MICROBLINK

Fintech Trends Explained

The Compliance Leader's Guide

An in-depth look at the most pressing issues compliance managers are facing today in identity in financial services, fintech, crypto and payments.

Financial services compliance is undergoing a seismic shift. Banks, fintechs, and payments providers are being squeezed in many directions. These include budget cuts, staffing reductions, mounting regulatory scrutiny, and the proliferation of sophisticated financial technologies. Compliance officers today must navigate increasingly strict oversight in many cases with fewer resources.

Compliance leaders are burned out

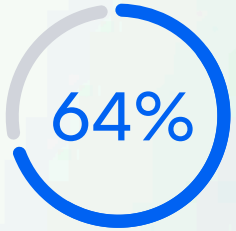
Headcount is shrinking

Regulations are changing

Technology is rewriting fraud and user experience

42% of financial crime prevention professionals had considered leaving their role due to burnout, indicating significant staffing pressure and retention risk across AML/compliance teams.

And according to LinkedIn's Financial Services Workforce Trends report, compliance roles grew just 2.1% in Q2, compared to 6.4% last year.



of U.S. banks and credit unions viewed keeping pace with regulatory changes as a moderate or high concern in 2024.

At the same time, regulators around the globe are continuing to issue new rules. The U.S. Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB) have ramped up their activity in areas such as open banking. Those in the EU, UAE, and Singapore are also updating their frameworks at a faster cadence, focusing on digital onboarding, open data exchange, and AI-driven decision-making.

The rapid advancement of technology is redefining what compliance even means. Innovations such as generative AI, open banking APIs, and tokenized digital assets promise more automation, personalization, and user-centricity.

But they also come with new attack surfaces and oversight risks. This means compliance leaders are being pulled into uncharted territory, where traditional approaches no longer scale, and innovation is mandatory.

That's why we are taking a deep dive into the most pressing issues for compliance managers at financial institutions today and outlining how product and compliance leaders can turn each into a strategic advantage.

In this report:

Open Banking

Agentic AI

Stablecoins

The Global Evolution of Open Banking

Open banking was once seen as a UK- and EU-centric phenomenon but that is no longer the case. Many countries are designing and implementing their own open banking standards. In this report, see a snapshot of the frontrunners.

AT A GLANCE

Open Banking Regulations Around the Globe

Brazil Open Finance Law

The Banco Central do Brasil (BCB) and the National Monetary Council (CMN) define this initiative as promoting the sharing of data, products and services between regulated entities, including financial institutions, payment institutions and other entities licensed by BCB at the customers' discretion.

Timeline: Rolling phases (2021 onward); supervised by BCB and mobile Open Finance Council

Fines / accountability: Institutions face administrative penalties for non-compliance under BCB enforcement rules

Singapore's SGFinDex

SGFinDex is a government-led data-sharing platform that allows Singaporeans to aggregate their financial information from banks, insurers, and the Central Provident Fund (CPF) into a single view, empowering smarter financial decisions.

Timeline: First phase launched in December 2020; extended to insurance data in 2022. Continuous API enhancements and new integrations planned through 2025.

Fines / cost of non-compliance: MAS enforces data protection compliance under the Personal Data Protection Act (PDPA). Breaches can lead to fines up to SGD $1 million, with ongoing regulatory audits.

UAE Financial Infrastructure Transformation (FIT)

The UAE's FIT program is a comprehensive strategy to modernize its financial system, focusing on instant payments, digital identity, and open finance frameworks to drive a cashless, digitally connected economy.

Timeline: Launched in February 2023, with a phased rollout through 2026. Key milestones include the Instant Payments Platform (IPP) by late 2025 and full Open Finance enablement by 2026.

Fines / cost of non-compliance: The CBUAE imposes financial penalties, licensing restrictions, and public enforcement notices for non-compliance with FIT regulations. Providers failing cybersecurity or KYC obligations face suspension.

In the U.S., while regulation still lags behind much of the rest of the world, the Consumer Financial Protection Bureau's (CFPB) proposed Rule 1033 is poised to standardize how consumer financial data must be shared between institutions, mandating that financial institutions must provide consumers with access to their financial data in a standardized, machine-readable format. It aims to create a regulated open banking ecosystem in the U.S., improving consumer control over data and enabling secure third-party access. Pending the final rule, financial institutions will likely face phased compliance deadlines starting in 2026

As data flows freely across institutions, compliance leaders face a new balancing act: enabling seamless access while protecting against misuse, data leakage, and identity fraud.

Open Banking Flow

Customer Consent → Bank A's API → TPP Aggregator → Bank B/Fintech → Risk Engine + KYC Verification → End User Dashboard

This process depends on highly secure data exchange protocols such as OAuth2.0 and FAPI (Financial-grade API), which enforce consent layers and authentication steps. But the integration work is complex. Banks must verify not just customers' identities, but the third-party providers (TPPs) requesting access to their data.

CASE STUDY

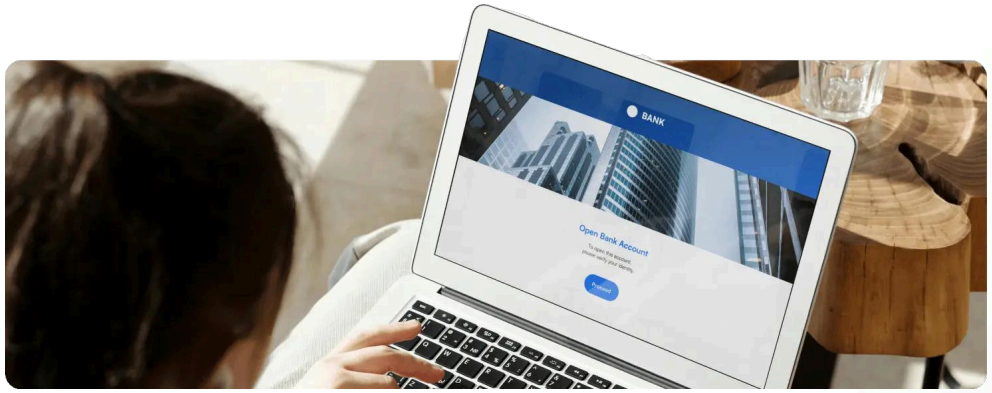
Monzo

UK challenger bank Monzo has built its entire infrastructure around open APIs.

Their system allows users to instantly connect external budgeting apps, payment providers, and credit tools — but only after robust device-based authentication and biometric consent.

Monzo's compliance stack includes:

- OAuth2.0 for authorization
- Mutual TLS for secure transport
- Risk scoring powered by real-time behavioral signals



Institutions still playing catch-up must adopt similar standards, especially as regulations such as Rule 1033 goes into effect. In theory, this move towards open banking should help reduce KYC and AML burdens on compliance teams.

As one Chief Innovation Officer of a mid-sized U.S. bank told Microblink in an interview:

> "If I've been banked with no red flags at one bank, why can't I open an account at another bank without doing KYC all over again?"
>
> - Chief Innovation Officer, regional bank

Screen Scraping Phase-Out

As open APIs become the norm, legacy screen scraping methods, where third-party apps "read" user bank accounts via login credentials, are sunsetting.

Screen scraping was primarily the method by which financial data was shared prior to open banking, and it was long criticized for privacy and efficiency reasons. This shift to open banking improves privacy and control, but also requires fast modernization from banks still relying on outdated integration points.

The key to open banking for compliance professionals is to ensure that customer data is always safe, and to not try and do too much, too soon. Start by testing the waters and creating guardrails.

As our bank CIO noted, "The customer's data and products are safe with us; it's not just handed off to the fintech or brand. We're listening to partners, but we're not jumping on every trend. Guardrails matter"

Open Banking

Regulatory Sentiment Summary:

Balanced, cautious optimism

Regulators are promoting open banking to boost competition and consumer control, but concerns over privacy, data protection, and secure API implementation remain front and center. Success (or failure) often hinges on execution details like authentication protocols and third-party governance.

In their Words:

"This train [open banking] is way too far down the tracks. They're not going to stop this one. Get to work complying with it."

- The Financial Brand

OPEN BANKING REGULATORY COMPLIANCE RESOURCES

- Banco Central do Brasil — Open Finance regulation
- Monetary Authority of Singapore (MAS) — SGFinDex / open finance guidance
- UAE Central Bank — FIT program updates
- CFPB / OCC (US) — Rule 1033 rollout and updates
- EU's PSD2 Rules

Agentic AI in Compliance

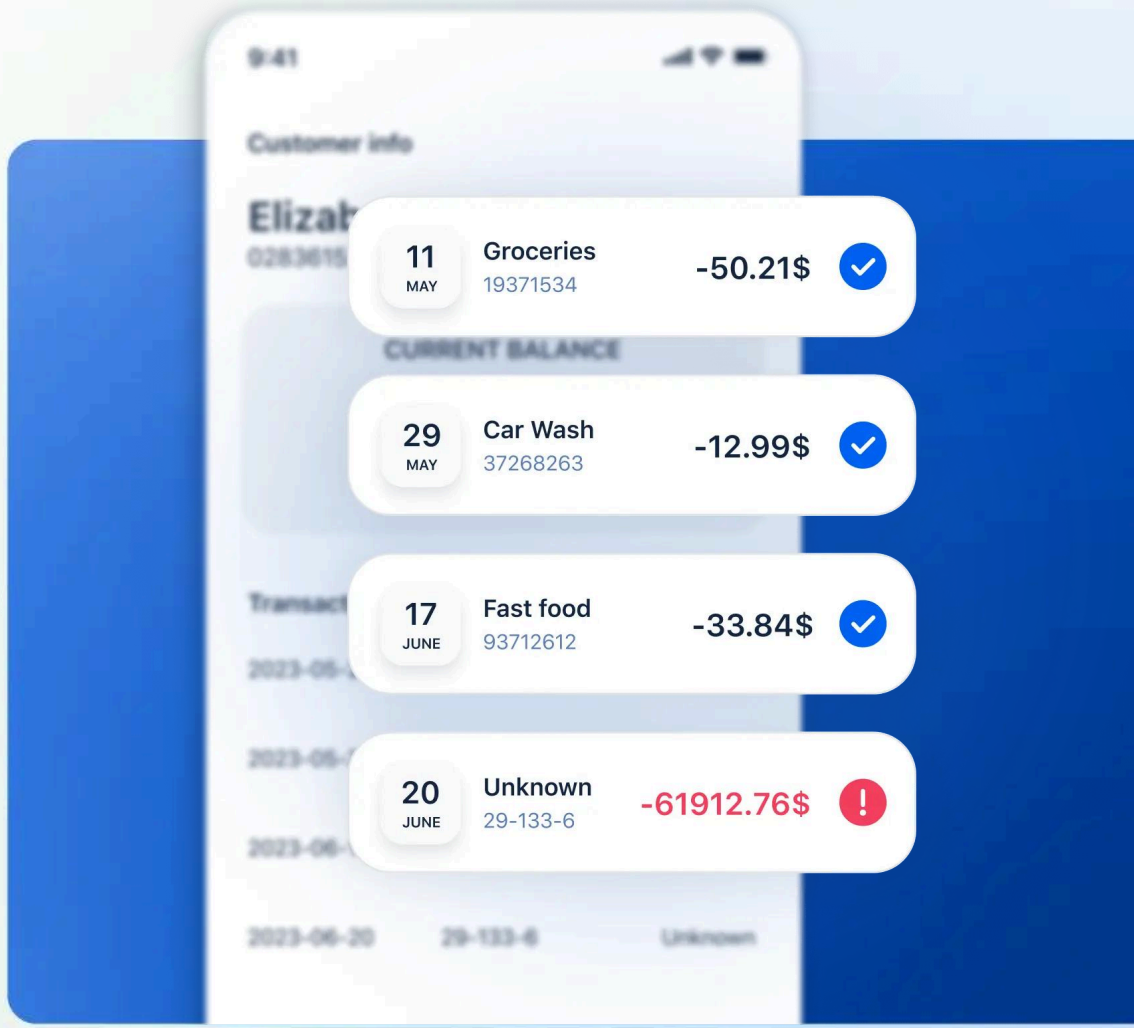
A New Regulatory Grey Zone

2025 has been a breakout year for agentic AI. These are frameworks that combine models with autonomous goal-setting, reasoning and multi-step execution. Such systems are already being used in financial services for tasks such as:

- Generating personalized onboarding experiences
- Pre-filling KYC forms based on behavioral data
- Flagging suspicious transactions in real-time
- Coordinating multi-system workflows across CRMs, KYC tools, and fraud platforms

But with these capabilities come new risks, such as hallucinations in model outputs, which can be exacerbated as the AI operates autonomously.

AI agents may also struggle to detect sophisticated synthetic identities since they may overly trust certain data sources or patterns. Finally, regulators will require decisioning explainability when it comes to agentic AI.



Agentic AI in KYC Workflows

Input: New user → AI Agent: Identity Pre-check → Document Validation API → Address Match + Watchlist Screening → Final KYC Decision + Audit Trail

One key challenge is explainability. Compliance leaders must prove to regulators (and internal auditors) that agentic systems' decisions are based on valid, auditable logic, and not opaque model weights or third-party data vendors with unknown provenance.

Our CIO source noted:
"AI systems are only as trustworthy as their feedback loops. Without a closed-loop audit mechanism, you're gambling with your license."

CASE STUDY

Klarna

Swedish fintech Klarna uses AI agents to power real-time fraud detection and frictionless onboarding across millions of users. Their AI stack includes:

- User flow simulations to optimize conversion
- Language-based AI agents to interpret ID documents in over 40 languages
- Real-time synthetic identity detection powered by anomaly pattern recognition

Klarna's approach shows how to harness agentic AI while maintaining compliance:

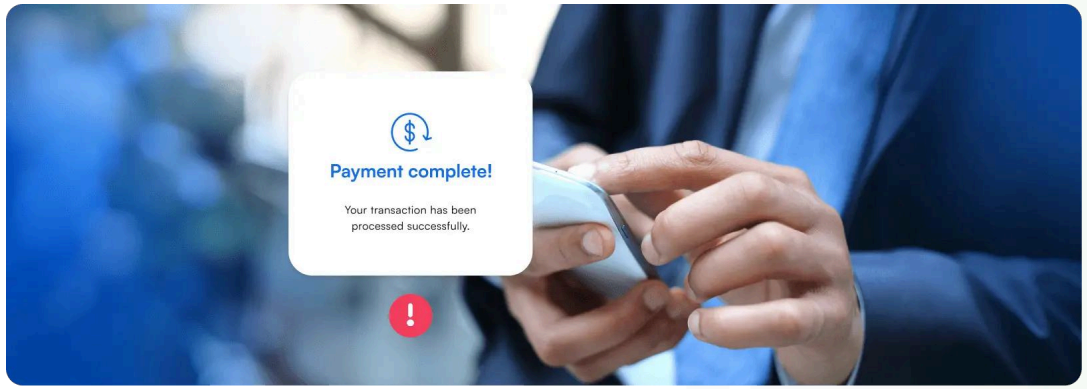
- They retain a human-in-the-loop for all flagged cases
- Every AI decision is paired with a "reason code" stored for audit trails
- A centralized compliance dashboard offers transparency across the pipeline

KNOW YOUR AGENT (KYA)

A New Mandate for Compliance Leaders

As AI systems start to function as autonomous agents capable of making decisions and interacting with external systems, “Know Your Agent” (KYA) is emerging as a critical compliance priority. Unlike traditional software, agentic AI systems can initiate actions, access sensitive data, and learn new behaviors dynamically, thus creating new vectors for operational risk, bias, and regulatory exposure.

Traditional KYC frameworks are insufficient to manage these AI-driven agents. KYA shifts the focus from verifying who a user is to verifying what an autonomous agent is authorized to do, under which context, and with which level of oversight.



Compliance leaders must:

Establish visibility into agent behaviors
Implement runtime monitoring that captures the decision pathways AI agents take, which datasets they access, and how these actions map to internal policy frameworks.

Implement dynamic risk controls
Traditional rule-based governance isn’t enough. KYA requires adaptive oversight mechanisms that evolve as agents learn and operate across changing data environments. This includes context-aware access controls and policy-driven execution constraints.

Ensure explainability and auditability
Regulators will expect clear documentation of an agent’s decision-making logic, model assumptions, and audit trails for every autonomous action taken. Compliance teams need tooling that can surface “reason codes” for AI-driven decisions in real-time.

Enter the Model Context Protocol (MCP)

One emerging solution to KYA challenges is the Model Context Protocol (MCP), a framework designed to standardize how AI agents declare their operational context, capabilities, and constraints when interacting with external systems. It should be noted that the MCP is still an emerging framework and there are no industry-accepted standards around it just yet.

As regulations such as the EU AI Act and state regulators in the U.S. start demanding “context-aware AI accountability”, protocols like MCP will become essential for proving that autonomous agents operate within the institution’s risk tolerance.

MCP enables compliance teams to:

- **Define a machine-readable “context envelope”** around AI agents, specifying allowed actions, decision boundaries, and data access privileges.
- **Track dynamic context shifts in real-time** as an agent learns or adapts, MCP provides a mechanism to update compliance constraints automatically.
- **Facilitate third-party verification** of agent behavior by providing standardized logs of decision flows and context declarations.

Emerging Regulation

The EU's AI Act (passed in 2024) places AI-powered identity verification and fraud scoring in the "high-risk" category, requiring detailed documentation, third-party auditing, and bias mitigation. This measure has been divisive. While some tech giants, such as Apple, Google and Microsoft, have signed on agreeing to participate with the rules, others — such as Meta — refused to sign, saying the measure stifles innovation.

While the U.S. has yet to pass similar national legislation, state regulators in California and New York are already drafting AI transparency rules and aligning these rules with algorithmic accountability and auditability principles. These rules are set to be formalized by 2026.

SPOTLIGHT ON

EU Artificial Intelligence Act

Who: The EU AI Act doesn't describe a specific person who is responsible for AI compliance. Instead, it casts the net wide and holds the organization itself accountable.

What: Defines risk-based regulation: • GPAI models (governance lines starting August 2, 2025) • High-risk AI systems

Timeline: Effective August 1, 2024; GPAI obligations August 2025; full enforcement August 2026

Fines / cost: Up to €35 million or 7% of global annual turnover for breaches

Who is responsible in firms: CCO / AI Ethics Officer, Data Science Compliance councils

Agentic AI

Regulatory Sentiment Summary:

Wary

Compliance leaders recognize the automation potential of agentic AI but are deeply cautious. Without clear frameworks in place, regulators and corporations alike fear opacity, rogue behaviors, and accountability gaps. Emerging legislation (such as EU AI Act and country-level AI rules) is pushing firms toward transparency and human oversight.

In their Words:

"Agentic AI is no longer theoretical. From AI co-pilots to autonomous decision agents, these systems are reshaping how businesses operate and interact with users. But autonomy doesn't mean freedom from regulation. In fact, agentic AI increases the regulatory burden, especially in demonstrating explainability, accountability, and legal responsibility."

- Dr. Nathalie Moreno

AGENTIC AI REGULATORY COMPLIANCE RESOURCES

- European Commission — AI Act implementation timeline and risk classification
- SCCE / ICA — AI regulation and compliance community events in finance
- PwC analysis of EU AI ACT requirements
- Analysis of legal considerations pertaining to agentic AI

Stablecoins

The New Frontier for AML Monitoring

Stablecoins like USDC, USDT, and PYUSD have moved from the crypto fringe to the mainstream. PayPal's recent integration of its own stablecoin (PYUSD) across merchant flows has accelerated adoption, along with regulatory interest. For example, the passage of the GENIUS Act in the U.S. mandates that stablecoin issuers and digital asset service providers comply with Bank Secrecy Act rules—this includes Know-Your-Customer processes, ongoing monitoring, and adhering to anti-money laundering protocols.

As stablecoin rails become embedded in peer-to-peer apps, treasury operations, and cross-border payments, banks must treat them like any other regulated asset.

Key Compliance Risks:

On/off-ramp laundering

Converting fiat to stablecoins (and back) can obscure source of funds and potentially be used for money laundering.

Wallet obfuscation

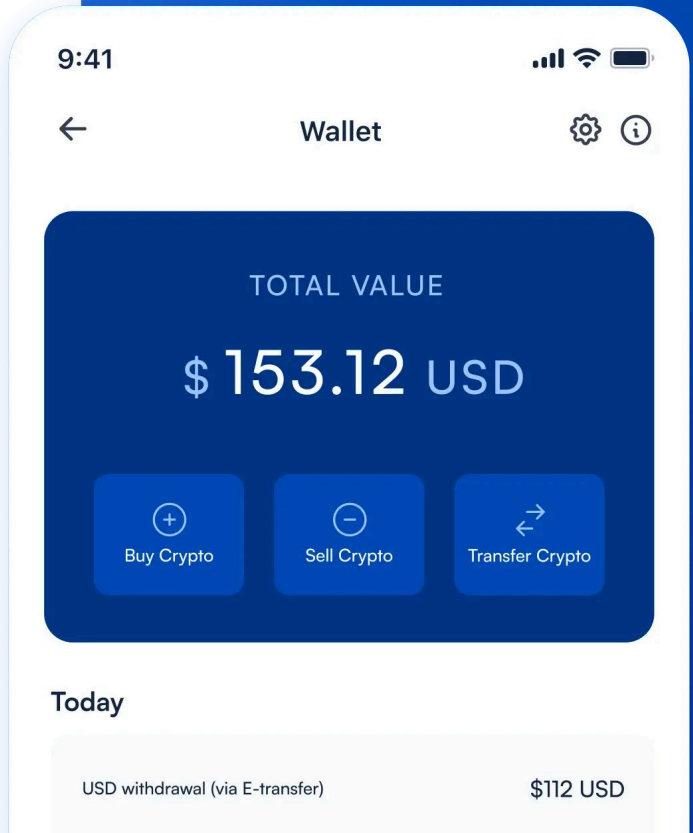
Use of mixers or stealth wallets to bypass AML controls.

Cross-jurisdiction flows

Transfers between different geographies create overlapping regulatory obligations.

Stablecoin Flow with AML Checkpoints

User Wallet → Stablecoin Issuer (e.g., Circle) → Merchant Platform → Settlement → Fiat Bank Account
↓
AML Transaction Monitoring + Wallet Risk Scoring + Sanctions Screening



Where Compliance Interacts at Each Stage of the Flow

1 Stablecoin Issuer

- **Compliance Role:** The issuer is responsible for KYC/AML onboarding of wallet holders, continuous transaction monitoring, wallet screening, and adherence to regulatory frameworks like MiCA in the EU and the U.S. GENIUS Act.
- **Key Compliance Risks:** Source of funds verification, wallet obfuscation, sanctions evasion.
- **Governing Regulations:** Bank Secrecy Act (BSA), OFAC sanctions, state-specific digital asset licensing (e.g. NY BitLicense).
- **Risk Burden:** High.
  Issuers are on the front line for anti-money laundering compliance and bear direct regulatory scrutiny.

2 Merchant Platform

- **Compliance Role:** Merchants must perform transaction-level screening to detect anomalous payments, fraudulent behaviors, or sanctioned wallets, often via third-party AML services.
- **Key Compliance Risks:** On/off-ramp laundering, fraud chargebacks, transaction structuring.
- **Governing Regulations:** Vary by jurisdiction, but typically include consumer protection laws and AML obligations if the merchant is classified as a Money Services Business (MSB).
- **Risk Burden:** Moderate.
  Merchants face fines for failing to detect suspicious transactions but typically rely on upstream partners (issuers/payment processors) for core compliance checks.

3 Settlement Layer (Payment Processor / Blockchain Settlement)

- **Compliance Role:** Payment processors facilitate the movement of funds and must maintain audit trails, real-time transaction risk scoring, and ensure settlement finality within regulatory bounds.
- **Key Compliance Risks:** Layering and placement of illicit funds, privacy coins or mixer integration.
- **Governing Regulations:** Varies depending on the region but often includes FATF recommendations and localized payment system laws.
- **Risk Burden:** Moderate to High.
  Processors are scrutinized for enabling illicit fund flows but may pass compliance attestations onto upstream partners.

4 Fiat Bank Account (Receiving Institution)

- **Compliance Role:** The bank is responsible for final source-of-funds verification, AML transaction monitoring, and Suspicious Activity Report (SAR) filings.
- **Key Compliance Risks:** Integration of illicit funds into the traditional financial system (money laundering "placement"), KYC mismatches.
- **Governing Regulations:** Bank Secrecy Act (BSA), FATF AML standards, country-specific financial regulations.
- **Risk Burden:** Very High.
  Banks are ultimately accountable to regulators for ensuring no illicit funds enter the traditional banking system. They face the most severe penalties for AML breaches.

5 Crypto Exchanges

- **Compliance Role:** The exchange is responsible for onboarding and verifying customers, conducting KYC/AML checks, monitoring transactions for suspicious activity, and reporting to relevant regulators or Financial Intelligence Units (FIUs).
- **Key Compliance Risks:** Onboarding of bad actors using synthetic IDs or deepfakes, facilitation of money laundering via anonymity-enhancing tools (mixers, privacy coins), use of sleeper accounts to move illicit funds later, sanctions breaches.
- **Governing Regulations:** FATF Travel Rule, country-specific virtual asset service provider (VASP) regulations, AMLD5/AMLD6 (EU), FinCEN AML requirements (U.S.), Monetary Authority of Singapore (MAS) AML/CFT guidelines.
- **Risk Burden:** Very High.
  Crypto exchanges are primary gateways between fiat and digital assets, making them prime targets for illicit activity. Regulatory expectations are increasing globally, and exchanges face severe penalties, license revocation, and reputational harm for AML/CFT failures.

Emerging Oversight

The Financial Stability Oversight Council (FSOC) in the U.S. has proposed treating major stablecoin issuers as Systemically Important Financial Institutions (SIFIs). This could subject issuers, and by extension their banking partners, to bank-like compliance requirements, including real-time transaction monitoring, independent audits, and capital reserves.

In the European Union, stablecoins fall under the scope of the Markets in Crypto-Assets (MiCA) regulation. While MiCA doesn't explicitly use the term "stablecoins", it categorizes them into two distinct types: E-Money Tokens (EMTs) and Asset-Referenced Tokens (ARTs). EMTs are digital tokens pegged to a single fiat currency, functioning similarly to electronic money. ARTs, on the other hand, are backed by a diversified basket of assets, which may include a mix of fiat currencies, cryptocurrencies, or tangible assets like commodities.

CASE STUDIES

JPMorganChase

JPMorgan Chase

JPMC's Kinexys (formerly Onyx) now uses blockchain-based settlement for institutional payments, including stablecoin equivalents. Their compliance architecture includes:

- Real-time blockchain analytics
- Wallet screening
- Transaction risk scoring tied to user KYC profiles

Central Bank of Bahrain

مصرف البحرين المركزي
Central Bank of Bahrain

Meanwhile, in the Middle East, Bahrain's central bank has greenlit pilot programs allowing licensed digital asset custodians, with automated AML monitoring pipelines feeding into central repositories.

Stablecoins

Regulatory Sentiment Summary:

Enthusiastic but urgent

Regulators (especially in the U.S.) are signaling strong support for stablecoins with many seeing them as both an innovation driver and a strategic fintech competitiveness tool. With the passage of the GENIUS Act and the CLARITY Act, compliance urgency has dramatically increased. Regulators expect operational maturity, full transparency, and robust AML/consumer protections.

In their Words:

"Our position is that stablecoins should be regulated by issuer, with non-bank issuers being regulated as issuing commodities or securities, and bank issuers being regulated as issuing a banking product akin to a tokenized deposit."

- White & Case LLP

STABLECOINS REGULATORY COMPLIANCE RESOURCES

- GENIUS Act factsheet
- FDICnote to banks engaging in cryptocurrency activity
- Financial Stability Oversight Council (FSOC) — SIFI designation updates
- GENIUS Act academic analysis from NYU

Conclusion

Compliance as a Competitive Advantage

Across open banking, agentic AI, and stablecoin infrastructure, one message for compliance leaders stands out:

Embrace emerging technologies, but demand explainability and control. As AI-driven systems become more embedded in your workflows, it's your responsibility to ensure their decisions are transparent, auditable, and aligned with evolving regulations.

At the same time, this is your opportunity to reframe compliance as a driver of competitive advantage. By proactively managing risks in new digital ecosystems—rather than reacting after the fact—you can help your organization move faster, build customer trust, and differentiate in a crowded market. The future of compliance isn't back-office oversight; it's front-line strategy.

This means:

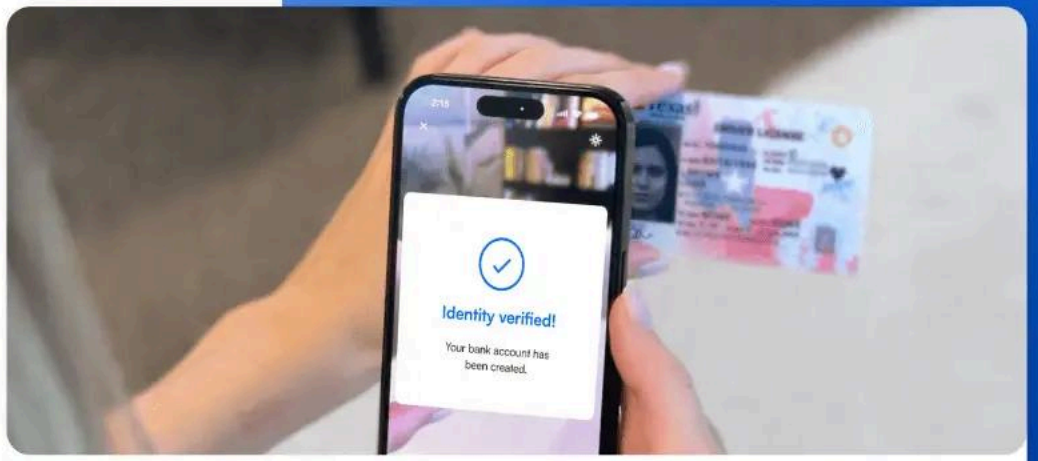
Investing in modular, API-first compliance architecture that can flex across jurisdictions and technologies.

Embedding explainability and auditability into every AI-powered process.

Proactively engaging regulators and standard bodies to shape evolving frameworks rather than waiting for mandates. This means regularly monitoring newsletters, industry associations, and regulators' guidance to anticipate changes. Events like Compliance Week, SCCE, ICA, BAI, or sector-specific compliance forums are invaluable. Associations like the International Compliance Association or Online Compliance Consortium offer peer networks, webinars, and tools to keep you informed and visible. Finally, identify someone responsible for regulator-facing communications, which ensures messages are consistent and timely.

Many companies dealing with legacy tech infrastructure may still run into issues. As the Bank CIO we interviewed put it, “U.S. banking technology is old, much of it was built 25 or 30 years ago. Most institutions can’t keep up with the investment needed to modernize. The majority of banks simply can’t execute at the pace regulators and customers expect.”

Firms face increasing pressure to modernize their tech infrastructure to meet evolving customer expectations, regulatory demands, and competitive pressures. However, large-scale core system replacements are often costly, risky, and time-consuming. Instead, many organizations are exploring solutions that enhance existing systems with modular, API-driven technologies, allowing them to innovate at speed without disrupting day-to-day operations.



How Microblink Can Help

Microblink’s identity verification and fraud solutions are designed to integrate seamlessly into your existing tech stack — no costly core system replacement required.

Our AI-powered document and card scanning technology delivers real-time verification, enhances fraud prevention, and optimizes user onboarding workflows, all while working alongside your legacy infrastructure. It’s innovation without disruption.