AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 5 of 7

# Sanctions Compliance Framework for Digital Asset Firms

OFAC, Global Sanctions Programs & Crypto Enforcement
AML & Sanctions Practices in the Digital Asset Industry

## Sanctions Compliance in the Digital Asset Industry

Sanctions compliance - ensuring a business does not facilitate transactions with sanctioned individuals, entities, or jurisdictions - is a critical and closely related component of AML for crypto companies. Due to crypto's global and pseudonymous nature, regulators worry it could be used to evade sanctions (for example, by enabling fund transfers to North Korea or Iran outside the traditional banking system). As a result, OFAC and other sanctions authorities worldwide have aggressively extended their oversight to the crypto sector, and crypto businesses have responded by implementing rigorous sanctions controls.

## Key practices and expectations include:

### Sanctions Screening of Customers (KYC) and Businesses (KYB)

As noted under KYC, exchanges screen all new customers against the major sanctions lists (e.g., OFAC's SDN list, EU consolidated list, UN Security Council list, UK's OFSI list, etc.). This is done during onboarding and routinely thereafter (since someone not sanctioned at signup could later be added to a sanctions list). Exchanges use database services (Refinitiv World-Check, Dow Jones, or various API providers) to get up-to-date lists and often leverage fuzzy matching algorithms to catch potential alias/name variations. If an individual or entity is a confirmed sanctions match, the exchange will typically block registration or freeze their account assets and report the matter to authorities, depending on legal requirements. For corporate customers, KYB includes checking the company and also its UBOs against sanctions lists. Given the U.S. "50% rule" (aggregating ownership of sanctioned persons) and similar rules elsewhere, if sanctioned persons own a significant share of a company, that company may be treated as sanctioned, so crypto firms watch out for that in KYB.

Geolocation controls are also standard: U.S.-based or compliant exchanges geo-block IP addresses from countries that are comprehensively sanctioned (Iran, North Korea, Syria, Cuba, Crimea region, etc.) and refrain from servicing users resident in those countries. Many have blocked access to their website or the app from those locales. While IP blocking isn't foolproof (VPNs can bypass it), it's a necessary measure and has been highlighted in enforcement cases (e.g., OFAC specifically faulted BitGo and Exodus for not adequately using available location data to bar sanctioned users).

## Screening of Crypto Addresses (Blockchain Sanctions Screening)

An area unique to crypto is the screening of blockchain addresses for sanctions connections. OFAC has added specific crypto addresses to its SDN List since 2018 (for sanctioned individuals and groups, such as various Iranian exchangers' Bitcoin addresses and North Korean hacker-controlled addresses). It also sanctioned entire smart contract addresses (Tornado Cash) in 2022, though this was partially challenged in court in 2023-2024.

Crypto compliance programs incorporate these addresses into their screening. Blockchain analytics tools automatically flag if an address involved in a transaction is on the OFAC list or is controlled by a sanctioned actor. For example, if a customer tries to withdraw crypto to an address associated with a sanctioned Russian entity, a good KYT system will flag or block the transaction. Exchanges also monitor exposure - e.g., if funds a customer is depositing came via a wallet that indirectly (a few hops back) received funds from a sanctioned address (like one of the OFAC-designated Tornado Cash wallets), the exchange may freeze or scrutinize those funds.

The degree of strictness varies, but U.S. regulators encourage a "zero tolerance" approach to known sanctions hits, even indirect. Some exchanges maintain custom internal blacklists of addresses linked to sanctioned jurisdictions or individuals (beyond official lists). Notably, after OFAC designated Tornado Cash, many platforms began blocking deposits originating from that mixer, treating them as potential sanctions violations.

## Preventing Access by Sanctioned Jurisdictions

In addition to IP blocking, exchanges will often disable accounts or forbid transactions involving sanctioned countries. For instance, if a user from Country X (under sanctions) were somehow onboarded, the exchange would lock the account once it was discovered. Major exchanges have off-boarded entire country user bases when sanctions expanded (for example, when new sanctions on Russia were introduced in 2022, many EU-based exchanges had to kick out certain Russian users). Custodial wallet providers like BitGo were penalized for allowing users in sanctioned regions to open wallets, even for small amounts. Now, these providers require sanctions screening for anyone who uses their services. The expectation set by enforcement is that "technical non-custodial" status is not

an excuse - if you are a U.S. company providing any service (even software or support) and you have the ability to restrict sanctioned users, you must do so. For example, after OFAC's settlement with Exodus, other Web3 developers are on notice to implement compliance measures (such as blocking certain IPs or not providing updates to users in sanctioned regions).

## Internal Controls and Training

Sanctions compliance is often handled in tandem with AML but has some distinct procedures: checking all customers and transactions against updated sanctions data daily, having escalation protocols for potential hits (which might involve legal counsel since sanctions breaches carry heavy penalties), and filing blocked property reports to OFAC if a U.S. person exchange ever holds assets of a sanctioned person. The training aspect is crucial because, as seen in the Exodus case, employees must be trained not to assist sanctioned users. OFAC noted that Exodus's staff willfully helped users from Iran evade controls (by suggesting VPNs), which was an egregious violation. Now, crypto companies train their support and compliance staff to recognize sanctions red flags and strictly avoid any advice or action that could be seen as circumventing sanctions.

## Evolving Sanctions Guidance

Sanctions in crypto have been a fast-moving area. After Tornado Cash was sanctioned, questions arose: Are all users who interacted with Tornado Cash in violation? How should DeFi protocols comply? A U.S. court (Fifth Circuit) in 2024 ruled that OFAC overstepped by sanctioning the Tornado Cash code itself, at least in part. This has introduced some ambiguity about sanctioning decentralized protocols. However, OFAC still has many tools: they continue to sanction individuals and will list any crypto addresses they use.

The lesson for industry is that even decentralized tech can become a target if tied to sanctioned actors. We've also seen sanctions used to target ransomware and hacking: entire address clusters associated with the Lazarus Group (North Korea) have been flagged in OFAC advisories. Crypto firms must therefore keep up not just with explicit list entries, but also with typologies (e.g., North Korean hackers use certain DeFi services - firms are expected to be on alert for those patterns). Globally, other countries' sanctions regimes are also applied to crypto: for instance, the EU in 2022 banned providing crypto services to Russian persons above a small value, which all EU-registered CASPs had to enforce. In practice, many global exchanges adopt the strictest common denominator: they implement U.S. OFAC sanctions screening even if not legally required in their base country, because secondary sanctions risks and future regulatory expansion make it prudent. This is why even non-U.S. exchanges often prohibit users from North Korea, Iran, and other OFAC-sanctioned regions.

## Sanctions Compliance in DeFi

As discussed, decentralized protocols cannot easily prevent sanctioned parties from using them - if a sanctioned person has crypto in a self-custodied wallet, they can trade on a DEX or use a lending protocol without revealing identity. OFAC took the extraordinary step of sanctioning Tornado Cash's smart contracts because they were being used by North Korea. While this was partially to deter usage, enforcement against individuals is still needed. DeFi front ends run by teams in certain jurisdictions have begun complying by blocking sanctioned addresses (as identified by analytics) from their UIs. MetaMask/Infura block access from sanctioned regions at the API level. But these measures are bypassable and don't cover all instances. We might anticipate new regulatory frameworks that hold certain participants (like liquidity pool operators or major liquidity providers) accountable for sanction screening, but as of 2025 this is unsettled. Law enforcement instead focuses on tracing illicit funds through DeFi and then collaborating with centralized exchanges or using chain analytics to seize funds when they eventually cross into the traditional sphere. A future possibility is deploying sanctions oracles on blockchain - for example, Circle and Coinbase's joint project "Travel Rule Universal Solution Technology (TRUST)" and other initiatives consider how to mark funds or wallets as tainted in a way that smart contracts could automatically reject them. No universal solution exists yet.

## Other Crypto Businesses

Similar to exchanges, any crypto business with a U.S. or EU nexus has to implement sanctions controls. Recent enforcement illustrates this: ShapeShift, though non-custodial at the time, was penalized $750k by OFAC in 2025 for 17,000+ transactions involving Iran, Cuba, Syria, and Sudan because it failed to screen and block those users. OFAC highlighted that ShapeShift had no sanctions program at all for years and began blocking sanctioned regions only after receiving a subpoena. The settlement stressed that even if a crypto business is foreign incorporated, if it has U.S. management or operations, U.S. sanctions law applies. So, any company in the crypto space, big or small, is expected to conduct sanctions screening and prohibit the use of sanctioned entities.

Crypto ATM operators in the U.S., for example, must ensure their machines aren't dispensing crypto to someone on the SDN list (typically by requiring identification and checking it). Mining companies have been advised that providing hash power to process transactions for sanctioned people could be a violation (a nuanced area, but some mining pools proactively filter transactions). NFT marketplaces: in 2022, OFAC sanctioned a Russian darknet marketplace (Hydra) and also an associated crypto broker - while NFTs aren't specifically addressed yet, the platforms are beginning to consider sanctions (e.g., OpenSea blocks sanctioned region IPs). As Web3 expands, sanctions controls are permeating all corners - from gaming token platforms to DAO treasury tools (a DAO that uses a centralized custodian for its treasury must ensure no sanctioned person is a beneficiary).

The sanctions compliance landscape is characterized by clear red lines (do not do business with sanctioned parties) but challenging implementation in a decentralized environment. The industry has therefore invested in tools and partnerships: Elliptic and Chainalysis both offer specialized "sanctions screening" products for crypto addresses; exchanges participate in information-sharing groups to identify evasion techniques by sanctioned entities. One encouraging sign is that analytics can often effectively de-anonymize illicit flows, making it harder for sanctioned actors to cash out without detection. OFAC, in its advisories, has praised the role of blockchain analytics in helping enforce sanctions. It has also cautioned that crypto firms must integrate all data (including IP and wallet info) into their compliance - basically urging a comprehensive approach to sanctions screening in crypto.

## Sanctions Screening and Watchlist Tools

For name screening, many crypto companies use the same systems banks use: e.g. Refinitiv World-Check, Dow Jones Factiva, Thomson Reuters screening solutions, or newer APIs like ComplyAdvantage and Sanctions.io. These consolidate global sanctions lists (OFAC, EU, UK, UN, etc.) and PEP lists so one query checks them all. They often include media searches to catch adverse news on a person (which could indicate risk even if not officially listed). Case management software like Actimize, Verafin, or SaaS tools specifically for crypto (e.g. Coinbase acquired Neutrino to build its own internal system) help manage alerts from name screening and transaction monitoring in one place, ensuring nothing is overlooked. Some exchanges have built custom screening engines optimized for transliteration variants and international naming conventions, given their user base across the globe.

## Privacy Coins and Mixing Services: An Evolving Sanctions-Adjacent Risk

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 practice, 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.

## Sanctions Compliance Comparative Summary

The table below compares sanctions controls across CEX, DeFi, and other crypto businesses:

| Dimension | Centralized Exchanges / Custodians | Decentralized Platforms (DeFi) |
|---|---|---|
| Customer Screening | All customers are screened at on-boarding against sanctions lists (OFAC, EU, UN, etc.). Accounts belonging to sanctioned individuals or entities are blocked. IP addresses and residency information are used to bar users from comprehensively sanctioned countries (e.g., no sign-ups from North Korea, Iran). Regular re-screening of customer base to catch updates. | No concept of customer identity, so the protocol cannot screen users by name or nationality. Some front-end UIs restrict access based on IP (e.g. blocking IPs from sanctioned regions) but users can often circumvent via direct blockchain interaction. There is no reliable way to prevent a sanctioned person from using a DeFi contract if they have access to it, absent community-agreed filters on the smart contract (which are rare and controversial). |
| Blockchain Address Screening | Robust address screening with blockchain analytics: transactions to/from any address on OFAC's list or linked to sanctioned entities are blocked or frozen. Exchanges subscribe to address blacklist feeds (and maintain internal blacklists). Funds traced to mixers or high-risk sources (like Lazarus Group wallets) are treated as potential sanctions issues and often frozen pending investigation. | Protocols do not inherently blacklist addresses (except in isolated cases where protocol code was updated after a sanctions event, which is extremely uncommon). Users can send tokens to/from any address. However, front-end providers and some token issuers (like USDC) maintain blacklists: e.g., USDC's smart contract will refuse to transfer tokens to certain blocked addresses. DeFi community responses to sanctioned addresses have been ad hoc (some pools manually rejecting deposits from Tornado Cash addresses post-sanctions). |
| Handling of Hits | Clear procedures: if a sanctions hit is confirmed (e.g., user is on SDN list), the account is locked, and the funds are frozen. A report is made to authorities (in the U.S., an OFAC blocking report). Often, services will also publicize that they comply (to discourage sanctioned actors from trying). Some exchanges have a zero-tolerance policy for even indirect exposure beyond a threshold - they might reject a deposit that has, say, >10% tainted funds from sanctioned sources. | Since there is no compliance department, hits are not "handled" by the protocol. The burden falls to others: a user who interacts with sanctioned addresses might later find that, when they send funds to an exchange, those funds are frozen. The protocol itself doesn't confiscate or freeze funds (unless a centralized admin key intervenes). Tornado Cash was an exceptional case where the protocol's front-end was taken down and users risk criminal liability for using it post-sanction, but the smart contracts still technically operate. This gap means sanctioned actors could use DeFi as a passthrough, and it's on regulators/analytics to detect it after the fact. |

| Dimension | Centralized Exchanges / Custodians | Decentralized Platforms (DeFi) |
|---|---|---|
| Other Crypto Businesses | Same expectations as for exchanges. Any business with a U.S./EU nexus must not transact with sanctioned parties. Wallet providers and others learned this through enforcement (e.g. OFAC fines to BitGo in 2020, BitPay in 2021, and Exodus/ShapeShift in 2025 for sanctions violations). These firms now have sanctions compliance programs: they collect at least IP or geolocation data to block access to embargoed jurisdictions, and they screen any identifiable customer data. Services like stablecoin issuers can freeze tokens for sanctioned individuals (as happened with USDT and USDC addresses). Even miners have, informally, complied (some mining pools refuse transactions to OFAC-sanctioned addresses to avoid facilitating prohibited transactions). | Consistent sanctions gap in purely decentralized operations. Regulators are studying whether developers or DAO participants could be liable for facilitating sanctions evasion, but practical enforcement in DeFi remains limited. The few exceptions are truly decentralized operations, which remain a headache for sanctions enforcement and likely targets for future regulation or technical solutions. |