



Regulatory frameworks enter the supervisory phase

Q3 2026 Crypto AML/CFT Regulatory Update

Author:

Andreas Katelari
Senior Compliance Officer

Cense AG | The Crypto Compliance Report
Q3 | Jul–Sep 2026





Executive Summary

In the EU, the MiCA transitional period ended on 1 July 2026, triggering AMLA guidance on the money-laundering risks of customer migration between authorised and unauthorised providers. The Council's 21st Russia sanctions package extended the crypto platform transaction ban, introduced a third-country restriction tool, and widened ownership and governance restrictions on Russian nationals in EU crypto businesses. AMLA continued technical-standards work under the AML Regulation, and ESMA's September risk report highlighted roughly USD 1 billion in H1 2026 hack losses and growing links between crypto and traditional finance.

In Switzerland, the revised AMLA and the new beneficial-ownership transparency law (LETA) enter into force on 1 October 2026, alongside FINMA supervisory findings on AML weaknesses, a country-risk communication reflecting June FATF listings, and sanctions notices under the Iran and ISIL/Al-Qaida regimes.

In the US, OFAC issued two further Iran-related digital-asset designations (7 August and 17 September), FinCEN proposed correspondent-banking restrictions on a UAE bank, GENIUS Act implementation proposals advanced, and the CLARITY Act market-structure bill failed a Senate cloture vote on 15 September, leaving its AML provisions at the proposal stage.

In the UK, the FCA's PS26/18 opened the cryptoasset authorisation gateway (from 30 September 2026) and further joint operations targeted unregistered peer-to-peer trading. Internationally, FATF reported continuing Travel Rule implementation gaps and persistent centralisation risk in DeFi arrangements presented as decentralised. Meanwhile, Australia's Travel Rule obligations took effect on 1 July.



European Union

MiCA transitional period ends, with AML risks around customer migration

The maximum transitional period under the Markets in Crypto-Assets Regulation (MiCA) expired on 1 July 2026. From that date, firms must hold a MiCA authorisation to keep providing crypto-asset services in the EU¹. Some Member States had already ended their transitional arrangements earlier, and ESMA's 17 April 2026 statement identifies categories of firms that could not rely on the transitional regime even before 1 July². The April statement keeps its original date. ESMA's 23 June public statement built its expectations of orderly wind-downs on it. That statement also expects an onboarding CASP that receives clients from an unauthorised provider to carry out all necessary AML/CFT checks, and it reminds non-EU CASPs that they cannot provide MiCA services to, or solicit, EU clients, including on a business-to-business basis³.

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: ESMA calls on unauthorised crypto-asset service providers to wind down orderly, while also safeguarding clients' interests, as MiCA transitional period ends (ESMA75-113276571-1710). https://www.esma.europa.eu/sites/default/files/2026-06/ESMA75-113276571-1710_Public_Statement_MiCA_transitional_period_ends.pdf

³ Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). (2026, June 29). Advisory note: ML/TF risks resulting from the end of the MiCAR transitional period and possible mitigating measures. https://www.aml.europa.eu/document/download/d82f7d00-324e-4231-8ca7-94431d4e75c2_en



Just before the deadline, on 29 June, the EU Anti-Money Laundering Authority (AMLA) issued an advisory note on the money laundering and terrorist financing risks arising from the expiry. Firms' duties continue to derive from existing AML/CFT law and MiCA. It sets out risks and mitigating measures for four groups:

- Unauthorised providers: compressed exit timelines may weaken AML/CFT frameworks, and abrupt exits may reduce transparency over asset flows. This creates opportunities for concealment, rapid movement of illicit funds and sanctions evasion. Firms are expected to run wind-downs in a structured and documented way, keep adequate AML/CFT governance and resources, and keep Customer Due Diligence (CDD) information up to date until regulated activities have ceased. They must also continue to identify and report suspicious activity.
- Authorised CASPs: rapid customer inflows may change risk exposure, including a concentration of higher-risk customers, and may strain transaction monitoring capacity. The note asks CASPs to check that their systems and staffing can handle increased volumes. It also asks them to integrate incoming customer risk information properly.
- AML/CFT supervisors: the note identifies blind spots over customer transfers and risk migration, and inconsistent supervisory approaches across Member States. It asks supervisors to prioritise oversight of exit planning and transfers, and to coordinate across borders.
- Financial intelligence units: the reallocation of customer bases may be used to obscure illicit flows, through rapid movement of assets across CASPs or jurisdictions. It may also itself increase reporting volumes.

The note's central message for receiving firms is that customers moving from an unauthorised provider should be assessed individually under a risk-based approach, with enhanced due diligence where higher risks are identified. They should not be subject to blanket de-risking solely on the basis of their former provider.



Key Compliance considerations

- Treat migration as an AML event. Assess each incoming customer individually. Do not reject customers because of their former provider, and do not onboard them on the strength of that provider's records alone. Apply enhanced due diligence when risk indicators are present, and document the reasoning.
- Look through the deposit. A receiving CASP may see only the final transfer, so blockchain analytics should trace the wider path. Assets may have moved through private wallets or several intermediaries before arriving.
- Check capacity before the inflow. Review transaction monitoring scalability, alert-handling backlogs, staffing and customer risk model calibration. Watch for a change in the overall risk profile of the customer base after onboarding.
- Integrate incoming risk information. Decide how data from the exiting provider is validated, how gaps are handled and how it feeds the customer risk score.
- Keep transfer traceability and sanctions controls in place. The Travel Rule and sanctions screening apply to migrations. ESMA's June statement expressly links wind-down to transfer traceability obligations.[3]
- For firms exiting the market: keep CDD current, monitor and file suspicious activity reports until activity has fully ceased, and retain adequate resources and governance during wind-down.
- Verify counterparties. Check regulatory status against the ESMA MiCA register. Confirm that non-EU counterparties are not providing services to EU clients in breach of MiCA, and that reverse solicitation is not being used to get around authorisation.
- Expect more reporting and supervisory attention. FIUs may see a rise in reports linked to migration flows, and supervisors are expected to focus on exit planning and transfers.

Crypto-specific sanctions expand beyond named platforms

On 23 July 2026, the Council adopted the 21st package of restrictive measures against Russia. Its crypto provisions have three parts⁴. The transaction ban was extended to 14 crypto-related service platforms based in Georgia, Panama, the United Arab Emirates, the Marshall Islands, Kyrgyzstan and Belarus.

- **Third-country tool.** The Council introduced a mechanism to prohibit transactions with crypto service providers and exchange or transfer platforms across a listed third country where authorities systematically and persistently fail to prevent sanctions circumvention. Activation requires a country's inclusion in Annex LVII, which contained no entries when the measure was adopted, and remains subject to the specified resident EU-national exception.
- **Ownership and governance.** From 25 August 2026, the prohibition on allowing Russian nationals or individuals residing in Russia to own or control, directly or indirectly, or hold governing-body positions in EU crypto businesses extends beyond wallet, account and custody providers to entities providing other MiCA-defined cryptoasset services. Exemptions remain for EU, EEA and Swiss nationals and holders of temporary or permanent residence permits in those jurisdictions.

⁴ Council of the European Union. (2026, July 23). 21st package of sanctions: EU hits Russian energy, financial services and crypto hard [Press release]. <https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/21st-package-of-sanctions-eu-hits-russian-energy-financial-services-and-crypto-hard/>



Key Compliance considerations

1. Ownership and governance

- a. Review the EU entity's direct and indirect ownership, control and governing bodies, including relevant nationality and residence information. Do not rely solely on AML beneficial-ownership thresholds.
- b. Confirm the rule's application to group structures and notified crypto service providers. Incorporate checks into share transfers, appointments and changes of control.
- c. Document findings and escalate potential breaches or unresolved questions to the board and legal advisers.

2. Customers and counterparties

- a. Re-screen customers, beneficial owners, controllers and service providers against relevant listings, applying the ownership and control tests appropriate to each measure.
- b. Distinguish transaction bans from asset freezes and jurisdiction-based restrictions, including their respective blocking, freezing and reporting requirements.
- c. Review names, aliases, wallets and transaction routes for exposure to listed platforms, taking account of application dates. Assess geographical links individually; a platform's listing does not prohibit an entire jurisdiction.
- d. Process withdrawals or account closures under a derogation only after confirming eligibility, deadlines and any required prior authorisation.



3. Connected parties and transaction flows

- a. Investigate shared ownership, directors, addresses, domains, wallets and recurring counterparties that may connect customers to listed parties, including relevant A7 network links.
- b. Assess indirect exposure through group entities, intermediaries and cross-chain transfers. Treat analytics findings as indicators requiring assessment, rather than automatic evidence of a sanctions breach.

4. Governance and control effectiveness

- a. Assign senior accountability and report material exposures, control gaps and remediation to the board.
- b. Update sanctions procedures to cover ownership restrictions, transaction bans, asset freezes, derogations and future jurisdiction-based measures.
- c. Retain evidence of screening, investigations and decisions. Test controls and train relevant staff to identify and escalate potential breaches.

AMLA continues to build the single rulebook

The AML Regulation (Regulation (EU) 2024/1624)⁵ applies from 10 July 2027, and AMLA's direct supervision of selected groups begins in 2028. During Q3 AMLA continued its work on the technical standards that will operationalise the rules.

- On **8 July 2026**, AMLA published its final report on the regulatory technical standards (RTS) under Article 53(10) of the sixth AML Directive. They set a common method for assessing the gravity of AML/CFT breaches. Supervisors weigh indicators such as duration, repetition and impact, and classify the breach into one of four levels of gravity. The standards apply to financial and non-financial sectors alike. Once adopted by the Commission, they will be directly applicable and binding.
- AMLA's draft RTS on group-wide requirements and third-country branches and subsidiaries (Articles 16(4) and 17(3) of the AML Regulation) are due to the Commission by 30 September 2026.

These are draft standards awaiting Commission adoption, not current obligations. They nevertheless show how supervisors will expect firms to demonstrate proportionality, and how they will assess breaches after 2027.

⁵ Authority for Anti-Money Laundering and Countering the Financing of,,, Terrorism (AMLA). (2026, July 8). Press release: AMLA introduces a common EU approach to enforcing anti-money laundering rules. https://www.amla.europa.eu/press-release-amla-introduces-common-eu-approach-enforcing-anti-money-laundering-rules_en

Key Compliance considerations:

- Track the RTS through Commission adoption. The gravity-assessment methodology and the group-wide/third-country RTS are draft standards submitted to the Commission, not yet binding; monitor for adoption and any amendment before treating either as final.
- Map the gravity criteria against internal escalation. Once adopted, the four-level gravity classification (weighing duration, repetition and impact) will inform how supervisors calibrate enforcement response. Compliance teams should test whether their own breach-severity assessments and internal escalation thresholds would map sensibly onto that scale.
- Prepare for group-wide and third-country branch requirements. Firms with group structures, branches or subsidiaries outside the EU should begin identifying which entities would fall within scope of the Article 16(4)/17(3) standards, and where group AML/CFT policies, information-sharing arrangements and third-country equivalence assessments may need updating ahead of the AML Regulation's 10 July 2027 application date.

ESMA risk monitoring: crypto-asset stress and hack losses

On 10 September ESMA published its Trends, Risks and Vulnerabilities Risk Monitor No. 2, 2026, covering the first half of the year⁶. The report is a market-risk assessment. It is not guidance and creates no AML obligations. However in the relevant report ESMA cites TRM Labs figures showing hack-related losses of around USD 1 billion in the first half of 2026, against USD 2.3 billion a year earlier.

⁶ European Securities and Markets Authority (ESMA). (2026, September 10). TRV Risk Monitor: ESMA Report on Trends, Risks and Vulnerabilities No. 2, 2026 (ESMA50-1949966494-4282). https://www.esma.europa.eu/sites/default/files/2026-09/ESMA50-1949966494-4282_TRV_Risk_Monitor_2_2026.pdf





A small number of large infrastructure compromises, which security analysts often attribute to highly organised, state-linked actors, accounted for most of the losses.

The examples given are the drain of about USD 285 million from Drift Protocol after attackers gained administrative control through a months-long social-engineering operation, and a roughly USD 290 million exploit of KelpDAO through manipulation of cross-chain bridge infrastructure. ESMA also notes that crypto markets are becoming more interlinked with traditional finance. It cites, among other examples, a Belgian bank launching crypto trading services, a bank consortium planning a regulated euro stablecoin, and a Swiss franc stablecoin sandbox run by UBS and other Swiss banks.

Key compliance considerations

- Large hacks and bridge exploits point to laundering of stolen funds through chain-hopping, decentralised exchanges and mixers. Check that monitoring and analytics cover cross-chain movement and rapid conversion to stablecoins.
- Define how the firm identifies funds linked to a publicised exploit, who decides to hold or reject them, and how quickly. State-linked attribution raises sanctions relevance, which is a matter for the firm's own analysis and not something ESMA asserts.
- As banks and other institutions connect to crypto, the AML controls of traditional firms handling crypto flows become more important. Firms on either side of that link should check the effective operation of data flows and escalation between them.
- Social engineering aimed at gaining administrative control was central to one of the large attacks. Include privileged-access controls, third-party dependencies and incident response in the financial crime risk assessment, and make sure incident response includes reporting and freezing steps.

Switzerland

Revised AMLA and LETA

The revised Anti-Money Laundering Act (AMLA) and the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA) enter into force on 1 October 2026. LETA creates a federal transparency register of beneficial owners. The revised AMLA brings certain advisory activities, such as legal-entity structuring and specified real-estate transactions, within the AML framework⁷. Transitional periods for registering existing entities begin on 1 October. The first register notification must be made within one month of the first commercial register amendment on or after that date.

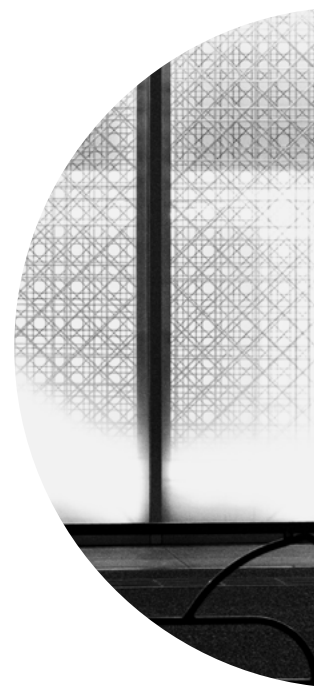
Key Compliance considerations:

1. Revised AMLA

- a. The revision extends AML duties to certain advisory activities, including legal-entity structuring and specified real-estate transactions. Following the consultation, thresholds were introduced to define what counts as professional advisory activity. Advisers in scope must join a self-regulatory organisation, with a short transitional period for existing advisers, but the substantive due diligence duties apply from entry into force.
- b. As reported, the revised AMLA require financial intermediaries to take organisational measures to prevent violations of Embargo Act measures. The Federal Council's message describes them as internal directives and a process or computerised system for screening business relationships and the originators and beneficiaries of transactions against sanctions lists. For crypto firms, this points to evidencing screening of counterparties and Travel Rule data, and not only of customers. FINMA is putting the same requirement into the AMLO-FINMA, whose revision is planned for 1 January 2027 and remains in consultation⁸.
- c. Prepare to show effectiveness. The Federal Council chose the timing so that the measures can be assessed at the next FATF evaluation, scheduled for 2027 to 2028. Compliance Officers should keep evidence that controls work in practice.

⁷ Swiss State Secretariat for International Finance (SIF). (2026, June 12). 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-aml>

⁸ CMS. (2026, May 26). Switzerland revises FINMA Anti-Money Laundering Ordinance: main changes (secondary commentary). <https://cms.law/en/che/legal-updates/Switzerland-revises-FINMA-Anti-Money-Laundering-Ordinance-main-changes>



2. LETA and the transparency register

- a. Own entity. Legal entities must identify their beneficial owners, verify the information, keep it current and report it to the register. The first notification is due within one month of the first commercial register amendment on or after 1 October 2026, and transitional periods depend on legal form.
- b. Definition of beneficial owner. The register covers natural persons who ultimately control an entity, in particular through at least 25% of capital or voting rights or control by other means. Review whether internal thresholds and control tests are aligned. For token issuers, foundations and DAO-type structures, “control by other means” needs a documented analysis.
- c. Using the register for customers. The register is not public. Access is limited to authorities and to financial intermediaries and advisers subject to the AMLA for the purposes of their due diligence duties. Treat it as an additional source. Do not treat it as the only verification, and keep your own identification and verification of owners and controllers. In addition, establish how mismatches between customer information and the register are recorded, escalated and, where suspicion arises, reported to MROS.
- d. Decide which existing legal-entity customers to re-verify first, and record the timetable, since the transitional periods begin on 1 October.

FINMA inspection findings

At its Small Bank Symposium, FINMA presented findings from on-site inspections of banks and securities firms⁹. On anti-money laundering, it reported recurring weaknesses in KYC documentation, particularly for cross-booked relationships, and delays in periodic reviews of business relationships. Some AML alerts fell outside the definition of a high-risk transaction in Article 14 of the FINMA Anti-Money Laundering Ordinance. Some monitoring systems recognised pass-through transactions only where cash was involved, so non-cash pass-through activity went undetected.

FINMA also noted high risk tolerance towards customers with high reputational risk. On crypto, it stated that money laundering risk is high, because cryptocurrencies are often used to pay for cyberattacks, in illegal online trading or to circumvent sanctions. The findings are supervisory observations drawn from banks and securities firms. They are not a new rule applying to crypto providers, but they show where inspections are finding gaps.

Key Compliance considerations

- Test whether periodic reviews are completed on schedule, and record the reasons for any backlog, its size and the remediation plan. FINMA identified delayed reviews as a recurring weakness.
- Check KYC files for cross-booked relationships, meaning customers served through more than one entity, desk or booking centre. Confirm that one file is complete and that all booking entities rely on the same information.
- Check that transaction monitoring recognises pass-through activity in crypto and not only in cash. In practice this means funds or assets that arrive and leave quickly with little economic purpose, across wallets, chains and stablecoins. Include such scenarios in model validation and back-testing.
- Confirm that the firm's own definition of a high-risk transaction captures the alerts it treats as significant. FINMA found alerts that fell outside the definition in Article 14 of the AMLO-FINMA.
- Review the board's risk tolerance for customers with high reputational risk. FINMA noted high tolerance in inspected institutions, and the tolerance should be set, documented and reflected in onboarding decisions.
- Treat FINMA's statement that crypto money laundering risk is high as a prompt to check that the business-wide risk assessment covers cyberattack proceeds, illegal online trading and sanctions circumvention. The findings come from banks and securities firms. They are not a rule for crypto providers, but they show what inspectors are testing.

⁹ Swiss Financial Market Supervisory Authority (FINMA). (2026, September 7). Small Bank Symposium of 7 September 2026 [Speeches and published articles]. <https://www.finma.ch/en/documentation/finma-publications/addresses-and-specialist-articles/kleinbankensymposium-2026/>

Country-risk communication

FINMA published FATF's June 2026 statements on high-risk and other monitored jurisdictions. It called on all financial intermediaries to take the FATF information into account in their risk management and asked recognised self-regulatory organisations to inform their members¹⁰.

FATF's statement distinguishes the two lists. For the high-risk list (North Korea, Iran and Myanmar), FATF calls for enhanced due diligence, in addition to countermeasures for North Korea and Iran. For jurisdictions under increased monitoring, FATF does not call for enhanced due diligence but encourages the information to be considered in risk analysis. The June Plenary added Bosnia and Herzegovina and Iraq to the increased-monitoring list¹¹. The FATF decisions date from June, so FINMA's July communication is the Q3 item.

Key Compliance considerations

- Update the geographic risk methodology for the June FATF lists, and record how each listed jurisdiction feeds customer and counterparty risk scoring.
- Distinguish the two lists in the methodology. For the high-risk list (North Korea, Iran, Myanmar), FATF calls for enhanced due diligence, and for countermeasures against North Korea and Iran. For jurisdictions under increased monitoring, FATF does not call for enhanced due diligence but asks that the information be considered in risk analysis. A listing should therefore not trigger automatic rejection or automatic enhanced due diligence.
- Extend the review to counterparties, meaning other virtual asset service providers, custodians, liquidity providers and the jurisdictions of their wallets, not only the customers' residence.
- Keep evidence of how the firm took the FATF information into account, since FINMA expects it to be reflected in risk management. Firms that are members of a self-regulatory organisation should also follow their organisation's communications.
- Record the treatment of Bosnia and Herzegovina and Iraq - the June additions to the increased-monitoring list.

¹⁰ FINMA. (2026, July 14). FATF has updated its statements. <https://www.finma.ch/en/news/2026/07/20260714-fatf-statement/>

¹¹ Financial Action Task Force (FATF). (2026, June 19). Jurisdictions under increased monitoring. <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-june-2026.html>

Sanctions notices

On 18 August FINMA reported the Swiss list update of 17 August under the Iran ordinance, in force from 18 August at 11 pm¹². It called on financial intermediaries to implement the prohibitions, freeze the assets of sanctioned persons and report affected relationships to SECO. It added that reporting to SECO does not remove the duty to make additional clarifications under Article 6 of the Anti-Money Laundering Act (AMLA) where suspicion arises. If the suspicion cannot be dispelled, a report must be made without delay to the Money Laundering Reporting Office Switzerland (MROS) under Article 9.

On 14 July FINMA reported a SECO update of the ISIL/Al-Qaida list following a UN committee decision of 10 July¹³. These are general financial sector notices, relevant to crypto providers because sanctions screening applies to wallets and transfer counterparties as well as to customers.

¹² FINMA. (2026, August 18). Aktualisierte Sanktionsmeldung: Islamische Republik Iran (SR 946.231.143.6). <https://www.finma.ch/en/news/2026/08/20260818-sr-946-231-143-6/>

¹³ FINMA. (2026, July 14). Aktualisierte Sanktionsmeldung: ISIL (Da'esh) und Al-Kaida (SR 946.231.08). <https://www.finma.ch/en/news/2026/07/20260714-sr-946-231-08/>



Key Compliance considerations

- Confirm that list updates reach screening systems promptly and that the update time is recorded. For the Iran update, the change took effect on 18 August at 11 p.m., so timing matters.
- Screen wallet addresses, transfer counterparties and originator and beneficiary data as well as customers, and state in the policy which lists are used.
- Keep a clear procedure for a match: apply the prohibitions, freeze the assets of sanctioned persons and report the affected relationships to SECO, as FINMA calls for.
- Do not treat the SECO report as the end of the analysis. FINMA states that it does not remove the duty to make additional clarifications under Article 6 AMLA where suspicion arises, and that a report must be made without delay to MROS under Article 9 if the suspicion is not dispelled. Use separate workflows and records for the two reports.
- Look at exposure to Iranian and other sanctioned-jurisdiction platforms, including indirect exposure. Sanctions activity by other authorities during Q3 has increased attention on crypto platforms with Iranian links, so Swiss-law compliance should be read alongside it.
- Keep a short audit trail for each list update showing when it was received, screened and resolved.



United States

Iran-related sanctions and digital assets

Sanctions enforcement was the most active area of US crypto AML activity in Q3.

- On **7 August 2026** OFAC designated the Shelbit exchange network and the Iran-based exchange Aban Tether¹⁴. The Treasury release noted that the UAE's Virtual Assets Regulatory Authority had taken enforcement action against a Shelbit entity in January 2025 and July 2026, yet the entity remained in business. Aban Tether was designated under E.O. 13902 for operating in Iran's financial sector.
- On **17 September 2026** OFAC designated the exchange BitBank, its software developer and three associates of the financier Babak Zanjani¹⁵. It alleged transfers of hundreds of millions of dollars in Bitcoin to the Islamic Revolutionary Guard Corps. Treasury stated that the designations rely on a determination under E.O. 13902 targeting Iran's digital asset sector, as part of a wider campaign against Iran.

¹⁴ U.S. Department of the Treasury. (2026, August 7). Treasury sanctions crypto exchanges funding Iran's IRGC and enabling illicit finance [Press release SB0598]. <https://home.treasury.gov/news/press-releases/sb0598>

¹⁵ U.S. Department of the Treasury. (2026, September 17). Operation Economic Outcast disrupts digital asset exchange enabling the Iranian regime [Press release SB0632]. <https://home.treasury.gov/news/press-releases/sb0632>



For non-US firms, the significance is exposure. OFAC's FAQs explain that foreign financial institutions and other non-US persons transacting with designated exchanges may face sanctions themselves.

Key Compliance considerations

- Refresh sanctions screening and exposure reviews for Iranian exchanges, their executives and associated wallet infrastructure, including indirect exposure through intermediaries.
- Identify respondents that serve crypto exchanges, payment processors, OTC desks, general trading companies and online gambling merchants, especially in the UAE, Georgia and Poland. Ask whether any respondent customers are, or are owned or controlled by, the designated Shelbit entities, Aban Tether, BitBank, its developer or the named individuals.
- FinCEN's May 2026 alert on IRGC networks describes unclear sources of funds, general trading companies with opaque ownership in UAE Free Zones, likely front companies transacting large amounts from non-resident accounts, unusual use of multiple exchange houses, unregistered peer-to-peer exchangers and nested digital asset service providers. It states that no single red flag is determinative. Add these to monitoring scenarios, including for stablecoin and gambling-related flows.
- FinCEN's alert asks institutions with exposure to consider reviewing blockchain ledgers for activity attributable to Iran-based digital asset service providers, and to be mindful of unregistered exchanges relying on liquidity from larger providers.
- As reported, on 28 August FinCEN proposed a special measure against Banque Misr UAE and OFAC blocked a Türkiye-based bank and two subsidiaries on 4 September for facilitating Iran's access to banking channels¹⁶. These show that the campaign reaches banks in third countries.
- The designations are entity-level. Treat the jurisdictions concerned as a risk factor to be assessed and evidenced, not as automatic grounds for exit.

¹⁶ Financial Crimes Enforcement Network (FinCEN). (2026, August 28). FinCEN proposes rule that would revoke Banque Misr UAE's correspondent banking access to U.S. financial institutions [Press release]. <https://www.fincen.gov/news/news-releases/fincen-proposes-rule-would-revoke-banque-misr-uaes-correspondent-banking-access>



US stablecoin implementation and AML programme reform

The GENIUS Act's general commencement date is the earlier of 18 January 2027 or 120 days after the primary federal payment stablecoin regulators issue final implementation regulations. Q3 brought further proposals, although the measures outlined below remained at the proposal stage as at 20 September 2026.

- **Stablecoin AML/CFT and sanctions programmes.** The April 2026 joint proposal from the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC), covering AML/CFT and sanctions compliance programmes for permitted payment stablecoin issuers, remained pending.
- **Broader AML programme reform.** On 9 July 2026, the Federal Reserve Board published proposed amendments to AML/CFT programme requirements for banks under its supervision, aligned with FinCEN's April programme-reform proposal¹⁷. This is a broader banking sector initiative, separate from GENIUS Act implementation, with relevance to banks supporting cryptoasset activities.
- **Payment stablecoin issuance, offers and sales.** On 18 August 2026, Treasury published proposed rules implementing section 3 of the GENIUS Act, with comments due by 19 October 2026¹⁸. The proposal clarifies that payment stablecoin issuers may also qualify as digital asset service providers and therefore fall within both sets of requirements. It also addresses offers and sales by digital asset service providers, including those involving foreign-issued payment stablecoins.

¹⁷ Board of Governors of the Federal Reserve System. (2026, July 9). Anti-Money Laundering and Countering the Financing of Terrorism Programs [Notice of proposed rulemaking; 12 CFR Part 208; Docket No. R-1835; RIN 7100-AG78]. 91 Fed. Reg. 42363 (Vol. 91, No. 130). <https://www.govinfo.gov/content/pkg/FR-2026-07-09/pdf/2026-13919.pdf>

¹⁸ U.S. Department of the Treasury. (2026, August 18). GENIUS Act regulations on payment stablecoin issuance, offer, and sale [Notice of proposed rulemaking], 91 Fed. Reg. 53368. <https://www.federalregister.gov/documents/2026/08/18/2026-16796/genius-act-regulations-on-payment-stablecoin-issuance-offer-and-sale>



CLARITY Act stalls in the Senate

On **15 September 2026**, the Senate rejected cloture on the motion to proceed to H.R. 3633, the Digital Asset Market Clarity Act, by **49 votes to 50**, falling short of the 60 votes required. This was a procedural vote, not a vote on final passage. No Democrat voted in favour. Four Republicans voted against, although Senator Thom Tillis did so to enable him to enter a motion to reconsider. That motion leaves open a procedural route to another vote but does not guarantee one¹⁹.

The House passed its version on 17 July 2025, by 294–134. The Senate Banking Committee advanced its substitute on 14 May 2026, by 15–9, and the bill was reported to the Senate on 1 June. Further negotiations combined the Banking and Agriculture Committee proposals. Sponsors released their final pre-vote draft on 14 September, incorporating changes to ethics provisions, stablecoin rewards and developer protections. This was the text they intended to offer as a substitute if the Senate proceeded^{20 21 22}.

¹⁹ U.S. Senate Press Gallery (Daily Press). (2026, September 15). Tuesday, September 15, 2026 [Senate floor log, 3:00 p.m. entry on H.R. 3633]. <https://www.dailypress.senate.gov/tuesday-september-15-2026/>

²⁰ Office of the Clerk, U.S. House of Representatives. (2025, July 17). Roll Call 199: H.R. 3633, Digital Asset Market Clarity Act, on passage [Yea-and-nay vote]. <https://clerk.house.gov/Votes/2025199>

²¹ U.S. Senate Committee on Banking, Housing, and Urban Affairs, Majority. (2026, May 14). Chairman Scott, Senate Banking Committee advance Clarity Act in historic bipartisan vote [Press release]. <https://www.banking.senate.gov/newsroom/majority/chairman-scott-senate-banking-committee-advance-clarity-act-in-historic-bipartisan-vote>

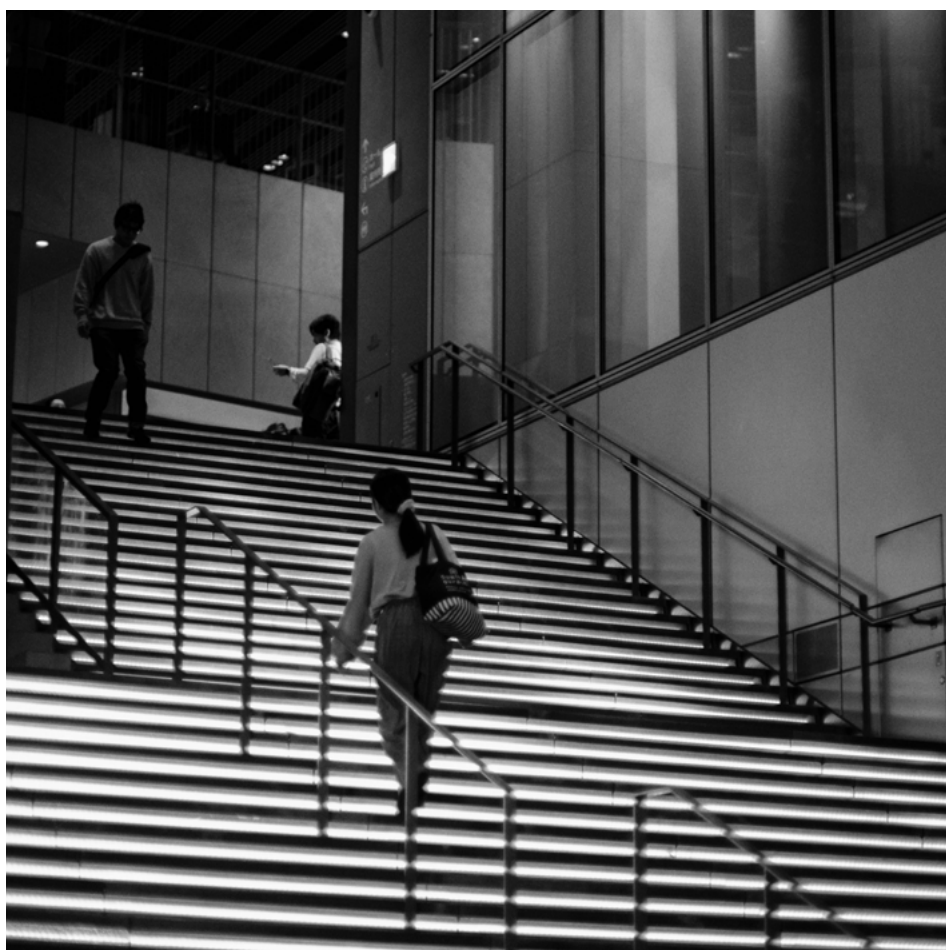
²² U.S. Congress, Senate. (2026, June 1). H.R. 3633 (RS), Digital Asset Market Clarity Act [Bill, reported in Senate with an amendment, 119th Cong., 2d sess.]. U.S. Government Publishing Office. <https://www.govinfo.gov/app/details/BILLS-119hr3633rs>

For AML compliance, the September draft remains relevant as an indication of possible legislative direction. It would expressly bring digital commodity brokers, dealers and exchanges within the Bank Secrecy Act's definition of financial institutions, expand Treasury's special-measures powers for certain digital-asset-related illicit finance, and introduce specific requirements for digital asset kiosks.

It also proposes protections from money-transmission requirements for qualifying non-controlling developers and providers. These protections depend on the statutory conditions, including the ability to control transactions; "non-custodial" should not be treated as a blanket exemption.

Key Compliance considerations

- **Maintain current controls.** Keep AML, sanctions and applicable licensing arrangements aligned with existing law. Treat CLARITY as a legislative monitoring item rather than an enacted compliance framework.
- **Track the latest AML provisions.** Assess potential changes to intermediary coverage, Treasury's special measures powers, kiosk requirements and the treatment of DeFi. Use the September draft when assessing the latest proposals.
- **Do not rely on proposed developer protections.** Firms using non-custodial tools or DeFi protocols should document their activities and control arrangements against current requirements. A proposed exemption provides no present protection.



United Kingdom

Authorisation gateway opens

On 16 September 2026 the FCA published policy statement PS26/18²³, setting out how the legislation underpinning the cryptoasset regime applies and which activities require authorisation. The regime comes into force on 25 October 2027. The authorisation gateway opens on 30 September 2026. Firms relying on the savings and transitional provisions must apply within a window closing on 28 February 2027. Existing registrations under the Money Laundering Regulations, and existing FSMA authorisations, do not convert automatically. Firms within the perimeter need to be authorised or vary their permissions.

This follows the FCA's final rules of 30 June (PS26/9 to PS26/13), which were covered in our Q2 update.

²³ Financial Conduct Authority (FCA). (2026, September 16). Crypto firms get guidance on how the new regime applies [Press release] (PS26/18). <https://www.fca.org.uk/news/press-releases/crypto-firms-get-guidance-how-new-regime-applies>



Draft proposal to FSMA

On 15 September 2026 HM Treasury laid a draft of the Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026. The draft instrument has not yet been made and is not in force. It follows HM Treasury's April draft. It would carve qualifying transfers of UK-issued qualifying stablecoins out of the regulated activities of dealing and arranging, pending separate payments reform²⁴.

The carve-out is narrower than a general exemption for stablecoins. It depends on the stablecoin being issued through the regulated stablecoin issuance activity, and lending and borrowing involving such stablecoins remain within the dealing perimeter. The dealing, arranging and financial promotion amendments are drafted to commence on 25 October 2027.

²⁴ HM Treasury. (2026). Explanatory memorandum to the draft Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026. [legislation.gov.uk](https://www.legislation.gov.uk). The date the draft was laid (15 September 2026) comes from secondary reporting and should be checked against Parliament's records. https://www.legislation.gov.uk/ukdsi/2026/9780348287233/pdfs/ukdsiem_9780348287233_en_001.pdf

Enforcement against unregistered peer-to-peer crypto trading

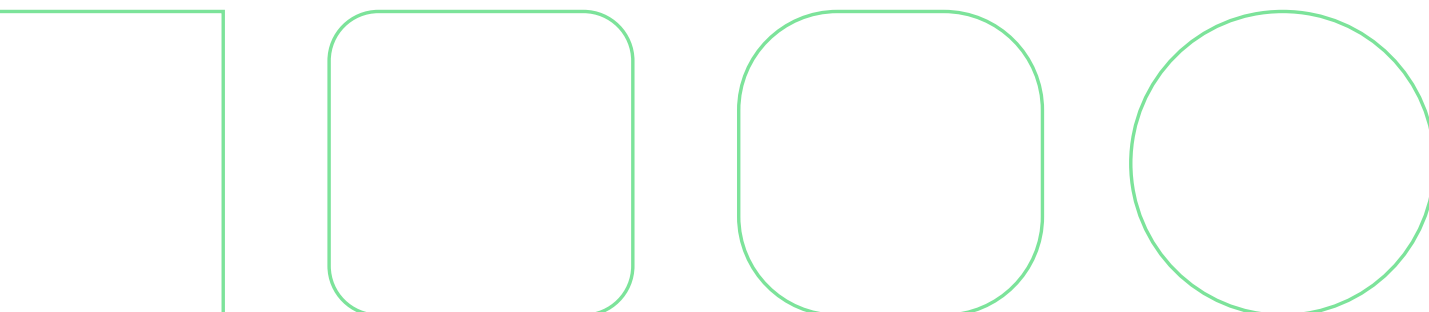
The FCA announced further joint operations against illegal peer-to-peer crypto trading in London. It worked with HM Revenue & Customs and the Metropolitan Police Service, targeted three premises suspected of illegal trading, and issued cease and desist letters at all three. The action was taken under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017²⁵. It follows an FCA-led operation announced on 22 April 2026 against eight premises, carried out with HMRC and the South West Regional Organised Crime Unit.

The legal position is one of existing registration requirements, not new rules. The FCA states that anyone carrying on peer-to-peer trading by way of business in the UK requires appropriate registration, and that there are currently no FCA-registered peer-to-peer crypto businesses in the UK.

The FCA's concern is that unregistered traders operate outside the controls designed to detect and prevent money laundering, and so can offer criminals a route to move and launder funds. The evidence gathered in the April operation is supporting criminal investigations.

The FCA notes that crypto remains largely unregulated in the UK, apart from anti-money laundering and financial promotion rules, until October 2027.[1] The significance for compliance teams is that supervisors and law enforcement are targeting the unregistered peer-to-peer segment now, ahead of the wider authorisation regime.

²⁵ Financial Conduct Authority (FCA). (2026, September 17). FCA and partners continues crackdown on illegal crypto trading [Press release]. <https://www.fca.org.uk/news/press-releases/fca-and-partners-continues-crackdown-illegal-crypto-trading>



Key Compliance considerations

- Test the “by way of business” line. Personal peer-to-peer activity does not require registration, but activity by way of business does.[2] For customers who trade in volume, document the analysis behind any view that their activity is personal.
- Look for the pattern in customer and account activity. Indicators include frequent high volume transfers linked to crypto sales, many counterparties, repeated purchase and resale, and business-like use of a personal account. For banks and payment firms these should prompt enhanced review, but the presence of peer-to-peer activity alone does not show illegality.
- Verify registration for business customers. Where a customer says it is a crypto business, check the FCA register and keep a record of the check. The FCA’s Firm Checker is available for this purpose.[1]
- Review on-ramp and off-ramp exposure. Consider where funds enter or leave the firm through unregistered intermediaries, including cash and same-day cash-out patterns.
- Prepare for law enforcement requests. Evidence from these operations is feeding criminal investigations, so firms should be ready to handle production requests, retain records and consider suspicious activity reporting where they hold relevant information.
- Registered firms should check their own scope. Confirm that any peer-to-peer, matching or broker-like activity sits within the registration or the authorisation being sought. Authorisation applications open on 30 September, and existing registrations do not convert automatically.



What is still to come

The FCA has announced an October 2026 consultation on targeted changes covering UK qualifying stablecoins, proprietary trading and market making, certain technology providers, decentralised protocols and safeguarding involving central securities depositories.[12] Further consultations are expected on financial crime requirements through the FCA's Financial Crime Guide, on custodian resolution and on DeFi guidance.[16]

Key Compliance considerations

- Decide whether to apply within the gateway window, and plan the AML/CFT evidence needed for the application alongside conduct, governance and prudential material.
- Do not assume that an existing MLR registration carries over.
- Watch the forthcoming Financial Crime Guide consultation, which is likely to define supervisory expectations for financial crime controls.

International standards and other jurisdictions

FATF: implementation gaps and DeFi

On 16 July 2026 the FATF published its seventh targeted update on implementation of its standards on virtual assets and virtual asset service providers (VASPs). It found that 83% of surveyed jurisdictions have passed legislation implementing the Travel Rule, up from 73% in 2025. It also found that many jurisdictions are still working on implementing the rules in practice, and that organised crime groups are taking advantage of the gaps²⁶. Many jurisdictions still struggle to turn risk assessments into supervision and enforcement, and 22% of assessed jurisdictions remain non-compliant with Recommendation 15. This publication was approved at the June Plenary, and it is a Q3 publication for the purposes of this update.

On 21 July 2026 the FATF published a targeted report on regulatory challenges from DeFi. It found that 132 of 143 responding jurisdictions have not implemented the FATF Standards for qualifying DeFi arrangements, and that only two of 142 have licensed or registered a DeFi arrangement in practice²⁷. The report confirms that DeFi arrangements fall within scope where a person exercises control or sufficient influence. It also finds that centralised elements frequently persist in arrangements presented as decentralised, including through governance token concentration, administrative privileges and control over upgrades, and it sets out indicators to identify such control.

The FATF has stated that DeFi requires a functional, risk-based approach, and it makes recommendations both to authorities and to institutions interacting with DeFi arrangements.^[26] It does not follow that all DeFi is regulated, or that any is exempt. The question is whether an identifiable person exercises control.

The Plenary of June 2026 also adopted the mutual evaluation reports of Canada and Türkiye, due for publication between September and October 2026²⁸.

²⁶ Financial Action Task Force (FATF). (2026, July 16). FATF calls for closing of regulatory gaps as virtual asset illicit finance risks become more complex [Seventh targeted update on implementation of the FATF Standards on virtual assets and VASPs]. <https://www.fatf-gafi.org/en/news/targeted-updated-va-vasps-2026.html>

²⁷ Financial Action Task Force (FATF). (2026, July 21). FATF urges action to respond to emerging risks from decentralised finance [Targeted report on regulatory challenges from DeFi]. <https://www.fatf-gafi.org/en/news/targeted-report-decentralised-finance-2026.html>

²⁸ Financial Action Task Force (FATF). (2026, June 19). Outcomes: FATF Plenary, 17–19 June 2026. <https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2026.html>



Australia: Travel Rule now in operation

Under AUSTRAC's transitional rules, the obligations for new virtual asset services, including the Travel Rule, were deferred until 1 July 2026²⁹. Virtual asset transfers by both existing and newly regulated providers are therefore now subject to Travel Rule requirements.

Key Compliance considerations

- Align Travel Rule and unhosted wallet controls with the FATF's findings, and evidence that risk assessments feed monitoring and escalation.
- When a customer or counterparty uses DeFi, document the analysis of control and influence instead of relying on the label "decentralised".
- Track the October Plenary and the Canadian and Turkish evaluation reports for supervisory themes.

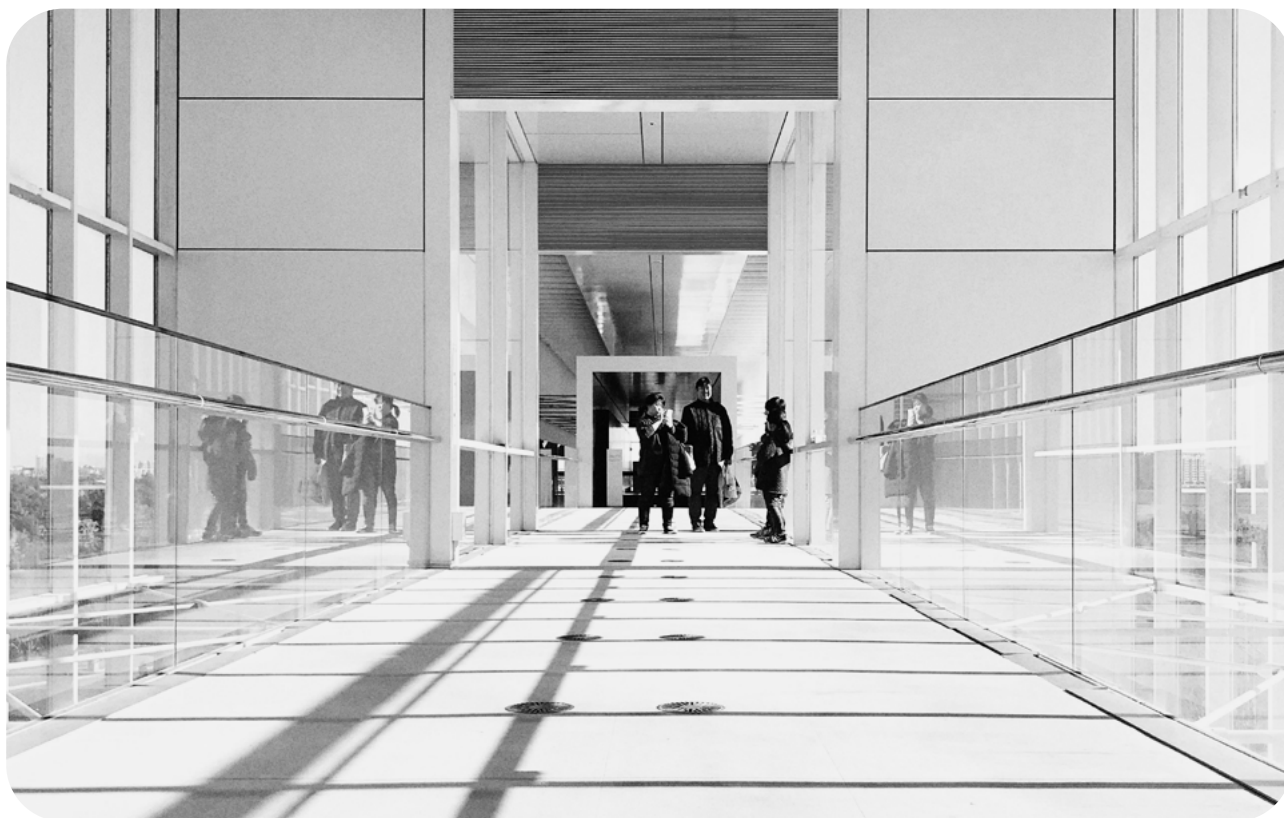
²⁹ Australian Transaction Reports and Analysis Centre (AUSTRAC). (2026). What to expect from the changes to the AML/CTF Rules. <https://www.austrac.gov.au/what-expect-changes-amlctf-rules>

Looking ahead

Several dates fall at or just after the end of the reporting period.

- **30 September 2026:** the FCA gateway opens; the MiCA review consultation closes; AMLA's group-wide RTS are due to the Commission.
- **1 October 2026:** Switzerland's revised AMLA and LETA enter into force.
- **October 2026:** the FCA consultation on targeted changes to the crypto regime; the FATF Plenary.
- **19 October 2026:** comments due on the Treasury GENIUS Act proposal.
- **1 January 2027:** planned date for the revised AMLO-FINMA.
- **18 January 2027:** the latest date on which the GENIUS Act takes effect.
- **10 July 2027:** the AML Regulation applies across the EU.
- **25 October 2027:** the UK cryptoasset regime commences.

The common thread is that enforcement and authorisation are now supervisory questions about evidence. Sanctions screening, ownership data, Travel Rule operation and the documented reasoning behind risk decisions are what supervisors will test.



Disclaimer

This newsletter is a marketing communication highlighting selected key regulatory developments. It is not exhaustive and does not constitute legal, regulatory, compliance or investment advice. Information reflects the position at the publication date and may change. Readers should review the underlying sources, assess how relevant developments affect their activities and seek independent professional advice where appropriate.



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