection requirements. AI models used in underwriting must account for this complexity. For example, a fintech using AI to underwrite commercial real estate loans must ensure its models can identify when a loan secured by real property improved by one-to-four family dwelling units and made to a natural person triggers consumer lending compliance, including adverse action notice requirements, regardless of stated business purpose. Failure to properly classify transactions exposes fintechs to compliance violations even where the borrower characterizes the loan as commercial.

For robo-advisory platforms, fiduciary obligations under the Investment Advisers Act remain central. The SEC expects algorithm-driven advice to be suitable, aligned with client disclosures, and subject to oversight and testing.

While proposed U.S. federal AI legislation remains unsettled, supervisory agencies already enforce expectations through existing authority. State AI laws, including Colorado's AI Act (effective 2026), impose additional transparency, risk assessment, and impact analysis requirements on high-risk AI systems, including those used in consequential decisions like credit and insurance underwriting.

Fintechs must treat AI as a regulated operational function, not a compliance workaround, and ensure AI systems can accommodate the nuanced regulatory classifications that depend on borrower, collateral, and transaction characteristics.

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

Regulators focus on governance, not just outcomes. Fintechs must evidence fairness and explainability through:

• **Documented model development lifecycles:** Defined objectives, training data validation, feature selection analysis, and periodic revalidation.

• **Fair lending risk assessments:** Disparate impact testing across protected classes and proxy methodologies where direct demographic data is unavailable.

• **Explainability in credit decisioning:** Even with advanced machine learning, firms must translate outputs into understandable adverse action reasons.

• **Vendor oversight:** Model documentation reviews and contractual audit rights for AI solutions providers.

• **AML and fraud monitoring:** Tuning and back-testing to ensure models don't systematically under- or over-flag certain populations, with documented human oversight.

For fintechs serving both consumer and commercial markets, AI governance becomes more complex. Models must properly classify transactions that may trigger consumer protection requirements based on borrower type, collateral characteristics, or occupancy status, not merely stated purpose. For example, an AI underwriting model for commercial real estate lending must be designed to identify loans secured by real property improved by one-to-four family dwelling units made to natural persons, flagging these for consumer lending compliance even when the borrower states a business purpose. Similarly, fintechs offering private student loans or small business lending products must ensure AI models account for applicable disclosure and reporting obligations that vary based on loan purpose, borrower characteristics, and loan amount. Training data should reflect this regulatory complexity, and model outputs must support compliant adverse action notices where required.

Human oversight remains mandatory. Even sophisticated AI systems require documented human intervention points. This includes escalation protocols when models produce unexpected results, periodic manual review of automated decisions, and clear authority for compliance personnel to override algorithmic outputs when warranted. Regulators are increasingly scrutinizing whether fintechs have maintained meaningful human control over automated decisioning, particularly in fair lending contexts.

Independent model validation, separate from development teams, has become best practice. Board and senior management reporting should reflect oversight of AI risk, not just performance metrics. Fairness must be measurable, documented, and revisited regularly. If a firm cannot explain how its model works, why it produces specific outcomes, how it accounts for regulatory classification nuances, and where humans remain in the loop, regulators will not be satisfied.

24. What are the IP and data-protection considerations around training proprietary AI

 © 2026 Legalease Ltd

models on financial data, and how can fintechs structure data-sharing agreements to minimize risk?

Training AI models on financial data raises intertwined IP and data-protection issues. Financial data is often subject to contractual confidentiality obligations, federal privacy statutes (e.g., the federal Gramm-Leach-Bliley Act (GLBA)), state privacy laws, and bank secrecy constraints.

From an IP standpoint, firms should clarify ownership of trained models, weights, and derivative improvements in employment and vendor agreements. If third-party datasets are used, license terms must explicitly permit AI training and commercial deployment.

Privacy laws impose additional guardrails. Use of consumer financial data for secondary purposes must align with disclosed privacy notices and permissible-use requirements. De-identification processes should be robust and documented, and may fail to satisfy regulatory scrutiny where the data is re-identifiable.

Data-sharing agreements should clearly address:

- Permitted use and retention limits;
- Security controls and audit rights;
- Allocation of liability for misuse; and
- Restrictions on model retraining beyond scope.

Given cross-border data flows, firms must account for transfer restrictions and localization laws.

The safest approach is often disciplined data mapping before model development begins.

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

Regulators do not distinguish between human and algorithmic decision-making when applying fiduciary or fair lending standards. If an AI-driven robo-adviser recommends portfolios, the SEC expects that advice to meet suitability and fiduciary obligations, be consistent with disclosures, and avoid conflicts of interest.

In credit decisioning, regulators apply ECOA and fair lending analysis to AI models. Disparate impact risk remains central. If an algorithm results in statistically significant disparities without defensible business justifications and less discriminatory alternative analysis, enforcement risk increases.

Disclosure obligations are evolving. Marketing materials describing "AI-powered" credit or investment solutions must avoid overstating capabilities. Regulators signal concern about "AI washing" (i.e., exaggerating AI sophistication without substantiation).

Supervisory expectations extend to governance, including board oversight, documented policies, and escalation protocols. Firms treating AI tools as vendor-managed "black boxes" risk findings related to third-party risk management and failure to supervise.

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

Expect increasing focus on negligent model governance and failure-to-supervise theories. Regulators may frame enforcement actions around inadequate testing, poor documentation and recordkeeping, or lack of meaningful oversight of automated systems. Meanwhile, plaintiffs' attorneys are expected to explore claims tied to algorithmic discrimination and misrepresentation. As many businesses race to leverage AI and overlook proper testing before implementation, significant failures can lead to negative publicity, customer impact, and class action litigation.

In AML and fraud detection, failure to calibrate models properly or maintain adequate human oversight could be characterized as an unsafe or unsound practice. Regulators have signaled concern about "set-it-and-forget-it" AI deployments where compliance teams cannot explain why transactions were flagged or cleared. In lending, inaccurate adverse action explanations tied to opaque AI outputs create litigation exposure. In investment advisory, algorithmic errors could trigger breach-of-fiduciary-duty claims.

Emerging liability theories include:

• **Inadequate human oversight:** Claims that fintechs delegated decision-making entirely to algorithms without maintaining human intervention capabilities.

• **Proxy discrimination:** Allegations that AI models use seemingly neutral variables that function as proxies for

 © 2026 Legalease Ltd

protected characteristics.

• **Misrepresentation of AI capabilities:** Marketing materials overstating model sophistication or accuracy, leading to consumer harm.

• **Vendor over-reliance:** Failure to supervise third-party AI providers or conduct adequate due diligence on purchased models.

To build defensible frameworks, fintechs should:

- Establish formal AI governance committees;
- Maintain documented model risk management consistent with regulatory agency guidance;
- Conduct periodic independent validation;
- Align disclosures with actual system functionality; and
- Implement clear human-override and escalation processes with documentation showing these mechanisms are actually used.

Documentation must demonstrate that risks were identified, assessed, and actively managed. When regulators evaluate AI systems, they judge not only outcomes, but also whether and to what extent leadership exercised reasonable oversight and whether meaningful human control remained in place.

Firms that treat AI governance as enterprise risk management, not product marketing, will weather scrutiny best.

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

Several interconnected trends have reshaped U.S. fintech markets over the past year, with regulatory scrutiny accelerating alongside innovation.

Embedded Finance and BaaS Maturation: Non-financial platforms increasingly integrate payments, lending, wallets, and insurance directly into their ecosystems through BaaS platforms and bank-fintech partnerships. What was once novel is now baseline infrastructure for vertical SaaS providers and e-commerce platforms. Payroll, accounting, point-of-sale, and enterprise resource planning systems now embed financial products—from working capital loans to card issuance, directly within their workflows. This has shifted fintech competition from consumer-facing brands to B2B infrastructure providers.

Simultaneously, sponsor-bank relationships have come under unprecedented regulatory scrutiny. Banking agencies have issued and enforced third-party risk management expectations, particularly around BSA/AML controls, customer disclosures, and program oversight. The embedded finance and BaaS models are maturing from growth-at-all-costs to infrastructure-first compliance discipline.

Payroll-Linked Financial Services and EWA: One of the most significant disruptions to financial services and products involves the rapid growth of EWA programs and payroll-embedded financial services, and the scrutiny with which such programs and services have been greeted at the state level. Fintechs are partnering with employers and payroll processors to offer employees early access to earned wages, often through tips-based or subscription models. This has drawn heightened regulatory attention, with states enacting new licensing frameworks and regulators debating whether these products constitute credit under TILA and state lending laws. Several states now require specific EWA licensing or registration, while others have issued guidance treating certain EWA structures as consumer loans. The regulatory landscape shifts with each legislative session, creating compliance uncertainty for fintechs scaling these products nationally.

Alternative Credit and Regulation Through Enforcement: Alternative credit products, including merchant cash advances, revenue-based financing, and non-recourse advance models, continue expanding whilst facing increased enforcement scrutiny. Regulators and state Attorneys General are challenging product characterizations through enforcement actions, arguing that transactions that function economically as loans should be regulated as such regardless of contractual labels. This extends to fintechs offering products straddling consumer and commercial classifications. For instance, fintechs providing fix-and-flip or bridge loans for real estate investment must navigate situations where loans secured by an interest in real property improved by one-to-four family dwelling units made to natural persons may trigger certain consumer mortgage lending requirements despite the business purpose characterization of the transaction. This regulatory classification complexity mirrors the broader "regulation through enforcement" trend seen in bank partnership lending models following Madden v. Midland Funding, where "true lender" and "valid-when-made" doctrine challenges create ongoing litigation risk.

AI-as-a-Service: Fintechs are increasingly offering AI-powered underwriting, fraud detection, and customer service tools to traditional financial institutions, creating

 © 2026 Legalease Ltd

new regulatory questions around vendor management, model governance, and liability allocation when AI decisioning is outsourced.

Institutional Tokenization: Rapid institutional adoption of tokenization and blockchain-based settlement pilots within regulated financial institutions represents another shift. Rather than competing with traditional finance, many fintech innovations are being absorbed into bank-led frameworks, particularly in payments modernization and liquidity management.

The net effect is a US fintech market that is still expanding, but with materially greater supervisory guardrails, enforcement risk, and infrastructure complexity than in prior cycles. Innovation continues, but increasingly within defined regulatory parameters established through both formal guidance and enforcement precedent. Fintechs must navigate not only product-specific regulation, but also the nuanced boundary between consumer and commercial regulatory frameworks where transaction characteristics, not stated purpose, determine compliance obligations.

28. 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?

The greatest accelerator would be meaningful harmonization within and among regulatory agencies, whether through coordinated stablecoin reserve standards, streamlined multi-state or preemptive federal licensing, or clearer digital asset classification at the federal level.

State-by-state licensing remains one of the most resource-intensive barriers to scaling payments and lending models. Continued adoption of harmonization efforts through coordinated supervision and standardized money transmission rules could materially reduce friction. Although the GENIUS Act provides a baseline federal framework for payment stablecoins, with some reserve, redemption, and supervisory standards, it did not broadly invoke preemption to displace state money transmitter licensing requirements, preserving the federal-state duality that imposes market complexity and hampers broader institutional participation.

Globally, interoperability of stablecoin reserve standards and cross-border recognition of prudential oversight would significantly reduce duplicative compliance burdens. MiCA has influenced global conversations, increasing industry discussion about aligning reserve quality and disclosure expectations across jurisdictions.

Structured cross-border regulatory dialogue, particularly between U.S. and EU regulators, around AI governance, digital identity, and payments modernization could reduce fragmentation, as well.

In short, clarity, not deregulation, will ostensibly be most operative in accelerating innovation. Markets move efficiently when rules are defined, supervisory expectations are transparent, and companies can plan capital deployment with confidence.

Contributors

Lisa M. Lanham
Partner, Head of Fintech Licensing

llanham@orrick.com

 © 2026 Legalease Ltd