AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 1 of 7

Global Regulatory Landscape & Supervisory Expectations

Regulatory Overview for Digital Asset Firms
AML & Sanctions Practices in the Digital Asset Industry

Introduction and Regulatory Overview

The rapid growth of the digital asset industry has led regulators worldwide to apply traditional anti-money laundering and countering the financing of terrorism controls to crypto businesses. In the United States and internationally, customer due diligence practices (encompassing identity verification for individuals and businesses), transaction monitoring, broader compliance programs, and sanctions screening are now expected of crypto service providers, much as they are for banks.

The Financial Action Task Force — the global AML standards body — updated its guidance in 2019 to explicitly include Virtual Asset Service Providers under AML/CFT regimes, meaning crypto exchanges, custodians, and other platforms must implement customer due diligence, monitor transactions, and screen for illicit activity just like traditional financial institutions. By 2024, over 60 jurisdictions had adopted the FATF Travel Rule (Recommendation 16) for sharing sender/recipient data on crypto transfers, signaling widespread international commitment to crypto AML controls.

Jurisdiction-by-Jurisdiction Overview

United States

In the U.S., crypto exchanges and similar businesses are classified as money services businesses under the Bank Secrecy Act and its amendments. They must register with FinCEN, implement risk-based AML programs, and comply with obligations such as customer identity verification, record-keeping, suspicious activity reporting, and sanctions screening. U.S. authorities have actively enforced these requirements: for example, FinCEN's 2019 guidance clarified that even peer-to-peer exchanges, decentralized application developers, and other crypto intermediaries may be money services businesses if they facilitate value transfer.

Enforcement actions have ramped up — e.g., Binance reached a $4.3 billion settlement in 2023 with U.S. agencies for AML/sanctions failures, and Coinbase was fined $100 million by New York regulators in 2023 for compliance backlogs. The U.S. Treasury's Office of Foreign Assets Control has also penalized crypto companies (exchanges, wallet providers, mixers) for sanctions violations, underlining that digital asset firms are squarely subject to U.S. sanctions laws.

International

Other jurisdictions likewise have tightened crypto compliance rules. Europe implemented the Markets in Crypto-Assets Regulation effective 2024, which designates Crypto-Asset Service Providers as obliged entities under EU AML directives. This means that exchanges and wallet providers in the EU must conduct customer due diligence and transaction monitoring in accordance with the EU's AML/CFT framework. The EU also updated its Transfer of Funds Regulation to extend the Travel Rule to crypto transfers as of December 2024, requiring data-sharing for transfers ≥ €1,000.

UK law similarly mandates that cryptoasset firms comply with the Money Laundering Regulations and the Travel Rule for transfers. Asia-Pacific regulators have also acted: Singapore's Payment Services Act and Japan's Payment Services Act require exchanges with full AML/KYC programs to be licensed, and Hong Kong in 2023 introduced a licensing regime for crypto trading platforms with strict AML obligations.

DeFi: The Regulatory Challenge

In most major markets, operating a centralized crypto exchange or custodial service without robust AML controls is illegal. Meanwhile, fully decentralized finance protocols pose a regulatory challenge since they often lack a clearly accountable entity. FATF guidance suggests that individuals or entities with sufficient influence over a decentralized protocol (like developers or operators of a front-end interface) might be considered Virtual Asset Service Providers and liable for compliance, but this area remains ambiguous and evolving.

Regulators in the EU have even floated an "activity-based" approach — overseeing decentralized finance activities via points of centralized oversight (such as regulating how regulated institutions interact with decentralized platforms, or specific features like back-end developers and oracles).

Overall Trend: Convergence

Overall, between 2024 and 2026, the trend is toward global convergence: centralized crypto businesses are expected to implement the full suite of customer due diligence, transaction monitoring, AML program governance, and sanctions controls, while policymakers grapple with extending those expectations into decentralized and novel blockchain contexts. Below, we examine each key compliance function — customer due diligence (individual and business), transaction monitoring, AML program implementation, and sanctions screening — comparing how they are implemented in centralized exchanges, decentralized platforms, and other blockchain-based financial institutions. We also highlight the tools and technologies in use (e.g., Chainalysis, TRM Labs, Elliptic, Jumio, Sardine) and note areas where guidance is clear, versus those that remain ambiguous or in flux.

Global Regulatory Convergence vs. Fragmentation

While FATF provides a baseline, the exact implementation of crypto compliance rules varies from country to country. There is ambiguity when a business operates globally: which rules apply when, say, an exchange in Country A serves customers in Country B? By 2025, more jurisdictions had licensing regimes, so exchanges end up obtaining multiple licenses and complying with each (or geo-fencing out countries where they are not licensed). We see convergence in broad strokes (Travel Rule adoption, basic KYC/AML requirements everywhere), but differences in detail — thresholds, data privacy constraints, specific record-keeping rules.

One evolving factor is the creation of the EU's Anti-Money Laundering Authority, set to start operations by 2024/25 and directly supervise large Crypto-Asset Service Providers (among other entities). This will unify enforcement across the EU to some extent. The UK has implemented stringent crypto AML requirements (the Financial Conduct Authority's registration regime had a high bar, leading many firms to withdraw or be denied). The U.S. is considering further tightening — e.g., Congress has proposed extending the Bank Secrecy Act explicitly to digital assets in new ways, and FinCEN may revisit the unhosted wallet rule. Meanwhile, some countries are still catching up, with weaker enforcement in certain smaller jurisdictions.

Guidance is evolving, especially in developing regulations: Dubai's VARA issued comprehensive rules in 2023, including compliance requirements; and Hong Kong's 2023 regime for exchanges includes detailed AML provisions aligned with FATF standards. In summary, the direction is toward clarity and consistency. Still, in this transition period (2024–2026), crypto firms often face uncertainty about differing rules and must err on the side of the strictest applicable standard to be safe.

Global Regulatory Snapshot

Jurisdiction	Key Framework	Core Requirements
United States	Bank Secrecy Act / FinCEN MSB rules / OFAC	FinCEN registration; risk-based AML program; KYC; SAR filing; Travel Rule; sanctions screening
European Union	MiCA (2024) / 5th–6th AMLD / Transfer of Funds Regulation	CASPs as obliged AML entities; KYC/ KYB; transaction monitoring; Travel Rule ≥ €1,000 (all transfers from Dec 2024)
United Kingdom	Money Laundering Regulations / FCA registration	Full MLR compliance; Travel Rule; high FCA registration bar
Singapore	Payment Services Act	Exchange licensing with a full AML/KYC program
Japan	Payment Services Act	Exchange licensing, AML/KYC; privacy coin restrictions
Hong Kong	2023 VASP licensing regime	Strict AML obligations; FATF-aligned Travel Rule
UAE (Dubai)	VARA framework (2023)	Comprehensive licensing; AML compliance program required
Canada	FINTRAC / MSB rules	MSB registration; AML program; Travel Rule

Conclusion and Forward View

Compliance in the digital assets industry has matured significantly, especially for centralized and custodial services. In leading jurisdictions, crypto exchanges and similar businesses are expected to meet the same standards for customer identity verification, AML program governance, and sanctions compliance as banks and traditional financial institutions. As detailed, centralized exchanges have implemented comprehensive programs: verifying customer identities, vetting corporate clients, monitoring transactions with advanced blockchain analytics, filing suspicious activity reports, and rigorously screening for sanctions exposure.

These controls not only satisfy regulatory requirements but also serve to build trust and stability in the market — a critical factor after past incidents of fraud and misuse. Indeed, strong compliance is becoming a competitive advantage: exchanges with robust programs can obtain licenses more easily, attract institutional partners, and avoid the costly enforcement actions that have befallen less compliant actors.
At the same time, the industry is navigating the challenges of applying these compliance measures to the decentralized and novel facets of crypto. Decentralized finance platforms,

by design, don't fit neatly into current regulatory frameworks, leading to gaps that authorities are eager to close. The coming years will likely bring more clarity: we anticipate new regulations or guidance that will either bring certain decentralized activities under compliance obligations or foster innovative solutions (like decentralized identity tools) to meet AML goals without sacrificing decentralization.

International bodies like FATF will continue to update their standards — for example, FATF's ongoing assessments of countries' crypto regulations and its 2025 emphasis on financial inclusion show their standards are living documents, adjusting to new realities. For crypto companies, keeping up with evolving rules is as important as day-to-day compliance operations.

Where guidance is clear — such as the need for thorough identity verification or sanctions screening — there is broad industry alignment and adoption of best practices. Where guidance is ambiguous — such as in decentralized finance or non-fungible tokens — proactive firms are engaging with regulators, piloting compliance technology, and in some cases self-regulating to pre-empt stricter mandates. The period of 2024–2026 is thus one of both consolidation and transition.

From a regulator's perspective, the message to the industry is consistent: "same business, same risks, same rules." Crypto doesn't exist in a lawless void; customer due diligence, transaction monitoring, AML governance, and sanctions compliance are non-negotiable for any entity that intermediates or facilitates significant value transfer. Industry practices by 2026 reflect this reality, with compliance teams and technologies now embedded in the operations of major crypto firms.

As regulations continue to catch up to technology — and technology adapts to meet regulatory demands — we expect the gap between centralized and decentralized compliance practices to gradually narrow. Clearer guidelines and innovative compliance solutions will bring more of the digital asset ecosystem into the fold of regulated finance, aiming to deter illicit activity while still preserving the openness and efficiency that make blockchain technology transformative.

Sources: The information in this series is based on a range of industry and regulatory sources, including compliance guidance from Chainalysis, FATF and national regulations, industry analyses (e.g., Notabene on DeFi), and recent enforcement cases (OFAC settlements with Exodus and ShapeShift), among others. These provide a current (2024–2026) perspective on how customer due diligence, transaction monitoring, AML program governance, and sanctions controls are implemented and where the crypto compliance landscape is heading.

Appendix: Acronym & Abbreviation Index

The following table defines all acronyms and abbreviations used throughout this document and the AMLRS Digital Asset Compliance Series.

Acronym	Definition
AMLA	Anti-Money Laundering Authority (EU supervisory body, to begin operations 2024/25)
AMLD	Anti-Money Laundering Directive (EU; 5th and 6th iterations referenced)
AML	Anti-Money Laundering
AMLRS	AML Regulatory Series (this publication series)
BSA	Bank Secrecy Act (U.S. primary AML statute)
CASP	Crypto-Asset Service Provider (EU term under MiCA)
CEX	Centralized Exchange
CFT	Countering the Financing of Terrorism
DeFi	Decentralized Finance
DEX	Decentralized Exchange
EU	European Union
FATF	Financial Action Task Force (international AML standards body)
FCA	Financial Conduct Authority (UK financial regulator)
FinCEN	Financial Crimes Enforcement Network (U.S. Treasury bureau)
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
KYB	Know Your Business (due diligence on corporate clients)
KYC	Know Your Customer (customer identity verification)
KYT	Know Your Transaction (transaction monitoring using blockchain analytics)
MiCA	Markets in Crypto-Assets Regulation (EU, effective 2024)
MLR	Money Laundering Regulations (UK)
MSB	Money Services Business (U.S. classification for crypto firms under BSA)
NFT	Non-Fungible Token
OFAC	Office of Foreign Assets Control (U.S. Treasury; administers sanctions)
SAR	Suspicious Activity Report
UAE	United Arab Emirates
UK	United Kingdom
VARA	Virtual Assets Regulatory Authority (Dubai/UAE)
VASP	Virtual Asset Service Provider (FATF terminology)