AC3O

AC3O Exclusive Compliance Terms

PREMIUM INDUSTRY INSIGHTS

30 Advanced Terms for Crypto Compliance Professionals

🔒 Exclusive Industry Knowledge

This premium collection features 30 advanced compliance terms that are rarely discussed publicly but essential for senior AML/KYC professionals working in crypto and virtual assets. These insights come directly from AC3O's global compliance intelligence network.

1 Flash Governance Loop

A flash governance loop occurs when attackers use flash-loaned governance tokens to pass a malicious proposal, execute the action, and immediately unwind the position — completing the attack within a single block. These loops frequently precede protocol drains.

DeFi Attacks

2 Mixer-Sidechain Sandwiching

Sandwiching involves routing funds through a sidechain before and after mixing to complicate tracing. This technique uses differing settlement times and privacy levels across chains to hide origins.

Obfuscation Techniques

3 Wash Lending

Wash lending occurs when borrowers and lenders—often controlled by the same entity—coordinate lending and borrowing cycles to generate fake financial activity. These patterns help disguise illicit flows as legitimate DeFi usage.

DeFi Manipulation

4 Compliance Blind Spot Chains

Certain emerging blockchains have little or no AML monitoring coverage. Criminals exploit these 'blind spot chains' to temporarily store or route illicit funds before bridging back to monitored ecosystems.

Infrastructure Risk

5 ZK-Rollup Privacy Exploits

Zero-knowledge rollups offer enhanced privacy. Criminals exploit ZK-rollups for high-volume, low-visibility fund movements, making it difficult for compliance systems to trace internal rollup flows.

Layer-2 Risks

6 Algorithmic Mixer Patterns

Algorithmic mixers automatically shuffle funds based on programmed randomness. Unlike traditional mixers, they lack clear transaction rounds, producing highly irregular patterns that complicate tracing.

Advanced Mixing

7 Laundering via Synthetic Derivatives

Criminals use synthetic derivatives (tokenized futures, perpetual swaps) to convert illicit crypto into leveraged positions, later cashing out 'clean' profits while obscuring original sources of funds.

Derivatives Abuse

8 Staking Reward Laundering

Illicit funds are deposited into staking pools to generate staking rewards. These newly earned tokens appear legitimate and can be used as a secondary exit path for laundering.

Staking Abuse

9 Token Vesting Manipulation

Criminals exploit vesting schedules to hide illicit holdings by locking stolen or fraudulently acquired tokens in vesting contracts until scrutiny fades. Sudden vesting unlocks can reveal hidden laundering attempts.

Token Economics

10 Hidden Liquidity Pools

Some DeFi protocols hide secondary liquidity pools that operate outside the public UI. Criminals use these pools for private swaps, reducing visibility and evading traditional monitoring tools.

DeFi Infrastructure

11 Meta-Wallet Laundering

Meta-wallets route transactions through multiple underlying wallets controlled via a single interface. This

16 Validator Laundering Networks

Validators in proof-of-stake systems may collude to process illicit transactions privately or sequence them to avoid detection. Validator-level laundering often overlaps with private mempool exploitation.

Network-Level Risks

Attackers rotate between validator identities to evade tracking or sanctions monitoring. Rapid validator

17 NFT Mixer Mechanics

Criminals buy and sell low-value NFTs between controlled wallets to mimic mixer-like behavior. This technique launders value by disguising it as digital collectibles rather than monetary transfers.

NFT Laundering

Criminals merge multiple illicit NFTs into a single asset using smart contracts, then sell the consolidated

18 Self-Swap Laundering

Self-swaps occur when an individual swaps ass en wallets they control, typically to break traceability. Compliance systems identify self-swaps through wallet clustering, routing timelines, and counterparty overlap.

Trading Patterns

Suspicious multi-sig patterns include rapid creation of multiple multi-sig wallets, unusual signer

19 Forced Liquidation Laundering

Criminals manipulate lending platforms to trigger forced liquidations, enabling asset transfer to new wallets under the guise of market activity. Liquidation cascades can hide the origin of illicit funds.

Lending Protocol Abuse

Attackers borrow large quantities of governance tokens using flash loans to manipulate DAO votes. After

20 Unlimited Approval Exploit

Many DeFi users grant unlimited token approval to contracts. Attackers exploit compromised or malicious contracts to drain approved assets. Compliance looks for approvals to known malicious contracts as a risk indicator.

Smart Contract Risks

21 Malicious Relayer Networks

Relayers forward user transactions in meta-transaction systems. Malicious relayers obscure the origin of high-risk transfers or bundle illicit operations. Compliance tools track relayers associated with laundering clusters.

Infrastructure Abuse

22 Wash Volume Fabrication

Criminals generate artificial trading volumes across DEXs or CEXs to make illicit flows look like legitimate market-making activity. Patterns include repetitive swaps, symmetrical swap pairs, and synchronized wallet activity.

Market Manipulation

23 Token Decoy Pattern

Attackers move illicit funds through dozens of low-liquidity or worthless tokens to confuse tracing tools. These decoys create false transaction paths before funds eventually converge back into valuable assets.

Obfuscation Techniques

24 High-Frequency Laundering (HFL)

High-Frequency Laundering uses automated bots to perform hundreds of small transfers, swaps, or cross-chain movements per minute. HFL overwhelms monitoring systems and creates noise to conceal illicit patterns.

Automated Laundering

25 Bribe Networks (Blockchain)

Bribe networks allow attackers to pay validators or block producers to prioritize, censor, or reorder transactions. These networks are used to conceal exploit flows or execute laundering sequences with minimal exposure.

Consensus Manipulation

26 Timelock Bypass Attacks

Timelocks delay the execution of protocol upgrades. Attackers exploit vulnerabilities that bypass timelocks to execute instant malicious upgrades and drain funds before detection. These events create immediate high-risk laundering flows.

Protocol Exploits

27 Exploit 'Smurf Routing'

Smurf routing breaks large exploit inflows into hundreds of smaller outflows across multiple wallets to mimic natural user behavior. This technique is used heavily after protocol hacks to dilute transaction visibility.

Fund Distribution

28 DeFi Circuit Laundering

Laundering circuits involve moving funds through a repeated sequence of DeFi protocols—swap, lend, borrow, bridge—creating predictable loops designed to exhaust AML analytics.

Protocol Hopping

29 Time-Bound Laundering Windows

Criminals exploit low-activity windows (e.g., weekends, holidays, or off-peak blockchain hours) to move illicit funds when monitoring tools are less responsive. These timing anomalies are an important red flag.

Timing Analysis

30 NFT-Backed Loan Laundering

Criminals use NFTs as collateral for loans on DeFi lending platforms. After securing a loan, they move the borrowed assets through mixers or DEXs, effectively laundering value while leaving the illicit NFT locked.

Collateral Abuse