AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 7 of 7

Emerging Risk Areas & Evolving Guidance

DeFi, NFTs, DAOs, Unhosted Wallets & Privacy Coins
AML & Sanctions Practices in the Digital Asset Industry

Areas of Ambiguity and Evolving Guidance

While much of the compliance framework for digital assets is now established, several areas remain unclear or in flux as industry practices and regulations continue to develop:

DeFi and Decentralized Protocols

This is the single biggest area of ambiguity. Regulators are still determining how to apply AML/CFT laws to decentralized systems. FATF's 2021 guidance says that "who maintains control or sufficient influence" over DeFi may be a VASP, but interpreting that in practice is difficult. The EU in 2023 indicated it might pursue activity-based regulation - regulating how DeFi interfaces with TradFi and imposing rules at those connection points rather than on autonomous code. The U.S. has not issued DeFi-specific AML regulations yet, but in April 2023 Treasury called for stronger measures to mitigate DeFi illicit finance risks. As of 2025, the industry is essentially self-regulating here, with some projects voluntarily implementing geoblocks or partnering with compliance firms (e.g., Notabene released guidance on DeFi Travel Rule compliance options). Expect evolving guidance, possibly including new definitions of "VASPs" that encompass certain DeFi participants or safe-harbor frameworks for compliant DeFi protocols. The outcome of legal cases (like the Tornado Cash sanction challenge) will also shape how far authorities can go in directly sanctioning or banning code-based services. In sum, the obligation to perform KYC/AML in DeFi is an evolving story - currently ambiguous, but unlikely to remain wholly unregulated as we move forward.

Peer-to-Peer Transactions and Unhosted Wallets

Related to DeFi, there's the question of transactions that don't involve a regulated intermediary (so-called "unhosted" wallet transfers). FATF and many governments are concerned about illicit flows through private wallets. Some jurisdictions, like Switzerland and the Netherlands, briefly flirted with requiring exchanges to verify ownership of

unhosted wallets (the so-called “wallet rule”), but this has not become widespread. FinCEN in the U.S. proposed a rule in late 2020 to require exchanges to collect counterparty information for transactions to/from unhosted wallets above $3,000, but it faced industry pushback and has not been implemented. As of 2025, the Travel Rule does not technically require information to accompany transfers to unhosted wallets, only between VASPs; however, many regulators encourage risk-based measures for such transfers (such as extra scrutiny or limits). Guidance here is somewhat unclear and inconsistent globally. We may see new due diligence requirements for unhosted wallet transactions, especially if high-profile cases show terrorists or sanctioned actors using personal wallets to circumvent controls. Exchanges are in a tough spot: they don’t want to block withdrawals to private wallets (which undermines a crypto use case), but they might be forced to implement verification or keep records to satisfy regulators in the near future.

Privacy Coins and Mixing Services

The regulatory stance on privacy-enhancing cryptocurrencies (such as Monero, Zcash, etc.) and mixers/tumblers remains evolving. Some countries (Japan, South Korea) have outright banned exchanges from listing privacy coins due to AML concerns. Others allow them but expect enhanced monitoring. The FATF has not banned privacy coins, but it reminds VASPs that they must mitigate risks. Many large exchanges have voluntarily delisted privacy coins to avoid trouble. The treatment is inconsistent worldwide, and guidance is somewhat ambiguous: are privacy coins incompatible with Travel Rule compliance? Can a VASP support them and still meet “effective” AML standards? In 2024-2025, this is still debated.

We anticipate either technological solutions (e.g. zero-knowledge protocols for proving compliance without revealing full info) or stricter rules that either ban or heavily restrict privacy coin usage on regulated platforms. Mixers like Tornado were directly sanctioned by OFAC, and the message is clear: using mixing services is high-risk. But on the flip side, EU courts have raised questions about blanket data retention rules that conflict with privacy rights - so the balance between privacy rights and AML is an evolving area of law. In practical terms, most compliant exchanges treat privacy coins and mixers with extreme caution or not at all, yet users still have access to them via unregulated channels.

NFTs and Emerging Digital Assets

Initially, NFTs (non-fungible tokens) were not seen as an AML focus, as they were mostly digital collectibles. However, as high-value NFTs can be used to move value (and cases of money laundering through NFT art sales have emerged), regulators are moving to bring NFT platforms under AML rules when relevant. The FATF’s 2021 guidance suggests NFTs could be covered if they are used for payments or investment in practice (not just for a unique art piece). The EU’s proposed AML Regulation (as of 2025 drafts) considers

including NFT marketplaces as “obliged entities” if they are intermediating transactions of a certain size. The guidance here is currently a bit ambiguous - NFT platforms are not uniformly treating themselves as VASPs, and some argue that many NFTs are outside the scope of financial regulation. Similar uncertainty exists for metaverse assets, gaming tokens, etc. - if they can be cashed out, should the platforms implement KYC/AML? Likely yes, eventually. Between 2024 and 2026, we expect clearer lines to be drawn. Industry participants in these niches are in a wait-and-see mode, but proactive ones are already looking at compliance (for example, some NFT marketplaces have started voluntarily checking large trades and reporting suspicious activity).

Global Regulatory Convergence vs. Fragmentation

While FATF provides a baseline, the exact implementation of crypto compliance rules varies from country to country. There’s 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 getting multiple licenses and complying with each (or geo-fencing out countries where they aren’t 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 (AMLA), which is ramping up operations and will be fully operational at the beginning of 2028 and directly supervise large CASPs (among other entities).

This will unify enforcement across the EU to some extent. The UK has implemented stringent crypto AML measures (the FCA’s registration regime set a high bar, leading many firms to withdraw or be denied registration). The U.S. is considering further tightening - e.g., Congress has proposed extending BSA explicitly to digital assets in new ways, and FinCEN may revisit the unhosted wallet rule. Meanwhile, some countries are still catching up (some smaller jurisdictions have weak enforcement). The industry must navigate this patchwork. Guidance is evolving especially in developing regulations - e.g., Dubai’s VARA issued comprehensive rules in 2023 including for compliance, and Hong Kong’s 2023 regime for exchanges includes detailed AML provisions aligned with FATF. In summary, the direction is toward clarity and consistency, but the current period is one of transition. Crypto firms often face uncertainty about differing rules and must err on the side of the strictest applicable standard to be safe.

Technological Solutions and Standardization

Another evolving area is the development of standards and protocols to improve compliance efficiency. For instance, messaging standards for the Travel Rule (such as the InterVASP IVMS101 data model) are now established, but ensuring that all VASPs adhere

to them is ongoing. API standards for blockchain analytics or for integrating identity verification are being discussed in industry groups. The goal is to reduce ambiguity by adopting common frameworks - if every VASP uses interoperable protocols for sharing KYC/KYB data or for Travel Rule compliance, it's easier to comply. Travel Rule still faces challenges of low rates of adoption and of interoperability, which is gradually improving through alliances and tech bridges (like Notabene's network connecting multiple Travel Rule protocols). There's also exploration of how CBDCs (central bank digital currencies) might incorporate automated compliance features, which could, in turn, indirectly set expectations for crypto. This is more speculative, but worth noting that if governments design digital currencies with built-in monitoring, they may expect similar transparency from crypto.

Clear vs. Ambiguous Guidance: A Recap

In general, guidance is clearest for centralized, intermediated activities - e.g., custodial exchanges must do KYC, KYB, KYT, etc. and regulators have published manuals and fines that make expectations plain. Where guidance is ambiguous or developing, it concerns activities that are novel to crypto's decentralized paradigm or tangential to financial services. DeFi is the prime example, as repeated above. Others are certain applications of crypto like DAOs (if a DAO provides financial services, who is responsible for AML? Currently unclear - by 2026 we may have legal precedents or new rules addressing this). We also see evolving guidance on cybercrime-related AML, such as how to treat the seizure of stolen crypto and how exchanges should handle ransomware payments (e.g., some countries might mandate blocking ransom payments, others require reporting them - not uniformly codified yet).

The industry is closely watching regulators' publications for more clarity. In late 2025, for example, TRM Labs' Global Crypto Policy Review noted that over 30 jurisdictions introduced or refined crypto compliance regulations in that year alone, signaling rapid change. Firms must stay agile and often seek legal counsel to interpret new rules. Collaboration between industry and regulators is increasing to clarify grey areas - through consultation papers, regulatory sandboxes, and industry associations (such as Global Digital Finance's working groups) that issue best-practice guidance where the law is silent.

Emerging Privacy-Preserving Compliance Technology

A forward-looking area is solutions that allow compliance checks without fully revealing personal data. Projects implementing Zero-Knowledge Proofs (ZK) for KYC are in pilot - for example, showing you are not on a sanctions list (or are over 18, or are from an allowed country) via a cryptographic proof, without revealing your exact identity. Some exchanges and DeFi platforms are interested in this to reconcile user privacy with regulatory demands. While not mainstream yet, by 2026, we may see more adoption of such decentralized identity frameworks (e.g., Polygon ID, zkKYC initiatives, ZKP-enabled travel rule data

sharing), especially in jurisdictions with strict data protection laws.
In essence, the compliance tech stack for a crypto business in 2026 consists of integrated solutions covering document verification, database screening, blockchain transaction tracking, case management, and secure data exchange - all tuned to meet the clear regulatory expectations established. The combination of these tools, when implemented properly, is now considered industry best practice and even a prerequisite to obtain licenses or banking partnerships. Many regulators assessing crypto firms will ask about which tools are in use as a quick gauge of the program's sophistication.

Conclusion

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 KYC, AML, and sanctions-compliance standards as banks and traditional financial institutions. As detailed, CEXs have implemented comprehensive programs: verifying customer identities, vetting corporate clients, monitoring transactions with advanced blockchain analytics, filing reports on suspicious activities, and rigorously screening for sanctions. These controls not only satisfy regulatory requirements but also build trust and stability in the market - a critical factor following past incidents of fraud and misuse. Indeed, strong compliance is becoming a competitive advantage: exchanges with robust KYC/AML 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. DeFi 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 DeFi 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 demonstrate that its 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 KYC or sanctions screening - there is broad industry alignment and adoption of best practices. Where guidance is ambiguous - such as in DeFi or NFTs - proactive firms are engaging with regulators, piloting compliance tech, and, in some cases, self-regulating to preempt stricter mandates. The period of 2024-2026 is thus one of both consolidation and transition: consolidation of compliance standards in the established areas of crypto finance, and

transition toward extending those standards (or creating new ones) for the next generation of crypto innovations.

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; KYC, KYB, 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 with technology - and technology adapts to meet regulatory demands - we expect the gap between centralized and decentralized compliance practices to narrow gradually. Clearer guidelines and innovative compliance solutions will bring more of the digital asset ecosystem into the regulated finance fold, aiming to deter illicit activity while 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, as cited throughout. These provide a current perspective on how KYC, KYB, KYT, AML, and sanctions controls are implemented and where the crypto compliance landscape is heading.