ALERT

Coordinated Digital Asset Market Manipulation and Layered Exit Typology

Synthetic Liquidity Pump-and-Exit

Purpose

The Financial Intelligence Agency Bermuda issues this alert to assist Bermuda-regulated digital asset businesses in identifying, preventing, escalating, and reporting suspected digital asset market manipulation involving coordinated account networks, artificial price or liquidity creation, rapid conversion into stablecoins, and layered off-platform exits. The typology summarised is indicative of activity being reported to the FIA affecting spot and derivatives markets, including pump-and-dump activity, wash trading, exploitation of thinly traded or low-liquidity pairs, circumvention of position limits, and manipulation of platform pricing or liquidation mechanisms. Disc-2665-26 (PROJ0073-2026)

13 August 2026

Executive Summary

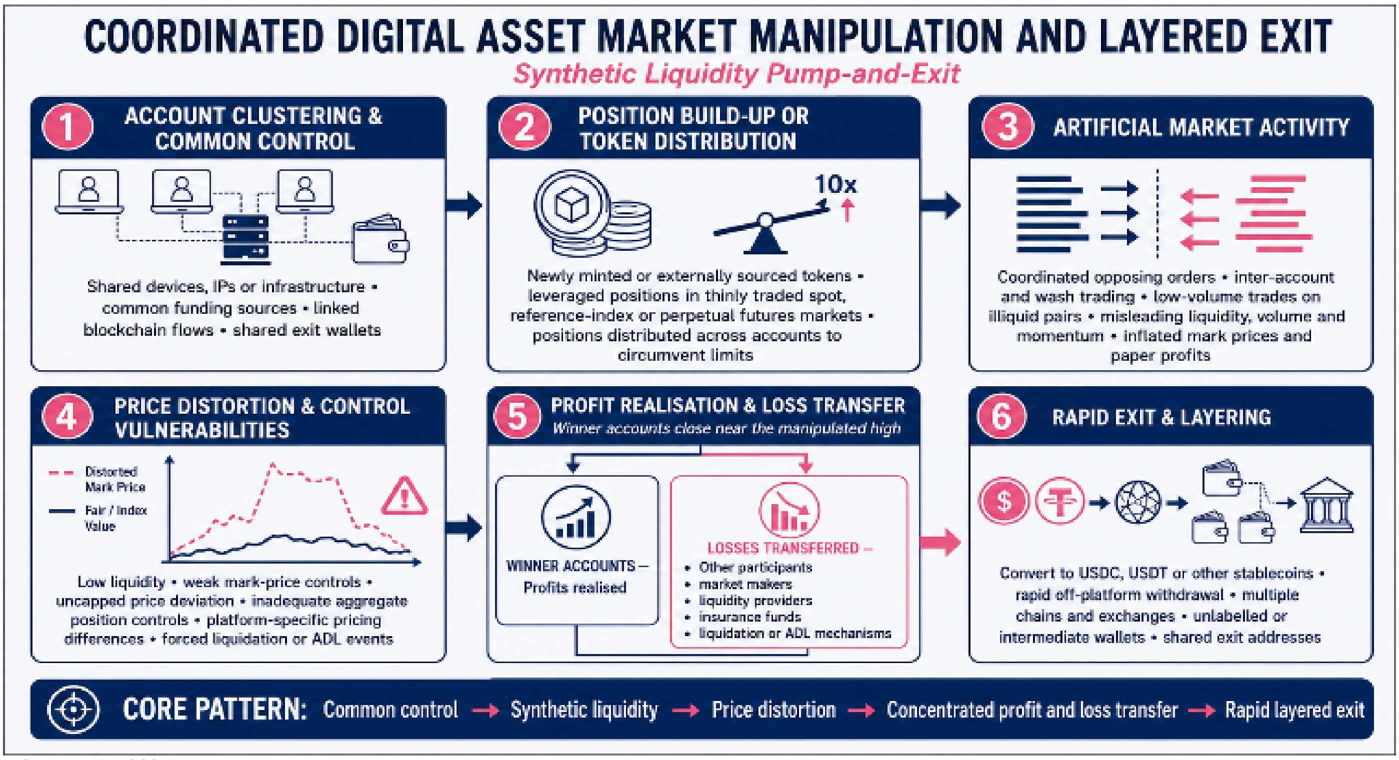
The FIA has observed conduct being reported by a small number of Bermuda-regulated digital asset businesses (DABs). Although limited, these reports, together with further anticipated reporting, anticipated, can have significant financial and market integrity impacts on digital assets associated with Bermuda. The activity involves coordinated groups opening or controlling multiple digital asset accounts, building positions in low-liquidity tokens or perpetual futures contracts, generating artificial market activity through cross-trading or wash trading, realising gains at inflated prices, and rapidly moving proceeds through stablecoins or external wallets.

In several instances, the conduct appears designed to transfer losses to retail participants, market makers, or platform risk mechanisms such as liquidation and auto-deleveraging processes. These behaviours align with known digital asset market manipulation risks identified internationally, including transaction patterns with no logical business explanation, use of multiple apparently unrelated accounts controlled through common infrastructure, unusual transaction size or frequency, and market conduct designed to mislead participants about demand, liquidity, or price discovery. To date, 3 reports have been made with potential losses up to **USD 4,308,535.00.**

Modus Operandi

1. Account clustering and common control: multiple customer accounts are opened in close succession, sometimes from the same jurisdiction, using shared device fingerprints, common IP or infrastructure indicators, shared funding sources, shared exit wallets, or linked blockchain flows.
2. Position build-up or token distribution: accounts receive newly minted or externally sourced tokens or build leveraged positions in thinly traded spot markets, reference index markets, or perpetual futures contracts, often across multiple accounts to avoid single-account thresholds or position limits.
3. Artificial market activity: accounts trade with one another, place coordinated opposing orders, execute low-volume trades on illiquid pairs or conduct wash trading to create misleading liquidity, price momentum, or volume. The activity may artificially inflate mark prices and generate paper profits on long positions before the manipulation is realised.
4. Price distortion or vulnerability exploitation: perpetrators exploit low liquidity, mark price weaknesses, uncapped price deviation, inadequate aggregate position controls, or differences between platform-specific pricing methodologies and broader market reference values to move the instrument away from its fair or

Figure 1- Typology Flow: Synthetic Liquidity Pump & Exit



Source: (FIA 2026)

index value. Artificial price inflation may trigger forced liquidations or Auto-Deleveraging (ADL) events on opposing positions, transferring systemic losses to market makers, liquidity providers, insurance funds, or platform risk mechanisms while selected accounts realize inflated gains.

5. Profit realisation and loss transfer: selected "winner" accounts close profitable positions at or near the manipulated high, while losses are transferred to other participants, market makers, insurance funds, or platform liquidation mechanisms.
6. Rapid exit and layering: proceeds are converted into USDC, USDT, or another stablecoin and moved off-platform within minutes or hours, often through multiple chains, exchanges, unlabelled wallets, or shared exit addresses.

Other Methodologies

- Spoofing and Phantom Liquidity Creation: Coordinated account networks place large, non-executable limit orders at various price levels to give the false impression of strong order book depth or demand. Once retail traders or market makers enter the market based on this synthetic depth, the manipulators cancel the orders and execute their pump-and-exit.

- Collateral Factor Exploitation: Depositing low-liquidity or newly minted tokens as collateral, artificially pumping their price to maximize borrowing capacity on the platform, borrowing major stablecoins/assets, and defaulting on the loan once the token price collapses.

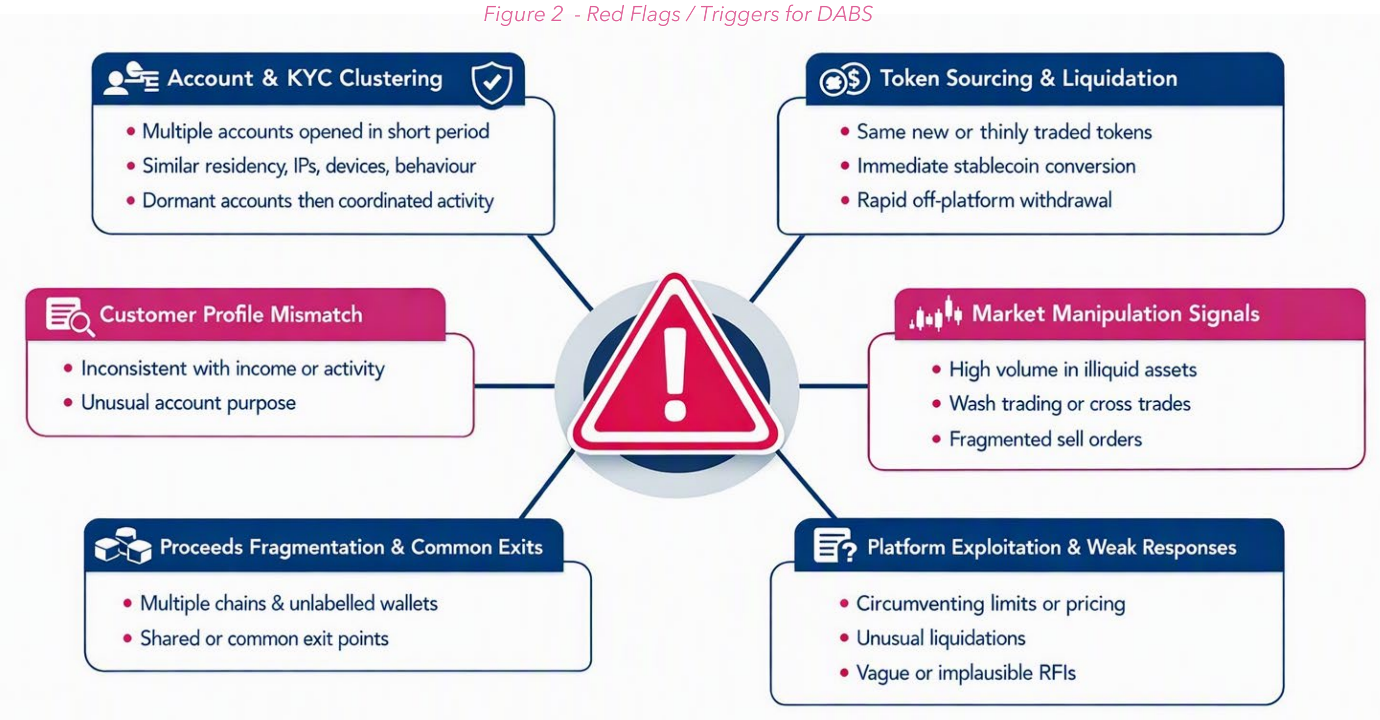
Case Indicators

- Token pump-and-dump and layered exits: multiple accounts received freshly minted tokens from a limited number of external wallets during a period in which the token increased from approximately $0.26 to $26.69 before collapsing to approximately $0.53 within 24 hours. The accounts immediately liquidated the chosen token into a stablecoin and sent proceeds off-platform, with shared or overlapping exit addresses and little evidence of legitimate trading activity.
- Syndicated account exploitation of platform controls: hundreds of accounts are registered within a concentrated window, often ranging from 20 minutes – 2 hours, pass identity verification, remain dormant for brief periods (days), and later used in a coordinated multi-phase attack on perpetual futures and spot markets. Such activity exploits mark price calculation weaknesses and low-liquidity conditions, generating profits. Reported profits have ranged from USD150k–USD3 mil.
- Per-account position limit circumvention and ADL loss transfer: The related accounts build coordinated exposure in a perpetual futures contract, including cross-trading among accounts and staged liquidation activity. Reported groups have realised gains over USD150k– USD3 mil per report to the FIA, while short-side market makers absorbed losses through an auto-deleveraging event following forced liquidation of large leveraged positions.

Potential Losses & Harm

- Direct losses to retail customers who buy at artificially inflated prices before a collapse.
- Losses to market makers or liquidity providers through manipulated liquidation events, adverse auto-deleveraging assignments, or distorted mark prices.
- Platform losses where insurance funds, market maker funds, or compensation arrangements are used to make affected participants whole.
- Money laundering exposure where manipulation proceeds are converted into stablecoins and layered through multiple platforms, blockchains, or unhosted wallets.
- Market integrity harm, including false liquidity, unreliable price discovery, reputational damage, and potential reduced confidence in Bermuda-regulated digital asset markets.
- Victims may include retail participants, market makers, liquidity providers, platform risk mechanisms, or other counterparties exposed to manipulated prices or liquidation events.
- Links were identified to foreign individuals, companies, and bank accounts, indicating broader international connections and cross-border financial activity.
- Losses ranging from USD100,000.00 – USD3million noted within received SARs/STRs.

Figure 2 - Red Flags / Triggers for DABS



Source: (FIA 2026)

Red Flags / Triggers

Account & KYC Clustering

- Multiple accounts opened in a narrow time window with similar residency, nationality, device, IP, behavioural, funding, or withdrawal characteristics.
- Accounts passing KYC but remaining dormant before coordinated high-volume trading begins.
- Positions are distributed across multiple accounts to circumvent per-account limits or avoid formal sub-account linkage.

Token Sourcing & Liquidation

- Multiple accounts receiving the same newly minted or thinly traded token from a small number of source wallets.
- Immediate sale of received tokens into USDC, USDT, or another stablecoin, followed by rapid withdrawal off-platform.

Customer Profile Mismatch

- Trading activity inconsistent with the customer's income, source of wealth, occupation, stated account purpose, or previous trading history.

Market Manipulation Signals

- High-volume trading in low-liquidity instruments without any identifiable public catalyst such as a listing, product launch, governance milestone, or market-wide news.
- Cross-trading, wash trading, or opposing orders between accounts with common indicators of control.
- Repeated small tranches or fragmented sale orders that appear designed to avoid detection or obscure aggregate liquidation.

Proceeds Fragmentation & Common Exits

- Use of multiple blockchains, unlabelled wallets, or external exchanges to fragment proceeds after liquidation.
- Shared exit wallets, shared intermediate wallets, or common off-ramp addresses across nominally unrelated customers.

Platform-Control Exploitation & Weak Explanations

- Circumvention of per-account position limits by distributing positions across multiple accounts that are not formally linked as sub-accounts.
- Sudden or material divergence between a platform's mark price, index methodology, or internal reference price and broader market fair

value, particularly where the methodology relies on thinly traded perpetual futures contracts, spot pairs, or platform-specific inputs that can be influenced by coordinated low-volume trading.
- Unusual liquidation or auto-deleveraging events that transfer losses to market makers or other third parties while related accounts retain gains.
- Non-responsive, generic, or implausible responses to requests for information, particularly where "arbitrage" is claimed but trading is one-directional or inconsistent with genuine arbitrage.

Mitigating Measures

- Improve monitoring of account-clustering models using device fingerprinting, IP intelligence, behavioural analytics, wallet linkage, funding patterns, and withdrawal destinations.
- Apply aggregate position limits across accounts assessed to be under common control, not only formal sub-accounts.
- Introduce hard caps or circuit breakers where mark prices diverge materially from external index prices or reference markets.
- Regularly review newly listed, newly minted, low-liquidity, or thinly traded tokens and pairs for abnormal price, volume, concentration, and liquidity patterns, and consider delisting or restricting vulnerable pairs where appropriate. Establish contextual triage protocols that distinguish legitimate high-frequency market making or cross-venue arbitrage from synthetic liquidity creation, including one-directional volume that tolerates slippage or economic loss to move mark prices, trade activity without offsetting cross-market hedge positions, and generic or non-responsive arbitrage claims that conflict with underlying trade telemetry.
- Detect wash trading and cross-trading through common beneficial ownership, common infrastructure, mirrored order timing, repeated self-matching, and circular trade patterns.
- Use velocity rules for rapid token receipt, conversion to stablecoin, and withdrawal off-platform.
- Require enhanced due diligence and supporting evidence where customer activity materially exceeds stated income, wealth, occupation, or expected use.
- Set automated alerts for newly funded accounts that rapidly withdraw profits, especially where initial funding and withdrawal amounts are near-identical across multiple accounts.
- Ensure incident response playbooks allow quick coordination between compliance, surveillance, engineering, treasury, legal, and senior management.
- Conduct post-incident reviews to close technical vulnerabilities, including mark price methodology, liquidity controls, liquidation mechanics, and ADL design.

Recommended Immediate Action

1. **Escalate internally:** immediately refer suspected coordinated manipulation to compliance, financial crime, market surveillance, and senior risk personnel.
2. **Preserve evidence:** retain order book data, trade logs, device fingerprints, IP logs, customer communications, KYC files, wallet addresses, blockchain analytics, RFIs, and withdrawal records.
3. **Assess common control:** review shared devices, shared IPs, related wallet flows, identical trade timing, common funding sources, coordinated withdrawals, and linked beneficiaries.
4. **Intervene promptly:** consider pausing withdrawals, freezing affected balances where permitted, restricting trading, limiting leverage, disabling vulnerable pairs, or placing accounts under enhanced monitoring.
5. **Review market integrity controls:** assess whether mark price methodology, index controls, price deviation caps, aggregate position limits, wash-trade controls, and liquidation/ADL mechanisms performed as intended.
6. **File suspicious activity reports:** where suspicion is formed, submit a SAR/STR to the relevant FIU without delay and include all relevant account identifiers, wallet addresses, linked entities, chronology, loss estimates, and supporting evidence.
7. **Notify relevant regulators where appropriate:** consider parallel notification to supervisory or regulatory authorities in accordance with licensing, market conduct, and incident reporting obligations.

Conclusion

The analysis of the identified fraud typology highlights a highly coordinated and evolving scheme. Bermuda-regulated digital asset businesses should treat suspected coordinated market manipulation as both a market integrity and financial crime concern. Where a DAB knows, suspects, or has reasonable grounds to suspect that funds, trades, accounts, or wallets are connected to criminal conduct, fraud, manipulation, money laundering, or attempted laundering, the matter should be escalated and reported to the FIA in accordance with applicable obligations.

-END

Statistical Disclaimer: The report's statistics are based on SARs and STRs submitted to the FIA between April 1, 2026 – July 28, 2026. These reports reflect suspicions from reporting entities and do not confirm the existence of criminal activity. The data is intended for analysis and may change as new information or investigations arise. While reasonable steps are taken to ensure accuracy, the FIA relies in part on information provided by reporting entities and other third parties and cannot independently verify all underlying data. Disclosure-xxxx-26 (PROJ0073-2026)