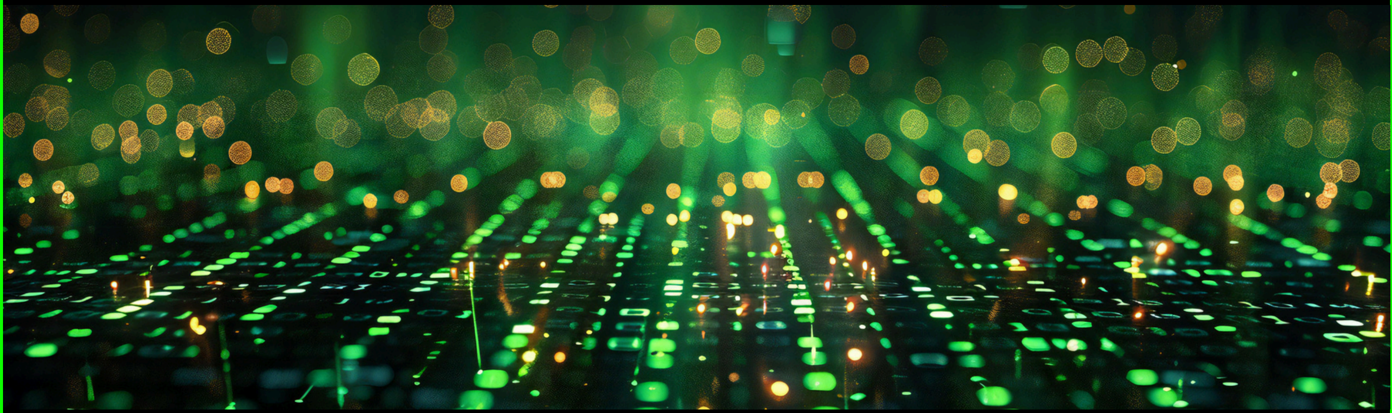
08 September 2026



Welcome to Scale Compliance's

NEWSLETTER

Regulatory Transitions Are Becoming a New Financial Crime Frontier

Recent fraud cases point to a broader trend: every major regulatory transition, from MiCA implementation to license withdrawals, legal entity migrations, wallet and custody changes, and KYC remediation, creates windows in which customers become more vulnerable to deception. What was once seen as purely operational or compliance-driven change is increasingly becoming a direct financial crime risk.

💡 What it Means for Compliance

Fraud prevention, cybersecurity, customer communications, AML, and compliance can no longer operate in silos. Regulatory transitions such as license revocations, wallet and custody migrations, or changes to stablecoin and exchange access create real financial crime exposure, not just operational disruption.

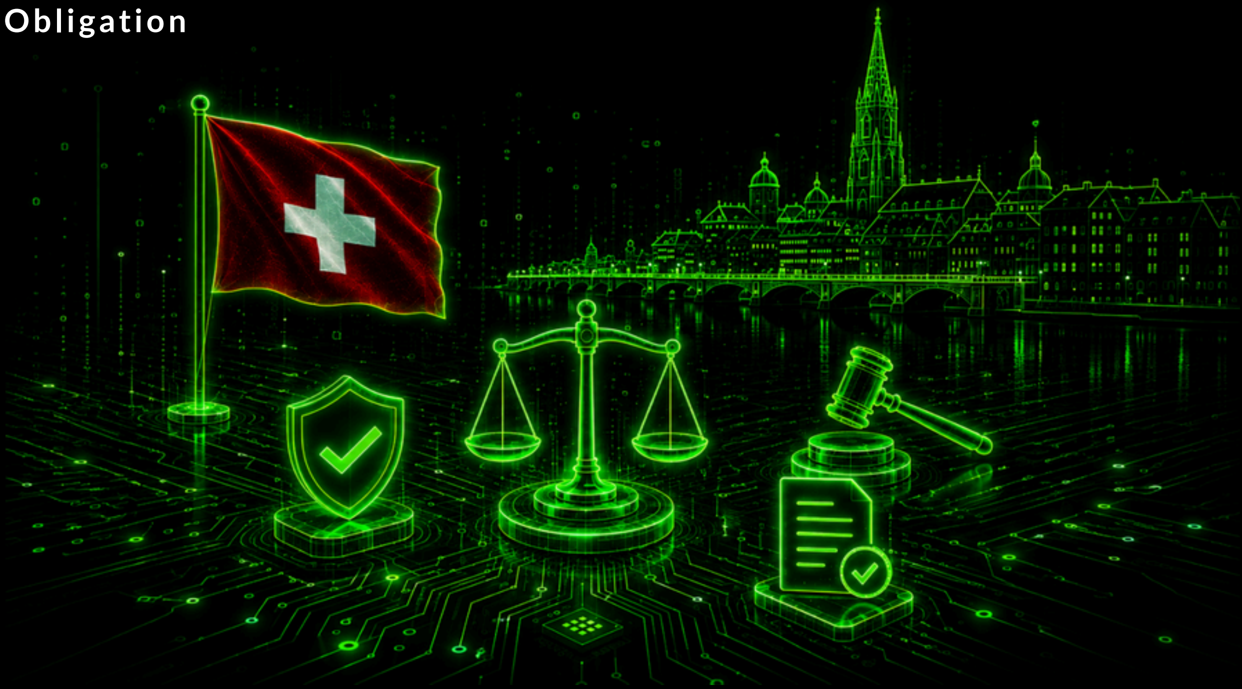
🔍 Scale Insight

This reflects a wider shift: the traditional line between "customer fraud" and "financial crime risk" is blurring. Regulatory change itself is becoming a distinct risk category, one that requires coordinated, cross-functional governance rather than siloed handling by individual teams.

🧭 Actionable Takeaway

Map upcoming regulatory transitions in your organisation, licence changes, entity migrations, KYC remediation campaigns, and identify where fraud, cybersecurity, and financial crime teams need closer coordination. Build cross-functional response protocols before a transition happens, not during it.

Swiss Court Draws the Line Between Sanctions Exposure and Legal Obligation



Months after the Swiss Federal Supreme Court's PostFinance decision, one distinction remains particularly relevant for financial institutions: legal sanctions obligations and institutional risk appetite are not the same thing. The case involved a customer subject to US and UK sanctions but not Swiss sanctions, and the Court confirmed that foreign sanctions alone did not provide sufficient legal basis to deny basic domestic payment services.

💡 What it Means for Compliance

Foreign sanctions exposure does not automatically create a Swiss legal prohibition, and heightened compliance risk is not the same as a legal obligation to exit a relationship. Compliance teams need to clearly separate legal prohibition, sanctions exposure, and internal risk appetite, and support risk-based decisions with case-specific assessments rather than general references to reputational risk.

🔍 Scale Insight

As sanctions regimes become increasingly complex and fragmented across jurisdictions, blurring these distinctions creates real legal and reputational risk. The ruling does not limit the general risk appetite of Swiss institutions, PostFinance operates under a specific statutory mandate, but it reinforces that de-risking decisions must be documented and defensible on their own merits.

🧭 Actionable Takeaway

Review your sanctions and de-risking frameworks to ensure they clearly distinguish between legal prohibition, sanctions exposure, and risk appetite. Document case-specific assessments for relationships involving foreign sanctions exposure, rather than relying on general risk language alone.

OFAC's Sector-Level Sanctions Push Redefines Digital Asset Compliance

The US Treasury has materially expanded the sanctions perimeter for digital assets. Effective 24 August 2026, Iran's digital asset sector was explicitly identified as sanctionable under Executive Order 13902. As part of Operation Economic Outcast, OFAC designated nearly 60 Iran-linked entities, individuals and vessels, and issued five sectoral sanctions determinations covering digital assets, technology, gold, aviation and shipping.

💡 What it Means for Compliance

Sanctions risk is no longer limited to specifically designated entities or wallet addresses, a counterparty's activities and connections to Iran's digital asset sector must also be considered. Institutions processing significant transactions for Iranian exchanges or digital asset businesses may face secondary sanctions exposure, including potential restrictions on access to the US financial system, even without a separate designation.

🔍 Scale Insight

Wallet screening alone is no longer sufficient. OFAC listed 30 Bitcoin, Ethereum and TRON addresses linked to Iran's Mabna Institute, which reportedly received around USD 16.8 million with activity dating back to 2018. This shows that sanctions compliance must extend beyond direct list matches to historical exposure, indirect transaction paths and wider network activity.

🧭 **Actionable Takeaway**

Review whether your sanctions framework is still primarily list-based, or whether it also captures sector-level and network exposure. For exchanges, payment providers and financial institutions, build monitoring that traces counterparty relationships and transaction networks, not just direct designations.

📌Takeaway

Across today's regulatory developments, one theme stands out: governance is becoming the foundation of institutional trust. Whether the topic is AML enforcement, sanctions, licensing, or regulatory transitions, supervisors increasingly expect firms to demonstrate documented, defensible decision-making rather than policies on paper.

For financial institutions and digital asset firms, the priorities are clear:

- Build governance frameworks that clearly separate legal obligations, risk exposure, and internal risk appetite
- Break down silos between fraud, cybersecurity, AML, and compliance teams, especially during regulatory transitions
- Treat regulatory positioning and licensing as a driver of market access, not just a compliance checkbox

Scale
Compliance

Our mailing address is:
info@scalecompliance.com
www.scalecompliance.com