STABLECOIN COMPLIANCE & REGULATORY ENFORCEMENT TRENDS

Early Warning Services, LLC

06.01.2026

BCLP

Today's Agenda

1. Introduction & Learning Objectives
2. Cross-cutting enforcement themes
2. U.S. Regulatory Landscape
3. U.K. Regulatory Landscape
4. Additional Jurisdictional Considerations
5. Key Takeaways

Speakers

Katie Hausfeld

Saurish Appleby-Bhattacharjee

John Budd

Suhail Mayor

Learning Objectives

What We Will Cover Today

- Where regulators are actually focused — not just what the rules say
- How the global enforcement landscape shapes stablecoin compliance programs
- What an Issuer must anticipate as it evaluates launching a stablecoin-based international remittance service

Why This Matters for Issuers

- Issuer plans to issue its own stablecoin for international remittance
- Remittance = one of the highest-scrutiny sectors in global AML enforcement
- Stablecoin remittance combines two heavily regulated activities — compounded risk profile
- The cost of getting it wrong:
  - Binance: $4.3B resolution + CEO imprisonment
  - Western Union: $586M for AML/remittance failures
- A single failure can trigger simultaneous enforcement across multiple agencies and jurisdictions

Cross-Cutting Enforcement Themes

Six Enforcement Themes That Cut Across Every Jurisdiction

Anti-money laundering and illicit finance — the most common, most severe, and most personally costly enforcement actions

Sanctions compliance as a threshold condition — technical blocking capability required before the first token is issued

Fraud and misrepresentation — particularly reserve accuracy and executive certification obligations

Bribery and corruption risks arising from global remittance operations in high-risk markets

Consumer protection as a rapidly escalating enforcement priority across major jurisdictions

Cross-agency and cross-border enforcement coordination, and an expanding enforcement perimeter that now extends beyond exchanges to banks, Issuers, brokers, custodians, and technology providers

U.S. Regulatory & Enforcement Landscape

A Brief Review of the GENIUS Act

Civil Monetary Penalties

- Up to $100,000/day for material violations by permitted Issuers
- Additional $100,000/day for knowing participation
- Unlicensed issuance of a USD-denominated stablecoin: up to $100,000/day
- No grandfather rights. No de minimis exception
- Enforcement clock **starts Day 1** of non-compliance

Criminal Liability

- False CEO/CFO reserve certifications: criminal liability under 18 U.S.C. § 1350(c) (the Sarbanes-Oxley provision)
- Unlicensed issuance: DOJ referral; fines, imprisonment, or both
- Reserve misrepresentation and AML failures are C-suite criminal risks — not regulatory technicalities

GENIUS Act + Bank Secrecy Act: Remittance-Specific Intersection

Issuers will operate simultaneously as a **permitted stablecoin issuer** and a **BSA-regulated MSB**

GENIUS Act AML/sanctions obligations layer on top of — not instead of — existing BSA/FinCEN requirements

An inaccurate certification is itself an enforcement trigger

Annual board-level AML/sanctions certification required

Who has enforcement authority?

DOJ/FBI	FinCEN	OFAC	CFPB/FTC	State AGs
Criminal prosecution; money laundering; unlicensed transmission	BSA/AML civil enforcement; SAR/CTR; MSB oversight	Sanctions — strict liability; SDN list includes wallet addresses	Consumer protection; Remittance Rule (Dodd-Frank §1073)	Money transmitter licensing; BitLicense; 50-state exposure

AML Enforcement — The Primary Risk for a Stablecoin Remittance Issuer

Primary Risks

- Stablecoin remittance services combine the AML risk of cross-border money transmission with the unique traceability challenges and anonymity risks of blockchain-based value transfer
- Regulators and FATF have specifically identified stablecoin remittance corridors as an emerging vector for the same illicit finance typologies traditionally associated with informal value transfer systems
- Issuers will be scrutinized under *both* the BSA/MSB framework *and* the GENIUS Act AML framework simultaneously

Key typologies regulators are targeting

- USDT/TRON-based cross-border illicit payments
- Hawala-like underground remittance via stablecoins
- Structuring below CTR/SAR thresholds
- Chain-hopping to break audit trails
- Nested exchanges and unregistered MSBs

Key AML Enforcement Actions

Case	Penalty	Key Lesson
Western Union (2017)	$586M	Awareness of suspicious activity without action is itself a violation — this is the remittance-sector AML benchmark
Binance/CZ (2023)	$4.3B; CEO imprisoned	An AML program that exists on paper but is not effective is itself a criminal violation — regulators look at actual outcomes
Bitfinex/Morgan & Lichtenstein (2022)	$3.6B seized	DOJ's blockchain tracing capability is highly sophisticated — stablecoin remittance flows are traceable
BTC-e/Vinnik (2017)	$110M + criminal indictment	Operating without MSB registration and without filing SARs is a criminal offense — not a regulatory infraction

AML Compliance Imperatives for Issuers

AML programs must be calibrated to crypto-specific and remittance-specific typologies — generic banking AML programs will not satisfy FinCEN for a stablecoin remittance issuer

Blockchain analytics tools (Chainalysis, Elliptic, TRM Labs) are now effectively standard industry practice; regulators expect their deployment for remittance monitoring

Transaction monitoring must cover counterparty and beneficiary wallets — not just customers

SARs must be filed for suspicious activity identified through blockchain analytics and remittance-specific red flags (structuring, unusually high remittance frequency, high-risk corridor activity)

OFAC Sanctions Enforcement – Strict Liability, No Exceptions

OFAC's Approach to Crypto

- Apparent violations are **strict liability** — no intent required
- Stablecoins constitute "property" subject to blocking obligations
- SDN list designations now include individual wallet addresses, exchanges, and operators
- Voluntary self-disclosure: up to **50% penalty reduction** for timely, good-faith reporting

Remittance-Specific Sanctions Risk

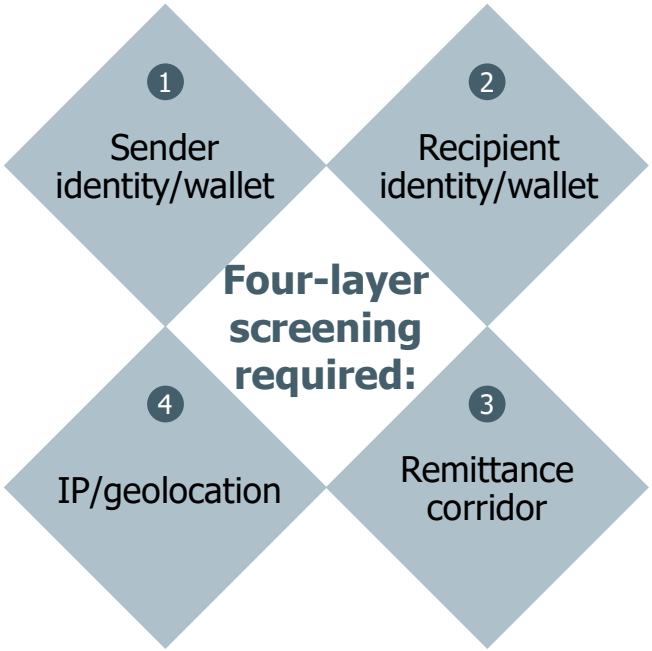
- Elevated risk corridors: Venezuela, Cuba, Iran, Russia-adjacent markets, Syria
- Beneficiary screening required — not just sender
- Some corridors may be **entirely prohibited**

OFAC Enforcement Actions – No Transaction is Too Small

Case	Penalty	Key Lesson
BitPay (2021)	$507,375	IP address screening, customer identity screening, and wallet-level screening are all required — any one alone is insufficient
Bittrex (2022)	$24.3M OFAC + $29M FinCEN	Bittrex subsequently filed for bankruptcy — simultaneous OFAC and AML penalties compound and can be existential
Kraken (2022)	$362,158	No transaction volume is too small to create OFAC liability — every remittance transaction must be screened
Binance — OFAC element (2023)	$968M (within $4.3B resolution)	Sanctions compliance cannot be outsourced to a third-party platform — issuer bears direct liability

Building OFAC Compliance into Issuer's Product Architecture

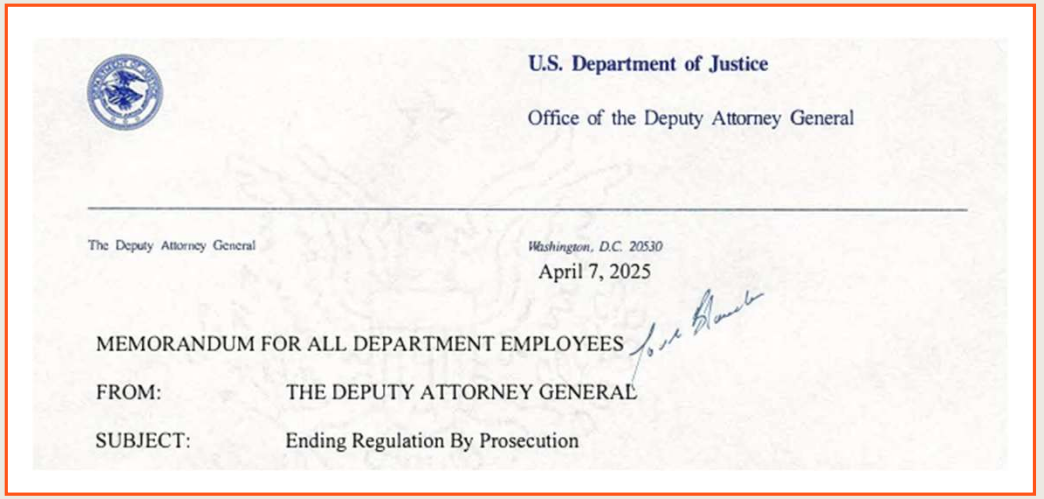
- Technical blocking capability is **mandatory under the GENIUS Act** — precondition to issuance



- Russia-adjacent corridors (UAE, Turkey, Kazakhstan, Georgia) are a specific OFAC monitoring priority
- Dedicate a sanctions compliance officer with direct board reporting
- Establish a self-disclosure protocol for discovered violations before enforcement contact

© Bryan Cave Leighton Paisner

DOJ Policy Shift: Ending Regulation by Prosecution



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

April 7, 2025

MEMORANDUM FOR ALL DEPARTMENT EMPLOYEES

FROM: THE DEPUTY ATTORNEY GENERAL

SUBJECT: Ending Regulation By Prosecution

Prosecutors should not charge regulatory violations in cases involving digital assets—including but not limited to unlicensed money transmitting under 18 U.S.C. § 1960(b)(1)(A) and (B), violations of the Bank Secrecy Act, unregistered securities offering violations, unregistered broker-dealer violations, and other violations of registration requirements under the Commodity Exchange Act—unless there is evidence that the defendant knew of the licensing or registration requirement at issue and violated such a requirement willfully.

> unless there is evidence that the defendant . . . **violated such a requirement *willfully*.**

FCPA Exposure — A Real Risk for a Global Remittance Operator

Remittance corridors may include markets with elevated corruption risk: Latin America, Southeast Asia, South Asia, Sub-Saharan Africa

Payments to foreign officials to facilitate licensing, banking access, or corridor access = FCPA violations

Facilitation payments to expedite MSB licensing in foreign markets = specific FCPA risk

Binance's compliance monitor expressly includes review of FCPA exposure — DOJ is watching global crypto operators

No stablecoin-specific FCPA action yet — but remittance operators with emerging market exposure are the highest-risk category

Fraud & Market Manipulation – Enforcement Actions Issuers Must Know

Key Risk Typologies

- Misrepresentation of reserve composition or backing — the most heavily enforced category
- De-pegging events exploited for market manipulation or front-running
- For a remittance issuer: misrepresentation of exchange rates, fees, or delivery amounts in consumer-facing disclosures — regulatory fraud and a consumer protection violation simultaneously

Key Enforcement Actions

- TerraUSD (UST) / Do Kwon (2022–2024): $40 billion in investor losses; $4.7 billion civil penalty; criminal proceedings pending for securities fraud, wire fraud, and market manipulation
- Tether / Bitfinex (CFTC, $41M, 2021): Tether misrepresented that USDT was always fully backed 1:1 — reserves were at times inadequate or commingled; reserve disclosure accuracy is an enforcement-grade obligation
- FTX / Alameda Research (2022–2023): Stablecoins used to obscure misappropriation; Sam Bankman-Fried sentenced to 25 years — robust counterparty due diligence across Issuers entire ecosystem is essential

Consumer Protection — CFPB Remittance Rule Is Active Enforcement

CFPB Remittance Rule

- Applies to any "remittance transfer provider" — Issuer will be subject to this rule
- Required pre-payment disclosures: exact exchange rate, all fees and taxes, amount received by beneficiary, funds availability date
- Disclosures must be in the sender's language where applicable
- Error resolution procedures mandatory

FTC & State AG Enforcement

- FTC and state AGs (NY, CA, TX) actively enforce against crypto consumer protection violations
- A regulatory violation triggers simultaneous regulatory enforcement and class action litigation risk

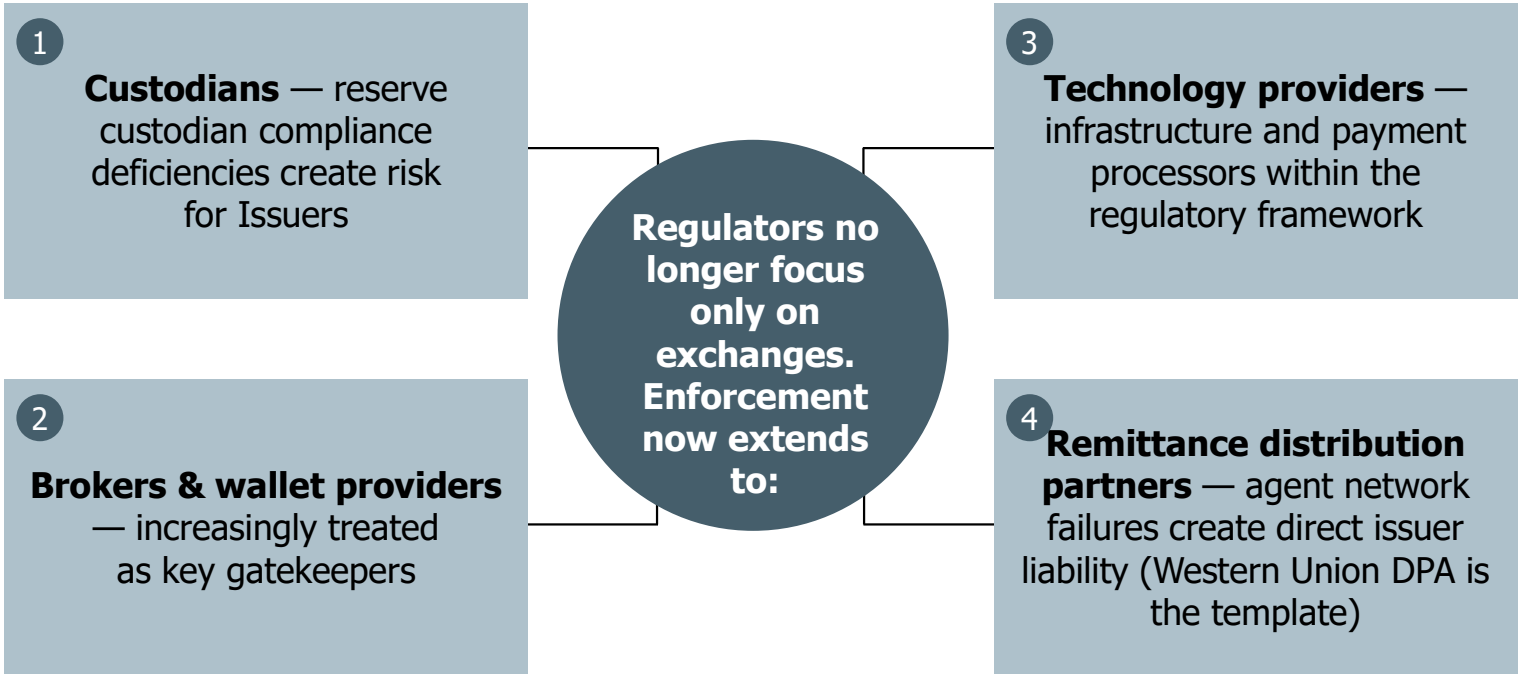
Board Accountability Is an Enforcement-Grade Expectation

- Regulatory authorities increasingly expect boards of directors and executive management to set the "tone from the top" by prioritizing compliance, risk management, and ethical conduct in all crypto-related activities — this is no longer a governance best practice; it is an enforcement expectation
- **What regulators expect from boards:**
  - Overseeing the development and implementation of crypto compliance frameworks
  - Ensuring that sufficient resources and expertise are allocated to compliance functions
  - Regularly reviewing and challenging management's approach to crypto risk
  - Receiving timely updates on regulatory changes and enforcement trends

- Companies are advised to appoint dedicated compliance officers with a direct reporting line to top management; pay and performance evaluations should consider compliance with regulatory objectives alongside financial results

Cautionary note: The Binance compliance monitor mandate — now overseeing board-level governance — is the consequence of regulators finding that tone from the top was absent.

Stablecoin Issuers Entire Ecosystem Is In Scope



Key principle: Issuer cannot insulate itself from enforcement risk by delegating compliance to a third party — the issuer is accountable for its entire operational ecosystem.

U.K. Regulatory & Enforcement Landscape

Relevant public authorities

Financial Conduct Authority (FCA)	Lead conduct regulator, governs AML/CTF registration and supervision and enforces financial promotions regime + pending expansion of regulated activities regime to cryptoassets.
Prudential Regulation Authority (PRA)	• Prudential supervision of dual-regulated firms (banks, insurers) with cryptoasset exposures. • PRA-regulated firms seeking crypto permissions require a variation of permission. The PRA rules for the crypto sector expected to follow FSMA commencement in 2027.
Bank of England	Oversight and supervision of systemic sterling-denominated stablecoins.
HM Treasury (HMT)	UK finance ministry that leads on policy and legislation, e.g. Financial Services Markets Act 2000 (Cryptoassets) Regulations 2026.
Office of Financial Sanctions Implementation (OFSI)	Financial sanctions enforcement.
National Crime Agency (NCA)	• Criminal financial investigation and SAR recipients. • Conduct crypto asset seizure, freezing and forfeiture under Economic Crime and Corporate Transparency Act 2023.
Serious Fraud Office (SFO)	SFO conduct investigation and prosecution of serious and complex crypto fraud.

Anti-Money Laundering (**AML**) / Registration Regime

1

Current position:

- Cryptoasset businesses providing services in the UK are currently subject to AML registration under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs").
- Registration required for "cryptoasset exchange providers" and "custodian wallet providers" before carrying on business in the UK.
- FCA has taken a tough approach to registration applications, with many rejected or withdrawn.
- However, the MLRs have a limited territorial scope, meaning it is possible to access UK customers from offshore.

2

Core ongoing obligations:

- Full AML/CTF obligations under the MLRs: customer due diligence (standard, simplified and enhanced), ongoing monitoring, PEP and sanctions screening, and Suspicious Activity Report (SARs) filing with the National Crime Agency.
- The SAR policy must include a clear route of escalation internally to the MLRO/Nominated Officer and externally to the National Crime Agency, including awareness of tipping-off obligations and Defence Against Money Laundering (DAML) SARs.
- Each year, all registered cryptoasset businesses must submit a REP-CRIM return (Annual Financial Crime Reporting) via the FCA's RegData system within 60 business days of the business's Accounting Reference Date.

3

Transition point:

- The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 ("Cryptoasset Regulations") amend the MLRs to reflect the shift from AML registration to full authorisation under the Financial Services and Markets Act 2000 ("FSMA") for newly regulated cryptoasset activities.
- The UK government recently announced an important policy shift: stablecoin payments will be regulated as payment services where the stablecoins in question have been issued under the forthcoming new regulated activity for qualifying stablecoin issuance in the UK.
- MLR registration continues as the gateway until the new FSMA regime goes live (25 October 2027).

Financial Promotions Regime

- In October 2023, the regulation of promotions for "qualifying cryptoassets" (QCs) targeting UK customers was brought within the remit of the FCA's financial promotions regime, aligned with existing rules for other high-risk investments, including that promotions must be fair, clear and not misleading.
- QC = In summary, any cryptographically secured digital representation of value or contractual rights that is fungible and transferable.
- A subset of QCs that seeks or purports to maintain a stable value by reference to a single fiat currency, backed by fiat or other assets.
- The rules are set out in FCA Handbook (Principles 7 and 12, COBS 4 and 10) and FCA Policy Statement PS23/6.

Four lawful routes to promote cryptoassets:

1. become an authorised person;
2. have promotion approved by an authorised person;
3. become registered under the MLRs; or
4. make communication using a limited exemption (e.g. where recipients are investment professionals).

Breach of financial promotion restriction at s.21 FSMA is a criminal offence, punishable by up to two years' imprisonment, a fine, or both.

Key consumer protections:

- Cryptoassets classified as Restricted Mass Market Investments require a mandatory risk warning: "Don't invest unless you're prepared to lose all the money you invest".
- Ban on referral bonuses and incentives with a minimum 24-hour cooling-off period for first-time investors. Regulator also mandates an appropriateness assessment.
- FCA enforcement has focused primarily on "finfluencers" engaged in unlawful promotions, resulting in a number of criminal convictions.

Upcoming Legislative Expansion

On 4 February 2026, HM Treasury made the Cryptoasset Regulations, which will bring a wide range of cryptoasset activities within the FSMA perimeter.

Approach:

- The Cryptoasset Regulations establish the legislative framework through which cryptoasset activities will be regulated using existing FSMA concepts, rather than through a standalone crypto-specific regime.
- They provide the statutory basis for extensive FCA rulemaking across conduct, disclosure, market integrity and prudential matters.

Consultation Papers:

FCA CP25/40 – Regulated cryptoasset activities

FCA CP25/41 – Admissions, disclosures and Market Abuse Regime for Cryptoassets

FCA CP25/42 – Prudential regime for cryptoasset firms

These consultations have now closed and the FCA is considering responses. New cryptoasset regime expected to come into force on **25 October 2027**

Authorisation under FSMA and UK Nexus

From 25 October 2027, the Cryptoasset Regulations will introduce new regulated activities for cryptoassets into the FCA's regulatory perimeter. Persons carrying on those activities by way of business "in the UK" will need to hold FCA authorisation.

In advance of that date, firms intending to undertake regulated cryptoasset activities must apply during the authorisation application window, which will run from 30 September 2026 to 28 February 2027.

Whether authorisation is required depends on a combination of factors that must be assessed together:

- is the person carrying on a regulated activity?
- is the activity carried on, or deemed to be carried on, in the UK?
- is it carried on by way of business?
- does an exclusion or exemption apply?

- The Cryptoasset Regulations are designed to bring within scope persons offering services to UK consumers regardless of whether they are based in the UK or overseas – as such, the overseas persons exclusion does not apply to the new regulated cryptoasset activities.

- Perimeter analysis will be inherently fact-specific, and firms cannot rely on the labels or terminology they use to describe their services. What will matter is the substance of the activity and the role performed.

"By way of business"

For regulated cryptoasset activities, a person will only be treated as carrying on a regulated activity "by way of business" if they are carrying on the business of engaging in one or more such activities; a deliberately narrower test, intended to focus the perimeter on persons whose business model involves providing or performing the relevant activity as a service to paying customers.

© Bryan Cave Leighton Paisner

Typical Business Models and Regulated Activities

Firm Type	Regulated Activity	Key Points
Stablecoin Issuers	**Issuing qualifying stablecoins** becomes a regulated activity broken down into three components: offering the stablecoin; redeeming the stablecoin; and maintaining the stabilisation mechanism.	For stablecoin issuance, all three limbs must be carried out from a UK establishment. Where all elements are carried out in the UK on behalf of an overseas person, that overseas person will be treated as carrying on the activity in the UK and will require FCA authorisation.
Exchanges / Trading Platforms	**Operating a qualifying cryptoasset trading** platform (**CATP**) a system which brings together multiple third-party buying and selling interests in qualifying cryptoassets, resulting in contracts for the exchange of those assets for money or other qualifying cryptoassets.	The QCATP activity does not extend to safeguarding cryptoassets before or after a transaction; firms typically require separate permissions for operating a QCATP and for safeguarding.
Custodians / Wallet Providers	**Safeguarding qualifying cryptoassets**, including certain tokenised specified investments, is regulated as a standalone activity capturing firms that hold cryptoassets on behalf of clients, whether as pure custodians or as part of a wider service offering.	Requisite control exists where a firm has the ability, by any means, to bring about the transfer of the benefit of a cryptoasset to another person. Ownership is therefore not determinative of whether safeguarding activity is being carried on.
Brokers / Dealers / OTC	**Dealing in qualifying cryptoassets as both principal and agent**, as well as arranging deals; capturing a wide range of brokerage, execution and OTC business models and also encompassing cryptoasset lending and borrowing services.	• Arranging deals includes both bringing about specific transactions and making ongoing arrangements that facilitate trading, including through trading apps and platforms. • With arranging, the perimeter may apply even where a firm provides only part of the facilities for a transaction.
Staking Providers	**Arranging qualifying cryptoasset staking** involves making arrangements on behalf of another person for blockchain validation using qualifying cryptoassets. In-scope activities may include managing the staking lifecycle, pooling customer assets to meet validator thresholds, and distributing staking rewards.	Purely technical services are generally out of the perimeter; operating a validator node or offering solo staking tools without further involvement is unlikely on its own to amount to arranging qualifying cryptoasset staking.

The Admissions & Disclosures (A&D) and Market Abuse Regime for Cryptoassets (MARC)

Designed to strengthen safeguards by:

- improving information quality at the point of admission to trading
- enhance market integrity by tackling fraud, scams and abusive practices such as insider dealing and market manipulation

- Under the A&D regime, CATPs must act as gatekeepers for public offers and admissions of qualifying cryptoassets. Platforms are expected to establish risk-based admission criteria approved by their governing body, publish these on their websites and review them periodically.
- MARC prohibits insider dealing, unlawful disclosure of inside information and market manipulation. Issuers, offerors and CATPs must disclose inside information promptly unless a justified delay is allowed.
- Exchanges and intermediaries must implement systems and controls to detect, prevent and disrupt abusive behaviour.

"Inside information" must be:

- ✓ Precise
- ✓ Non-public
- ✓ Related to a given cryptoasset
- ✓ Likely to have a significant effect on market price

Prudential and Safeguarding Regime

- The FCA's proposals introduce capital, liquidity, risk management and governance requirements tailored to cryptoasset business models
- The regime introduces baseline permanent minimum capital requirements (PMR), activity-based "K-factor" style capital metrics, liquidity requirements, and enhanced governance and risk management obligations

Proposed PMR levels:

- **£75,000** for dealing as agent / arranging
- **£150,000** for trading platforms, staking and safeguarding
- **£350,000** for stablecoin Issuers
- **£750,000** for dealing as principal

Safeguarding emphasis:

The FCA's approach places particular emphasis on safeguarding exposures, reflecting concerns regarding operational failures, cyber risks and the irreversible nature of cryptoasset transactions.

Wind-down and liquidity:

Firms must maintain sufficient liquid resources to support ongoing operations and enable orderly wind-down; cryptoassets will not generally qualify as liquid assets for prudential purposes due to volatility and valuation unreliability.

PRA position:

PRA involvement in cryptoasset prudential supervision continues to evolve. The PRA has signalled supervisory interest particularly where banks and PRA-regulated firms have cryptoasset exposures. PRA rules for "systemic" stablecoins are not yet finalised and a senior official recently signalled a willingness to soften its position.

© Bryan Cave Leighton Paisner

Sanctions

- In August 2022, cryptoasset firms were added to the list of "relevant firms" under UK sanctions regulations made under the Sanctions and Anti-Money Laundering Act 2018 (**SAMLA**)
- Relevant firms must inform OFSI as soon as practicable if they know or have reasonable cause to suspect a person is a designated person or has committed a breach of UK sanctions obligations

Compliance requirement:

Real-time sanctions screening, blockchain analytics and robust customer identification are essential compliance tools

OFSI July 2025 Cryptoassets Threat Assessment Key Findings:

- OFSI states it is "almost certain" that UK-based cryptoasset firms have under-reported suspected breaches of financial sanctions since August 2022.
- It is highly likely that UK cryptoasset firms have been directly or indirectly exposed to the designated Russian exchange Garantex since its designation in 2023, resulting in breaches of UK financial sanctions.
- It is highly likely that UK-based cryptoasset firms are currently at risk of being targeted by DPRK-linked hackers and IT workers seeking to steal or obtain funds through illicit means.
- It is likely that UK cryptoasset firms are currently facilitating transfers to Iranian cryptoasset firms with suspected links to designated persons.

Enforcement Actions and Trends

Regulator	Firm / Target	Action	Ground	Outcome
FCA	CB Payments Ltd (Coinbase Group)	Fine	AML / financial crime controls – despite a Voluntary Requirement (VREQ) restricting services to high-risk clients, the firm allowed over 13,000 high-risk customers to trade cryptoassets, generating transactions of approximately $226 million.	£3.5 million fine: first FCA enforcement action against a firm enabling cryptoasset trading, brought under the Electronic Money Regulations 2011; fine reduced by 30% for early settlement.
FCA	Multiple unregistered / unauthorised firms	Consumer alerts; website takedowns; app store removals	Communicating financial promotions without authorisation or MLR registration. Targeting UK customers without FCA permissions.	As at Q3 2024, the FCA had issued 1,702 consumer alerts about illegal crypto promotions, taken down over 900 scam crypto websites and removed 56 apps from UK app stores.
FCA	"Finfluencers" (multiple individuals)	Criminal prosecution; fines	Breach of s.21 FSMA — unlawful communication of financial promotions via social media without authorisation	FCA led international crackdown on illegal finfluencers.
FCA	HTX (formerly Huobi) and others	Removal from online platforms	Providing or promoting financial services to UK customers without FCA permissions.	In February 2026, the FCA requested social media companies block HTX's social media accounts to UK-based consumers and requested the removal of HTX applications from the Google Play and Apple stores in the UK.
SFO	Basis Markets	Criminal investigation; arrests	Fraud and money laundering: alleged misappropriation of $28 million raised from investors for a purported "crypto hedge fund" through two fundraising rounds in 2021	SFO launched investigation November 2025: Two men arrested on suspicion of multiple fraud and money laundering offences; first SFO crypto investigation, marking a notable shift in the agency's operational capacity and willingness to pursue complex crypto-based misconduct.
OFSI	Bank of Scotland PLC	Fine	Russia sanctions breach: failure to recognise a customer's designated status due to a spelling variation of their name in their UK passport	£160,000 fine in January 2026: OFSI confirmed it will not tolerate errors in sanctions screening due to transliteration as an excuse for inadvertent non-compliance; directly relevant to crypto firms' own screening obligations.

Additional Jurisdictional Considerations

EU Regime

Markets in Crypto-Assets Regulation (MiCA)

- MiCA is the first attempt to create a uniform EU-wide framework for crypto rather than relying on fragmented national regimes
- Applies directly in all Member States without local implementation differences. This is a key shift from prior regimes where firms had to navigate inconsistent licensing approaches across jurisdictions
- MiCA introduces a harmonised rulebook governing conduct, prudential requirements, and disclosures
- Once authorised in one EU Member State, firms can passport services across the EU without additional licences. This creates a scalable "hub-and-spoke" operating model, typically with one licensing jurisdiction

The regime is deliberately broad:

- **Issuers**: anyone offering tokens to the public or seeking trading admission
- **Cryptoasset Service Providers (CASPs)**: exchanges, custodians, brokers, advisory businesses

Issuers of crypto-assets under MiCA are subject to a regulated disclosure regime, including the requirement to publish a detailed whitepaper setting out:

- the characteristics;
- rights; and
- risks of the token.

Digital Operational Resilice Act (**DORA**) applies to CASPs as regulated financial entities and requires them to implement comprehensive ICT risk management, cybersecurity controls, incident reporting processes and third-party risk oversight.

Expectations for real-time screening against EU sanctions lists; breach is grounds for MiCA authorisation withdrawal.

APAC Regime

- The APAC region has moved decisively ahead of many Western jurisdictions in enacting dedicated stablecoin legislation and building out comprehensive virtual asset AML frameworks.
- The Financial Action Task Force (**FATF**) is the international standard-setter for AML/CFT and its Recommendations apply globally across all three jurisdictions above, as well as the UK and EU.
- FATF also requires countries to license or register VASPs and subject them to AML/CFT supervision – Singapore, Hong Kong and Japan all meet this standard, creating a degree of baseline regulatory consistency that facilitates cross-border compliance frameworks for global firms.

Jurisdiction	Regulator(s)	Stablecoin Regime	Key Points
Singapore	Monetary Authority of Singapore (**MAS**)	MAS finalised its single-currency stablecoin (SCS) framework in 2023. Only stablecoins pegged to a single fiat currency and issued by MAS-regulated banks or holders of a Major Payment Institution licence qualify as "MAS-regulated stablecoins".	• Singapore has established one of the most detailed and internationally influential stablecoin frameworks globally. • Non-compliance with AML obligations has attracted MAS enforcement action and public censure
Hong Kong	Hong Kong Monetary Authority (**HKMA**) Securities and Futures Commission (**SFC**)	The Stablecoins Ordinance came into force on 1 August 2025 and it establishes a licensing regime administered by the HKMA for issuers of fiat-referenced stablecoins.	• A 3 month non-contravention period applied to pre-existing issuers until 31 October 2025 • The SFC has actively enforced against unlicensed platforms and has published a list of suspicious virtual asset trading platforms
Japan	Financial Services Agency (**FSA**)	Japan was the first G7 jurisdiction to enact stablecoin legislation. It restricts stablecoin issuance to banks, registered money transfer service providers, and trust companies only.	• Japan's model is the most conservative globally

Enforcement Themes

Theme	Illustrative Examples	Practical Implication
Unlicensed / Unregistered Activity	Binance ordered to cease services in Belgium (June 2023) and placed on MAS Investor Alert List in Singapore; JPEX operated in Hong Kong without SFC licence with 80+ arrests, US$205 million in investor losses	Jurisdictional nexus analysis must precede any market entry
AML / KYC Failures	Binance failed AML/KYC audit – regulators imposed substantial fines, required stricter due diligence, and appointed external monitors	• Regulators are broadening their areas of attention, extending scrutiny beyond exchanges to banks, issuers, brokers and custodians • AML/KYC controls must be crypto-specific
Stablecoin Compliance as a Gateway Function	Tether (USDT) delisted from regulated EU venues for retail clients from 31 December 2024; HK Stablecoins Ordinance (August 2025) restricts permitted offerors to licensed issuers, SFC-licensed platforms and authorised banks	• Licensing requirements operate as a self-executing gateway • Non-compliant stablecoins are excluded from regulated markets without any formal enforcement proceedings being required
Algorithmic / Unbacked Stablecoin Risk	• Terra/LUNA collapse (2022) - Do Kwon sentenced to 15 years' imprisonment; South Korean prosecutors pursuing separate charges; • Terraform Labs settled SEC civil charges for approximately US$4.5 billion; collapse was the direct catalyst for stablecoin legislation in all three APAC jurisdictions and for MiCA's express exclusion of algorithmic stablecoins	All major regimes now expressly exclude algorithmic and unbacked stablecoins from their regulated stablecoin categories
Cross-Border Coordination & Regulatory Arbitrage	JPEX ringleaders subject to Interpol red notices; Terra/LUNA prosecuted across US SDNY and South Korea simultaneously	Regulators globally are increasing their focus on cross-border enforcement, operational resilience, and the integration of ESG considerations into crypto compliance ; firms cannot assume that regulatory arbitrage between APAC and EU will provide a safe harbour — cross-jurisdictional cooperation is now a live and well-resourced enforcement tool
Perimeter Creep	Brokers, custodians, and wallet providers are increasingly regarded as key gatekeepers even technology providers that build market-access infrastructure, such as payment processors or blockchain analytics firms, are increasingly seen as falling within the regulatory framework	The regulatory perimeter is widening beyond exchanges Third-party and vendor risk management must be integrated into compliance frameworks
Financial Crime & Asset Recovery	FATF's 2025 asset recovery guidance sets out best practices for seizing, managing, and ultimately returning cryptoassets, and explicitly encourages countries to use blockchain analytics and public-private partnerships to improve outcomes	Cryptocurrency has evolved from a niche tool for darknet transactions to a component of professional money laundering networks supporting a diverse range of crime types

Key Takeaways

Key Takeaways

Stablecoins have a unique risk profile as they combine the AML / sanctions risks associated with cross-border money transmission with the unique traceability challenges and anonymity risks of block-chain based value transfer.

The regulatory and enforcement environment surrounding stablecoins is multi-agency, cross-border and continuing to develop.

An issuer's entire ecosystem is in scope, including custodians, brokers and wallet providers, technology providers, and remittance distribution partners.

The risks and associated compliance obligations that apply to an issuer will vary depending on their specific business model. E.g., stablecoins used as a settlement rail between financial institutions are likely to be lower risk than those held directly by retail customers.

Risk mapping and monitoring developing legislation will help issuers stay ahead of the changing regulatory landscape

Strong compliance controls with appropriate board and senior management oversight – particularly surrounding AML and sanctions – are critical.

BCLP. Client Intelligent

bclplaw.com

[This document] provides a general summary and is for information/educational purposes only. It is not intended to be comprehensive, nor does it constitute legal advice. Specific legal advice should always be sought before taking or refraining from taking any action.

[illegible] document