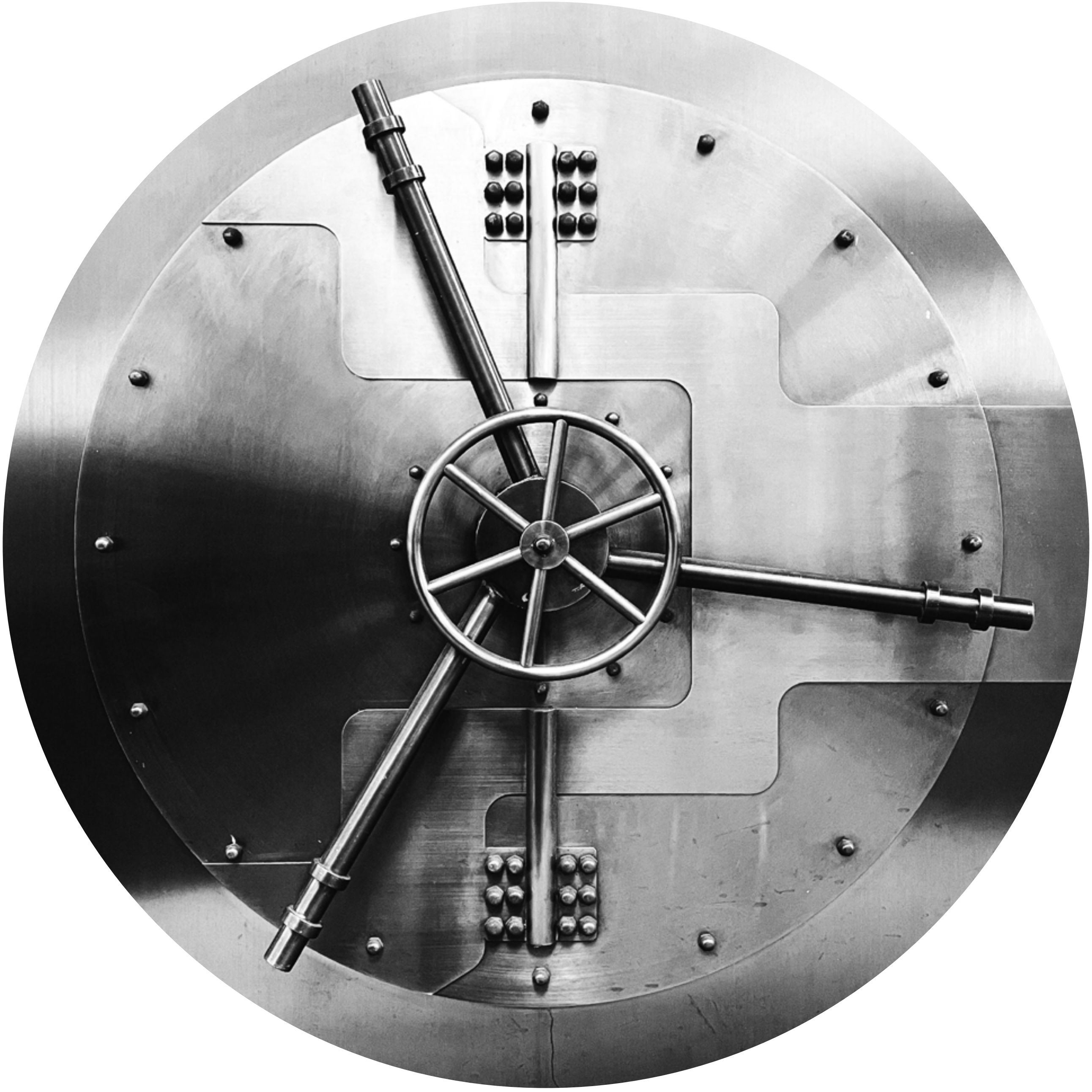
Regulatory frameworks enter the supervisory phase

Q2 2026 Crypto AML/CFT Regulatory Update

Author:
Andreas Katelari
Senior Compliance Officer

Cense AG | The Crypto Compliance Report
Q2 | Apr–Jun 2026

Cense



Executive Summary

During Q2 2026, global crypto regulation entered a new phase as jurisdictions increasingly shifted their focus from policy development to supervisory implementation and enforcement.

The European Union entered the enforcement phase of the Markets in Crypto-Assets Regulation (MiCA), while the United Kingdom advanced its cryptoasset regulatory framework through the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, signalling a move beyond AML registration towards a comprehensive financial services regulatory regime. Switzerland strengthened its AML/CFT regime through reforms to beneficial ownership transparency and supervisory expectations ahead of its forthcoming FATF Mutual Evaluation, while the United States focused on payment stablecoin AML obligations and continued enforcement against crypto-enabled financial crime.

At the international level, the Financial Action Task Force (FATF) reinforced expectations regarding the effective implementation of AML/CFT standards for virtual assets, including the supervision of Virtual Asset Service Providers (VASPs), the Travel Rule and risks associated with stablecoins and unhosted wallets.

Collectively, these developments reflect a clear global trend: regulators are moving beyond establishing crypto regulatory frameworks towards supervising implementation, strengthening enforcement and aligning digital asset regulation with broader financial crime, prudential and conduct standards.

This quarterly update summarises significant re gulatory, legislative and supervisory developments affecting cryptoasset businesses and financial institutions between 1 April and 30 June 2026. It is intended to support compliance professionals in understanding emerging regulatory expectations and assessing their potential impact on AML/CFT and broader financial crime compliance programmes.

European Union

MiCA transition period ends: focus shifts to enforcement

On 1 July 2026, the final MiCA transitional periods applicable across Member States ended, marking the start of full supervisory enforcement across the European Union. With the expiry of the grandfathering arrangements for existing Crypto-Asset Service Providers (CASPs), firms providing regulated crypto-asset services are now expected to operate under a MiCA authorisation or cease activities where no authorisation has been obtained.

Ahead of the deadline, the European Securities and Markets Authority (ESMA) issued supervisory statements[1, 2] reminding National Competent Authorities (NCAs) that unauthorised CASPs should implement an orderly wind-down of their activities. During this period, firms should only undertake actions necessary to protect existing customers, including facilitating the sale, transfer or withdrawal of crypto-assets.

1 European Securities and Markets Authority (ESMA). (2026, April 17). Statement on the end of transitional periods under MiCA (ESMA75-113276571-1679). https://www.esma.europa.eu/sites/default/files/2026-04/ESMA75-113276571-1679_Statement_on_the_end_of_transitional_periods_under_MiCA.pdf

2 European Securities and Markets Authority (ESMA). (2026, June 23). Public statement on the end of the MiCA transitional period and wind-down of unauthorised crypto-asset service providers (CASPs). https://www.esma.europa.eu/sites/default/files/2026-06/ESMA75-113276571-1710_Public_Statement_MiCA_transitional_period_ends.pdf

ESMA also confirmed that authorised CASPs onboarding customers from exiting providers are expected to apply robust Customer Due Diligence (CDD), sanctions screening and AML/CFT controls. In the same statement, ESMA reinforced that the Article 61 reverse solicitation exemption must not be used to circumvent the MiCA licensing regime, reiterating that it only applies where a customer initiates the relationship entirely on their own exclusive initiative.

To support supervisory convergence and market transparency, ESMA continues to maintain and update its MiCA Register, with the latest update published on 3 July 2026. The register provides a centralised source for verifying authorised CASPs, notified crypto-asset white papers, significant Asset-Referenced Tokens (ARTs), Electronic Money Tokens (EMTs), and a dedicated register of Non-Compliant Crypto-Asset Service Providers (NCASPs). As supervisory activity increases, the register is becoming an essential due diligence tool for financial institutions, payment service providers and crypto firms when assessing the regulatory status of counterparties.

The end of the transition period is already reshaping the European crypto market. Several providers have announced service restrictions, customer migrations or market exits where MiCA authorisation has not been obtained. One notable example is Dutch crypto platform Knaken, where prosecutors applied to the Rotterdam court to declare the firm bankrupt after the company ceased operations in June 2026[3]. The case follows regulatory concerns raised by the Dutch Authority for the Financial Markets and highlights the operational and commercial challenges faced by firms unable to transition to the new MiCA licensing framework.

While supervisory authorities are now focused on enforcing the existing framework, policymakers are already considering its future evolution. On 20 May 2026, the European Commission launched a targeted public consultation to evaluate the operation of MiCA and identify areas where the framework may require further refinement[4]. The consultation covers emerging sectors that currently fall outside, or are only partially within, MiCA's scope, including decentralised finance (DeFi), staking, crypto lending and borrowing, non-fungible tokens (NFTs), and the interaction between MiCA and wider EU financial services legislation.

3 DutchNews.nl. (2026, June 30). Prosecutors request bankruptcy for Dutch crypto firm Knaken. https://www.dutchnews.nl/2026/06/prosecutors-request-bankruptcy-for-dutch-crypto-firm-knaken/

4 European Commission. (2026, May 20). Targeted consultation on the review of the Markets in Crypto-Assets (MiCA) Regulation. Directorate-General for Financial Stability, Financial Services and Capital Markets Union. https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en

The conclusion of the MiCA transitional period represents a significant shift in the EU regulatory landscape. Regulatory expectations are moving beyond implementation towards active supervision, with greater emphasis on licensing, governance, market integrity and the effective management of AML/CFT risks. At the same time, the European Commission's consultation demonstrates that MiCA is intended to evolve alongside the crypto market, with further legislative developments expected as new business models emerge.

Key compliance considerations

- Integrate the ESMA MiCA Register and the Register of Non-Compliant Crypto-Asset Service Providers (NCASPs) into third-party risk management processes to support the verification of counterparties and ongoing monitoring of their regulatory status
- Reassess exposure to crypto exchanges, custodians and virtual asset service providers that have not obtained MiCA authorisation, particularly where services are provided on a cross-border basis or through non-EU entities
- Strengthen onboarding controls for customers migrating from exiting CASPs by applying enhanced Customer Due Diligence (CDD), sanctions screening and AML/CFT measures in line with ESMA's supervisory expectations
- Establish monitoring mechanisms to track market exits, customer migrations and exchange restructurings, identifying potential operational, regulatory and financial crime risks affecting customers and counterparties
- Evaluate strategic exposure to emerging crypto activities such as DeFi, staking, crypto lending and NFTs, taking into account the potential for future regulatory developments following the European Commission's ongoing review of the MiCA framework.

Switzerland

AML/CFT Framework strengthened ahead of FATF Mutual Evaluation

Switzerland continued to strengthen its anti-money laundering and counter-terrorist financing (AML/CFT) framework during Q2 2026 through a series of legislative and regulatory reforms aimed at enhancing beneficial ownership transparency, strengthening supervisory expectations and aligning the country's framework with international standards. The developments come ahead of Switzerland's 5th FATF Mutual Evaluation, scheduled for 2026–2027, and demonstrate the country's continued commitment to addressing recommendations arising from previous FATF assessments[5].

On 12 May 2026, the Swiss Financial Market Supervisory Authority (FINMA) launched a consultation on the partial revision of the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA)[6]. The proposed amendments are intended to align the ordinance with recent revisions to the Anti-Money Laundering Act (AMLA), implement outstanding FATF recommendations and incorporate FINMA's existing supervisory practice into binding regulation. The consultation closed on 9 June 2026.

The AMLO-FINMA applies exclusively to FINMA-supervised financial intermediaries, including banks, securities firms, asset managers and crypto-asset businesses that fall within FINMA's supervisory remit. The proposed revisions strengthen requirements relating to customer ownership and control structures, introduce more explicit organisational measures to prevent sanctions breaches and enhance transparency requirements for certain account structures. For FINMA-supervised crypto firms, the consultation reinforces expectations that governance, customer due diligence, sanctions screening and transaction monitoring frameworks will remain aligned with evolving supervisory standards.

5 State Secretariat for International Finance (SIF) – Financial Action Task Force (FATF): https://www.sif.admin.ch/en/financial-action-task-force-2

6 FINMA – Consultation on the Partial Revision of the Anti-Money Laundering Ordinance (AMLO-FINMA) (12 May 2026): https://www.finma.ch/en/news/2026/05/20260512-mm-anh-gwv-finma/

Separately, on 12 June 2026, the Swiss Federal Council confirmed that the revised Anti-Money Laundering Act (AMLA) and the new Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA) will come into force on 1 October 2026[7]. A key element of the reform is the establishment of a federal beneficial ownership register, providing competent authorities with improved access to reliable information on the individuals who ultimately own or control Swiss legal entities.

Unlike the AMLO-FINMA revisions, the legislative reforms extend beyond the traditional financial sector. The revised AMLA expands AML obligations to certain advisory activities, including aspects of company formation, legal entity structuring and selected real estate transactions, bringing specified activities undertaken by lawyers, notaries, fiduciaries and other professional advisers within the scope of the AML framework. The reforms have generated considerable discussion within the legal and professional services sectors and represent one of the most significant changes to Switzerland's AML regime in recent years.

---

7 Swiss Federal Department of Finance – Revised Anti-Money Laundering Act (AMLA) and Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA): https://www.sif.admin.ch/en/anti-money-laundering-act-amla

For crypto firms, these developments reinforce Switzerland's continued commitment to strengthening financial integrity while maintaining its position as a leading digital asset jurisdiction. Enhanced beneficial ownership transparency, stronger governance expectations and closer alignment with FATF standards are expected to improve customer due diligence, legal entity verification and the detection of complex ownership structures associated with financial crime risk.

Key compliance considerations

- Review AML/CFT policies and procedures against the proposed AMLO-FINMA revisions, with particular focus on beneficial ownership, ownership and control structures, sanctions governance and documentation standards
- Update legal entity onboarding and customer due diligence processes to prepare for the introduction of Switzerland's federal beneficial ownership register
- Assess whether existing customer risk assessments, enhanced due diligence measures and transaction monitoring controls adequately address complex ownership structures and higher-risk crypto-related activities
- Strengthen governance arrangements for sanctions compliance, including screening controls, escalation procedures and evidence supporting ongoing effectiveness
- Monitor the finalisation of the AMLO-FINMA revisions and the implementation of the revised AMLA and LETA ahead of their entry into force
- Consider the potential impact of Switzerland's forthcoming FATF Mutual Evaluation on future supervisory expectations and the continued enhancement of AML/CFT compliance frameworks.

United Kingdom

Cryptoasset regime moves beyond AML registration towards full FCA authorisation

The United Kingdom continued to advance its comprehensive cryptoasset regulatory framework during Q2 2026, marking a significant shift from the existing anti-money laundering registration model towards a broader financial services authorisation regime.

On 21 April 2026, HM Treasury published a policy note and draft statutory provisions amending the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026[8, 9]. The amendments refine the UK's incoming cryptoasset framework and ensure that the regime operates effectively alongside wider payments legislation, including the treatment of qualifying stablecoins and tokenised payment arrangements.

Although the UK's Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 are not a direct replica of MiCA, the two frameworks are broadly aligned in seeking to establish comprehensive authorisation, prudential, conduct and financial crime requirements for cryptoasset businesses. The principal distinction lies in the UK's decision to integrate cryptoasset regulation into the existing Financial Services and Markets Act (FSMA) framework, applying many of the same regulatory principles that govern traditional financial services. The UK also adopts a different approach to stablecoins, regulating qualifying payment stablecoins within the wider payments and electronic money framework, whereas MiCA establishes a dedicated regime for EMTs and ARTs. In addition, the UK framework extends more broadly to activities such as crypto lending, staking and certain decentralised finance (DeFi) business models, reflecting an activity-based approach that may capture service providers facilitating these activities, whereas MiCA currently excludes genuinely decentralised services from its scope and does not establish a comprehensive regulatory regime for crypto lending or staking. These differences demonstrate the UK's intention to integrate cryptoassets into its established financial services framework while maintaining regulatory flexibility to address emerging business models and evolving financial crime risks.

8 HM Treasury – Policy Note: Draft statutory instrument amending the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (21 April 2026): https://www.gov.uk/government/publications/policy-note-draft-statutory-instrument-amending-the-cryptoasset-regulations

9 UK Legislation – The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026: https://www.legislation.gov.uk/uksi/2026/102/contAlthoughents/made

The UK regime is designed to bring a broad range of cryptoasset activities within the Financial Conduct Authority's regulatory perimeter, including cryptoasset trading platforms, intermediation, custody, staking and certain stablecoin-related activities. This represents a material expansion of the FCA's role, moving beyond the existing Money Laundering Regulations and financial promotions framework towards prudential, conduct, governance and market integrity supervision.

On 30 June 2026, the FCA published final rules and guidance for firms that will be authorised under the new FSMA cryptoasset regime from 25 October 2027[10], including its formal Policy Statement on the cryptoasset regime. The FCA confirmed that authorised cryptoasset firms will be subject to standards including the Principles for Businesses, Consumer Duty and the Senior Managers and Certification Regime, reinforcing the UK's intention to regulate cryptoasset firms in a manner closer to traditional financial services.

For crypto compliance teams, the UK developments are important because they change the regulatory baseline. Firms will no longer be assessed primarily through an AML registration lens; they will need to demonstrate broader governance, operational resilience, consumer protection, systems and controls, market abuse and financial crime capability. Existing crypto firms serving UK customers should therefore treat the transition period as an implementation window rather than a policy consultation phase.

10 FCA – Policy Statement: Cryptoasset regime (30 June 2026): https://www.fca.org.uk/publications/policy-statements/, including stablecoin regulation, illicit finance risks,cryptoasset-regime

Key compliance considerations

- → Assess whether current UK-facing cryptoasset activities fall within the new regulated activities perimeter, including trading, intermediation, custody, staking and stablecoin-related services
- → Prepare for FCA authorisation under FSMA by reviewing governance arrangements, senior management accountability, prudential readiness, operational resilience and conduct risk frameworks
- → Map existing AML/CFT controls against the broader requirements expected under the incoming FCA regime, including customer protection, conflicts management, complaints handling and market integrity controls
- → Review UK stablecoin and payment-token business models in light of HM Treasury's April 2026 amendments and the interaction between cryptoasset regulation and payments legislation
- → Develop an implementation roadmap ahead of the 25 October 2027 commencement date, including regulatory permissions, policies, systems, controls and senior manager responsibilities.

United States

Stablecoin AML rules and crypto enforcement remain key regulatory priorities

The United States continued to strengthen its regulatory and enforcement framework for digital assets on stablecoin regulation, illicit finance risks and crypto-related enforcement during Q2 2026. While broader market structure reform remains an ongoing policy issue, the quarter was marked by concrete action on payment stablecoin AML/CFT obligations and continued enforcement against crypto-enabled money laundering and fraud.

On 8 April 2026, the U.S. Treasury Department and FinCEN issued a proposed rule to implement the GENIUS Act's anti-money laundering and sanctions compliance requirements for Permitted Payment Stablecoin Issuers (PPSIs)[11, 12]. The proposed rule would treat PPSIs as financial institutions under the Bank Secrecy Act and subject them to obligations relating to AML programmes, sanctions compliance, customer identification, due diligence, suspicious activity monitoring and recordkeeping.

11 FinCEN – Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements (8 April 2026): https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism

12 FinCEN – Fact Sheet: Proposed Rule to Implement the GENIUS Act's Anti-Money Laundering and Sanctions Requirements: https://www.fincen.gov/system/files/2026-04/FactSheefinancial-crime controls, particularly where stablecoins are used for payments, cross-border transfers, or settlement activitiest-PPSI-program-NPRM.pdf

The proposed rule is significant because it brings payment stablecoin issuers more clearly into the U.S. financial crime compliance framework. It also reflects the growing expectation that stablecoin issuers should maintain bank-like financial crime controls, particularly where stablecoins are used for payments, cross-border transfers or settlement activity. For crypto firms and financial institutions interacting with stablecoins, this increases the importance of issuer due diligence, reserve transparency, sanctions controls and transaction monitoring.

Enforcement activity also remained active throughout Q2. In April 2026, the Department of Justice announced major actions targeting Southeast Asian scam centres involved in cryptocurrency investment fraud, including the seizure of more than $700 million in cryptocurrency allegedly laundered from stolen funds[13]. On 11 June 2026, U.S. prosecutors charged two individuals in connection with a cryptocurrency money laundering service that allegedly laundered more than $389 million in unlawful transactions. [14]

These cases demonstrate that, even as U.S. policymakers move towards clearer regulatory frameworks for digital assets, enforcement agencies remain focused on crypto-enabled fraud, laundering networks, sanctions exposure and illicit financial infrastructure. The practical direction for compliance teams is clear: stablecoin governance, blockchain analytics, scam typologies, sanctions screening and counterparty risk management remain central to U.S. crypto compliance.

Key compliance considerations

- → Review exposure to payment stablecoins and assess whether issuers have credible AML/CFT, sanctions, customer identification and suspicious activity monitoring frameworks
- → Update stablecoin counterparty due diligence to include issuer status, reserve structure, sanctions controls, redemption arrangements and Bank Secrecy Act readiness
- → Strengthen blockchain analytics coverage for cross-chain movement, high-risk counterparties, obfuscation services and exposure to sanctioned or illicit finance networks
- → Review escalation procedures for suspected scam proceeds, suspicious activity reporting, law enforcement requests and asset-freezing obligations
- → Monitor finalisation of the FinCEN stablecoin AML/CFT rule and assess implementation impacts for issuers, exchanges, custodians and financial institutions supporting stablecoin activity.

13 DOJ – Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting U.S. Victims (April 2026): https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting

14 DOJ – Two Charged in Connection With Cryptocurrency Money Laundering Service That Allegedly Laundered Over $389 Million in Unlawful Transactions (11 June 2026): https://www.justice.gov/usao-edpa/pr/two-charged-connection-cryptocurrency-money-laundering-service-allegedly-laundered

International standards

FATF reinforces AML/CFT expectations for virtual assets

During its June 2026 Plenary[15], the Financial Action Task Force (FATF) reaffirmed the importance of the effective implementation of its Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) standards, including those applicable to virtual assets and Virtual Asset Service Providers (VASPs). FATF emphasised that jurisdictions should continue strengthening supervisory effectiveness, improving implementation of the FATF Recommendations and addressing emerging financial crime risks associated with digital assets.

Although the Plenary did not introduce new virtual asset-specific standards, it reinforced the direction established through FATF's previous work on virtual assets, including its March 2026 Targeted Report on Stablecoins and Unhosted Wallets[16]. That report highlighted the increasing use of stablecoins in cross-border payments and the growing exploitation of stablecoins by criminal networks involved in fraud, ransomware, sanctions evasion and money laundering. It also identified peer-to-peer (P2P) transfers and unhosted wallets as presenting heightened financial crime risks where transactions occur outside regulated Virtual Asset Service Providers (VASPs) or where Customer Due Diligence (CDD), Travel Rule compliance and transaction monitoring controls are ineffective.

15 Financial Action Task Force (FATF): Outcomes of the FATF Plenary, June 2026: https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2026.html

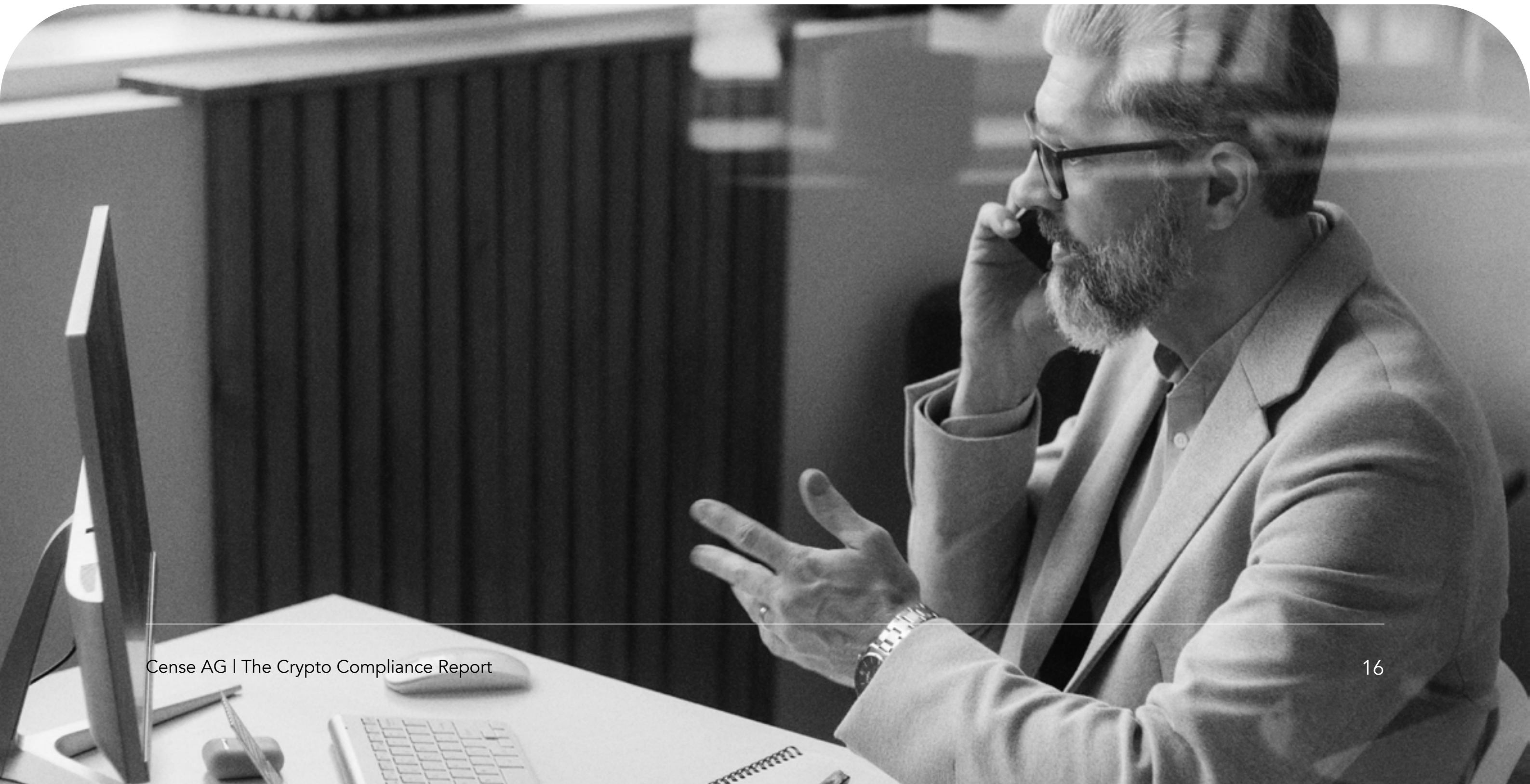
16 Financial Action Task Force (FATF): Targeted Report on Stablecoins and Unhosted Wallets (March 2026): https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

For regulators and financial institutions, these publications collectively reinforce that effective implementation – not simply the existence – of AML/CFT frameworks is becoming the primary supervisory expectation. This direction is reflected across several of the developments covered in this quarterly update, including the European Union's transition to full MiCA supervision, Switzerland's AML/CFT reforms ahead of its FATF Mutual Evaluation, the United Kingdom's move to a comprehensive cryptoasset authorisation regime and the United States' strengthening of AML requirements for payment stablecoin issuers.

The FATF's continued focus demonstrates that international supervisory expectations are increasingly centred on governance, customer due diligence, sanctions compliance, Travel Rule implementation, blockchain analytics and the effective management of cross-border virtual asset risks.

Key compliance considerations

- Review AML/CFT frameworks to ensure continued alignment with the FATF Recommendations relating to virtual assets, Virtual Asset Service Providers (VASPs) and the Travel Rule
- Assess transaction monitoring controls for stablecoin activity, peer-to-peer transfers and unhosted wallets, ensuring higher-risk scenarios are appropriately identified, investigated and escalated
- Strengthen blockchain analytics and sanctions screening capabilities to detect typologies involving fraud, ransomware, sanctions evasion and other forms of crypto-enabled illicit finance
- Review customer and counterparty risk assessment methodologies to ensure they adequately consider jurisdictional risk, VASP licensing status and exposure to higher-risk virtual asset ecosystems
- Continue monitoring FATF Plenary outcomes, Mutual Evaluation Reports and jurisdictional implementation of the FATF Recommendations to identify emerging supervisory expectations and incorporate them into AML/CFT governance and financial crime risk assessments.



Looking ahead

Key regulatory themes for Q3 2026

As regulatory frameworks mature, compliance teams should expect supervisory authorities to increasingly focus on implementation rather than policy development. Firms should anticipate heightened regulatory scrutiny of governance arrangements, customer due diligence, sanctions compliance, Travel Rule implementation and the management of crypto-related financial crime risks.

Several themes are expected to shape the regulatory landscape during Q3 2026:

- **MiCA enforcement:** National Competent Authorities are expected to increase supervisory engagement with authorised Crypto-Asset Service Providers (CASPs), while continuing to oversee the orderly wind-down of unauthorised firms and monitoring reliance on the reverse solicitation exemption
- **Stablecoin regulation:** Stablecoins are expected to remain a key supervisory priority as jurisdictions continue refining licensing frameworks and AML/CFT expectations for issuers and service providers
- **Travel Rule and cross-border supervision:** Regulators are likely to place greater emphasis on the effective implementation of the FATF Travel Rule, cross-border information sharing and the supervision of Virtual Asset Service Providers (VASPs) operating across multiple jurisdictions
- **Emerging crypto activities:** Policymakers will continue assessing regulatory approaches to decentralised finance (DeFi), staking, crypto lending, tokenisation and other evolving digital asset business models as the market continues to mature.

Strategic priorities for compliance functions

Financial institutions and crypto firms should use the coming quarter to:

- → Review crypto counterparty due diligence frameworks, including verification of licensing and regulatory status across all relevant jurisdictions
- → Reassess customer risk assessment methodologies to reflect evolving supervisory expectations relating to stablecoins, cross-border activity and emerging financial crime typologies
- → Strengthen governance, documentation and evidence supporting AML/CFT, sanctions compliance and Travel Rule implementation
- → Monitor consultations, supervisory statements and legislative developments that may affect future regulatory obligations, particularly in relation to MiCA, the UK FSMA regime and Switzerland's AML reforms
- → Continue investing in blockchain analytics, transaction monitoring and financial crime controls to ensure compliance frameworks remain proportionate to the evolving risk environment.

Cense AG
Registered:
Commercial Register:
Canton Zug, Switzerland
Reg. Number:
CHE-334.198.597
Address:
Neuhofstrasse 22,
6340 Baar, Switzerland
Tel.:
+41 793450689
Email:
contact@cense.com

Start a conversation with cense

Transform your approach to compliant crypto onboarding at speed and scale.

Contact us now