When $400,000 Is Worth $1: Token Valuation in Li v Shen

November 26, 2026

A dollar sign on a trading app is not a dollar. That distinction is easy to ignore while withdrawals are open, and fatal in court once they close.

In *Li v Shen; Shen v Li* [2026] NSWDC 380 (21 October 2026), Judge Andronos SC of the District Court of New South Wales addressed a problem that recurs across distressed crypto platforms: how a court values illiquid platform tokens when a counterparty breaches an obligation to return them. The plaintiff ("Susan") transferred tokens with a face value of US$400,000 on the "AEGlobalLink" platform to accounts controlled by the defendant ("Ashley") as a short-term loan. Ashley refused to return them. Susan prove d a binding contract and proved breach (para.47). She was awarded US$1.00 in nominal damages, and ordered to pay Ashley US$101,000 on a cross-claim for actual fiat loans (para. 67).

The judgment turns entirely on how common-law damages principles value non-fiat digital assets. Four legal tests governed the outcome.

1. **The "Money" Test: Liquidity Defines Classification**

Because Susan sued in damages rather than debt (para. 11), the threshold question was whether the transferred platform credits were "money" or an "asset." If they were money, the loss was US$400,000. If they were an asset, "that asset must be identified and valued" (para. 50).

Applying *Moss v Hancock* [1899] 2 QB 111 and *Re Collings* [1933] Ch 920, the Court applied a strict liquidity test. Money "confers complete liquidity on its holder" and is "that which

passes freely from hand to hand throughout the community in final discharge of debts and full payment for commodities," including bank deposits (para. 51).

Platform balances failed on every count:

"What Susan transferred to Ashley on 28 March 2023 was not money. It was not a generally accepted medium of exchange and it did not confer liquidity on its holder. It could not pass freely from hand to hand throughout the community in final discharge of debts and full payment of commodities. The Platform was not a bank." (para. 52)

Displaying a USD figure on a mobile interface (para. 21) does not convert a closed-ledger credit into currency.

2. **The Secondary-Market Test: Proof of Buyers and Price at Breach**

AE Global Link Seychelles-registered operator was dissolved in 2022, ASIC issued an unlicensed-entity warning, its web domain changed three times, and a July 2024 platform notice admitted it had been "designated as a pyramid scheme case by the mainland GA in September 2021" (para. 23). Withdrawals had been frozen since at least early 2023 (para. 24).

Notably, the Court did not rely on a finding of fraud to value the tokens at zero. Judge Andronos SC noted that "[i]f it were a scam, the Court could not ascribe any value to trading it as an asset," but proceeded on the assumption, in Susan's favour, that the platform was legitimate (para. 53). Even on that generous premise, valuation required hard market evidence as at the date of breach:

- **Internal trading price:** Where fiat withdrawals are blocked, "the tokens could only have value, as at the time of the breach, referable to the price at which they could be traded internally on the Platform. Such a price would need to be the subject of evidence" (para. 53).

- **Willing-buyer proof:** “In addition to establishing the existence of a market, Susan would need to establish the existence of a buyer or buyers willing to acquire the tokens and the price at which they might be prepared to do so, given the illiquidity of the asset. There was no such evidence” (para. 53).

Without verifiable secondary-market pricing or proof of a willing buyer, illiquid tokens carry no provable market value.

3. **The Contingent-Redemption Test: No Valuation by Speculation**

Holders of frozen platform balances routinely argue that their tokens retain value because withdrawals may eventually resume. The Court rejected speculative future-value arguments outright:

“However, if an investment’s value is entirely contingent on a highly unpredictable future event, it is impossible to assign a positive value to it without speculating.” (para. 54)

Susan and a supporting witness both honestly believed the platform remained viable (para. 21). Subjective belief is irrelevant to valuation. Because there was no evidence of “the likelihood that the funds have been retained by the Platform” or “if, and when, it might have been expected, as at April-June 2023, that tokens could be redeemable in the future for actual US dollars,” the Court refused to assign a positive figure (para. 55).

4. **Compensatory Limits: Nominal Damages and In-Specie Return**

Contractual damages are strictly compensatory: they place the claimant “in the same situation, with respect to damages, as if the contract had been performed” (para. 49). Had Ashley performed in June 2023, Susan would have received unredeemable tokens with no proven market price. Consequently, breach

produced no compensable financial loss, restricting recovery to “nominal damages, which I have assessed in the customary amount of US$1.00” (para. 57).

That valuation also decided the rest of the case. Susan’s defence to Ashley’s US$80,000 cross-claim relied on offsetting her US$400,000 token claim against the fiat debt (para. 60). With the tokens valued at zero, no set-off existed, leaving Susan liable for A$101,000 inclusive of pre-judgment interest (para. 67). To address the remote chance that the platform ever unlocks, the Court simply noted Ashley’s formal undertaking to “do what is reasonable to transfer the same Tokens back” if transfers ever become possible (paras. 58–59).

Li v Shen draws a clear line for digital asset disputes. Courts will not convert a frozen, illiquid platform balance into a fiat judgment on the strength of a screen display. Unless a claimant can prove either a functioning secondary market with willing buyers or a non-speculative path to fiat redemption, a breach of contract over locked tokens is worth one dollar.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Crypto Mining Power, AI Evidence, and the Shelf of

Death: Six Legal Tests from One Purpose v DMG Blockchain

November 26, 2026

Digital asset operators may treat legal documentation as an administrative afterthought, assuming industry norms or chat-app assurances will fill the gaps if a counterparty underperforms. Courts take the opposite view. As cross-border crypto commentary from Wasel & Wasel has consistently noted, from Canadian authorization disputes like *HoneyBadger Enterprises Ltd. v Bue* to regional analyses of WhatsApp-based crypto deals, judges do not treat digital asset litigation as legally exotic. Established contract, fraud, and evidentiary doctrines govern, and written risk allocation controls.

One Purpose Corp Limited v DMG Blockchain Solutions Inc. (2026 BCSC 2133), decided on November 3, 2026, by Justice Hoffman of the Supreme Court of British Columbia, applies that principle directly to cryptocurrency mining infrastructure. Dismissing all claims brought by Ether miner One Purpose against hosting provider DMG and two of its executives, the judgment distills six legal tests that every hosting operator, miner, and digital asset counsel should understand.

Fraudulent Misrepresentation: Present Fact vs. Deployment Schedules

To prove fraudulent misrepresentation under *Catalyst Pulp* and *Wang v Shao*, a claimant must establish five elements: a representation of fact, falsity, knowledge of falsity or recklessness, intent to induce action, and actual reliance (para. 82). While there is “no heightened standard of proof merely because the claim sounds in fraud,” the evidence must still be “sufficiently clear, convincing, and cogent” under *F.H. v McDougall* (para. 86).

For crypto infrastructure disputes, two constraints within this test prove decisive:

- **The Entire Agreement Barrier:** One Purpose relied heavily on a post-contract internal email from DMG's CTO noting that "[e]xpectations were set by James [McDowall] that we had open shelf space and that we would have miners online as soon as they arrived at our facility" (para. 90). Yet informal chats cannot override contract architecture. Because One Purpose never secured a written timeline and signed an "entire agreement" clause disclaiming external representations (para. 100) and admitted on discovery that it had no other suitable global hosting options, both representation and reliance failed (paras. 102–105).
- **Forward-Looking Schedules Are Not Representations of Fact:** Under *PD Management*, actionable statements "must relate to a past or presently existing state of facts" (para. 84). A future rollout schedule is only actionable under *Pan v Dong* if "it can be demonstrated that the party making it did not have the intent to carry out that conduct" when made (para. 84). Because DMG pivoted to temporary stacks and racked 985 miners within two weeks of its target date, with the shortfall largely explained by defective rigs, including non-operable units relegated to what technicians called the "shelf of death" (paras. 112–114, 117), Justice Hoffman was "unable to conclude that, when the schedule was provided, DMG had no intention of attempting to meet it" (para. 118).

Good Faith Is Not a Fiduciary Duty, And Liability Can Be Capped

Relying on the Supreme Court of Canada's trilogy (*Bhasin*, *Callow*, and *Wastech*), One Purpose argued that unanswered emails, electrical buildout deliberations, and DMG's shift toward self-mining breached the duty of good faith and honest

performance (para. 120).

Justice Hoffman drew the exact statutory and common-law boundaries of that doctrine:

- **No Duty to Subordinate Self-Interest:** Good faith requires performing contractual duties "honestly and reasonably and not capriciously or arbitrarily" (para. 122), and *Callow* prohibits "failing to correct a misapprehension created through its own misleading conduct" (para. 123). However, the duty "does not impose either a duty of disclosure or the loyalty required of a fiduciary. Nor is a party required to subordinate his or her own interests to those of the other party" (para. 124).
- **Internal Deliberations Are Not Deception:** Even an internal August 2020 email from DMG's former CEO proposing to "boot Brad [Yasar] (or increase his hosting cost) as he must be making a ton of money right now, to make more room at CL" did not breach honest performance (para. 159). As the Court held, "DMG had no duty to disclose its internal deliberations to One Purpose or its views of One Purpose as a client" (para. 163).
- **No Free Upgrade to Tiered Service:** Many of One Purpose's complaints amounted to "assertions that DMG failed to provide One Purpose with a level of service that One Purpose neither bargained nor paid for under the terms of the Hosting Agreement" (para. 156). Maintenance was optional and separately billed under Clauses 3.2 and 6; unpaid goodwill repairs did not create a perpetual obligation (paras. 133–138).
- **Limiting Damages for Bad Faith:** In *obiter*, Justice Hoffman cited *1401380 Ontario Limited (Wilderness North Air) v Hydro One Remote Communities Inc.* (2025 ONCA 827) for a point of immediate drafting utility: "while parties are not permitted to exclude the duty of good faith through contractual terms, they remain free to

construct contracts to limit the scope of their liability for breach of the duty" (para. 165).

"Reasonable Endeavours" Requires Proof of Industry Practice

Mining hosting agreements commonly dilute uptime guarantees into "reasonable endeavours" clauses. Under *Atmospheric Diving Systems* and *1092369 Alberta Ltd.*, reasonable efforts impose a lesser standard than "best efforts," requiring only a "prudent and moderate measure of sustained diligence" (para. 171).

Critically, Justice Hoffman applied *Banque Indosuez v Canadian Overseas Airlines*: "to establish a breach of a reasonable endeavours obligation under a contract, the onus lies on the party alleging the breach to lead evidence to establish the industry practice against which the conduct in question can be judged" (para. 172). Because One Purpose "did not call any evidence to establish industry practice for non-tiered hosting facilities," its contract claims on power, connectivity, security, and maintenance failed on the evidentiary record alone (para. 173).

Technical Notice Breaches Yield Zero Damages Without Causation

DMG committed one undisputed contractual breach: Clause 10.1 required 60 days' termination notice, but DMG's June 28, 2021, letter mistakenly stated 15 days (paras. 158, 174). In commercial litigation, however, a technical breach is inert without causal loss. Because DMG granted One Purpose's request for additional time and provided its own staff to help pack the rigs through mid-August 2021, Justice Hoffman found she was "not satisfied that any loss has been proven to flow from the deficiency in the notice provided" (para. 174).

Missing On-Chain Records and Adverse Witness Inferences

Where memories fade, courts test testimony against "the preponderance of the probabilities which a practical and informed person would reasonably see as arising in the

relevant context" (*Faryna v Chorny*, para. 48). One Purpose failed to produce core operational records, including "mining pool records, financial statements, business plans, financial projections, tax records," written equipment warranties, and its own AirTable repair log (paras. 63, 80, 117).

Equally instructive is the Court's application of *Gondor v British Columbia (Attorney General)* (2025 BCCA 281) to One Purpose's decision not to call its owner, Adam Melton, who lived outside the Court's subpoena power in Washington State (paras. 73, 77). Because a party bears its own burden of proof and Melton was practically accessible to One Purpose, Justice Hoffman exercised her discretion to draw an adverse inference: "I infer that Mr. Melton's evidence would not have assisted One Purpose in establishing its reliance on the alleged misrepresentations or its alleged mine and hold strategy" (para. 79).

Unverified AI-Generated Litigation Aids Carry No Evidentiary Weight

Finally, the decision offers a clear 2026 rule of thumb on artificial intelligence in the courtroom. During trial, DMG's CTO used AI to synthesize disclosure and trial testimony into Excel spreadsheets tracking facility capacity and miner rollout, and "acknowledged that he did not independently verify the AI-generated document against the source information" (para. 70). Justice Hoffman excluded it from her fact-finding: "As an after-the-fact consolidation of information from multiple sources, this document has limited evidentiary value. I have not relied on these spreadsheets to make any factual determinations" (para. 70).

The Bottom Line for Digital Asset Investors

One Purpose v DMG Blockchain reduces complex mining litigation to a clean commercial checklist. Informal chat assurances will not bypass an entire agreement clause; reasonable-endeavours provisions cannot be litigated without expert evidence of non-

tiered industry benchmarks; limitation-of-liability clauses can be drafted to cap even good-faith exposure; and neither missing mining-pool logs nor unverified AI spreadsheets will survive judicial scrutiny. In digital asset infrastructure, the margin between a viable claim and a costs award is built in the contract, and preserved in the records, long before the rigs go offline.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

War Series: Letters of Credit in the Crossfire – Sanctions Clauses, Frozen Reimbursements, and the Erosion of UCP 600 Autonomy

November 26, 2026

Global trade runs on physical molecules and sovereign plumbing. When the custodians of the plumbing weaponize access, no amount of standardized paper can force a payment to clear.

For nearly a century, international commerce has operated on a disciplined legal fiction: the autonomy of the documentary credit. Under Articles 4 and 5 of the International Chamber of Commerce's Uniform Customs and Practice for Documentary

Credits (UCP 600), banks deal exclusively in documents, never in the underlying goods, commercial disputes, or geopolitical grievances of the trading parties. Present a spotless bill of lading, a compliant commercial invoice, and a valid insurance certificate, and the confirming bank is irrevocably bound to pay. In theory, a confirmed letter of credit (LC) is the closest equivalent to cash in cross-border trade.

In practice, that bedrock guarantee is quietly disintegrating.

As the 2026 Middle East conflict disrupts physical shipping lanes and accelerates the weaponization of financial clearing networks, the autonomy principle is colliding with a far more potent force: the extraterritorial reach of sovereign sanctions and the retaliatory blocking statutes erected against them. Exporters are confronting a harsh operational reality. A complying presentation under UCP 600 no longer guarantees settlement when the bank holding the reimbursement instructions fears regulatory exile in Washington, or faces statutory retaliation in Beijing.

The market is witnessing the structural erosion of neutral trade finance. What was once a mechanical, document-driven settlement engine has mutated into a contested geopolitical arena where banks price regulatory survival far above contractual certainty.

The Plumbing Beneath the Paper

To appreciate the magnitude of this fracture, one must examine the underlying mechanics of global trade settlement rather than the idealized prose of trade rules. According to the Asian Development Bank's Global Trade Finance Gap Survey, unmet global demand for trade finance stands at $2.5 trillion, roughly 10% of global merchandise trade. More revealing than the headline figure is its migration up the corporate food chain: rejection rates for mid-cap and large corporate borrowers surged from 30% in 2023 to 40% in the latest survey

cycle.

This contraction is not a shortage of global capital; it is a crisis of financial plumbing. Roughly 80% to 85% of global trade finance transactions remain denominated in U.S. dollars. Every dollar-denominated LC, whether issued in Dubai to finance industrial inputs or confirmed in Singapore to settle petrochemical flows from the Arabian Gulf, must ultimately clear through correspondent accounts anchored in the United States. The architecture is inherently hierarchical. UCP 600 may be politically neutral, but the banks that animate it are anything but.

The ICC Global Banking Commission has fought a valiant rearguard action to preserve the integrity of its rules. In its Consolidated ICC Guidance on the Use of Sanctions Clauses (revised in November 2024), the ICC cautioned financial institutions that sanctions clauses should not be inserted routinely, should refrain from unparticularized references to foreign laws, and should avoid referencing internal "bank policy and procedure" at all times. Similarly, in its April 20, 2026 guidance on the Middle East conflict, the ICC urged market participants to continue applying UCP 600, URDG 758, and URC 522 in the usual manner despite operational disruptions.

Industry guidance, however, carries neither statutory force nor the power to revoke a banking charter. When a compliance committee weighs a non-binding ICC recommendation against a U.S. Treasury enforcement action, the math is brutally straightforward.

The 2026 Gulf Stress Test: Kinetic Disruption Meets Dollar Chokepoints

Nowhere has this divergence between physical logistics and financial compliance been more acute than across the Gulf Cooperation Council (GCC) in 2026. Following the February 28,

2026 escalation of hostilities and severe disruption in the Strait of Hormuz, annual marine war-risk cover vanished into voyage-by-voyage pricing. According to a Howden Re market report, Gulf transit war-risk premiums jumped up to 12-fold in the opening weeks of the conflict, reaching 2% to 3% of insured vessel value, while Lloyd's List reported single-voyage war-risk cover topping $10 million for a very large crude carrier by July. After crude oil breached $100 per barrel in September, credit insurer Coface issued its October 13, 2026 Risk Review, downgrading country-risk ratings for Saudi Arabia (A3 to A4), the UAE (A2 to A3), and Qatar (A3 to A4) due to energy-infrastructure and Strait of Hormuz exposure.

For trade finance operations, the shock struck on two simultaneous fronts.

First, physical rerouting began generating documentary discrepancies at scale. As vessels diverted away from Gulf ports toward alternative Red Sea and east-coast gateways, legacy LCs naming a single port of discharge or imposing rigid 14-day presentation windows suddenly failed strict documentary compliance, handing risk-averse banks a clean contractual off-ramp to refuse payment.

Second, and far more consequential, Washington tightened the correspondent banking vise. On August 24, 2026, U.S. Treasury Secretary Scott Bessent launched "Operation Economic Outcast," expanding secondary sanctions risk under Executive Order 13902 across Iran's shipping, aviation, gold, technology, and digital-asset sectors, as reported by the Associated Press. The enforcement cadence that followed left zero ambiguity for regional lenders:

- On August 28, 2026, the U.S. Treasury moved to sever U.S. correspondent banking access for Banque Misr UAE, alleging the bank processed approximately $1.8 billion for 103 companies potentially tied to Iranian shadow

banking networks.

- On September 4, 2026, Treasury designated Türkiye-based Golden Global Bank and two subsidiaries for providing correspondent banking access tied to Iranian oil revenue channels.
- On September 14, 2026, Treasury designated Russia's VTB Bank under E.O. 13902 for establishing correspondent accounts and national-currency settlement mechanisms with sanctioned Iranian banks.
- On October 5, 2026, the Office of Foreign Assets Control issued an explicit OFAC Alert to Foreign Financial Institutions, warning that non-U.S. banks facilitating Iranian financial channels or commodity-linked shadow banking face direct sanctions and potential civil or criminal enforcement.
- On November 23, 2026, Treasury escalated further, sanctioning over two dozen additional Iranian exchange houses, front companies, and operatives after FinCEN identified nearly $15 billion in potential Iranian shadow banking activity between January 2025 and August 2026.

The second-order effect was immediate and entirely predictable. International confirming banks curtailed regional limits, repriced confirmation margins, and leaned heavily on sweeping sanctions exclusion clauses. When a regional trade flow touches a transshipment hub, an opaque vessel charterer, or a third-country intermediary, the correspondent bank's rational survival instinct is to freeze first and litigate later.

The Tripartite Fracture: London, Singapore, and Beijing

If global courts shared a unified doctrine on how sanctions interact with documentary credits, market participants could at least price the exposure. Instead, the three premier legal arenas governing cross-border trade, London, Singapore, and China, have fractured into irreconcilable camps.

London: Statutory Supremacy Over Contractual Autonomy

On March 25, 2026, the UK Supreme Court delivered a watershed decision in *UniCredit Bank GmbH, London Branch v Celestial Aviation Services Ltd* [2026] UKSC 10 that permanently altered the calculus for English-law credits. The dispute arose out of standby letters of credit originally issued by Russia's Sberbank and confirmed by UniCredit's London branch to secure aircraft leases for Russian airlines. When the UK amended Regulation 28(3)(c) of the Russia (Sanctions) (EU Exit) Regulations 2019 to classify aircraft as restricted goods, UniCredit withheld payment until securing regulatory licenses.

The lessors invoked the autonomy of the credit, contending that payment demands under the confirmations were legally distinct from the underlying leases. A unanimous Supreme Court rejected that argument. Delivering the judgment of the Court, Lord Stephens confirmed that statutory sanctions cast a deliberately wide net: "in connection with" captures a broad factual link to a prohibited arrangement, suspending payment obligations even where the underlying leases and credits predated the sanctions.

More dramatically, the Supreme Court held that Section 44 of the Sanctions and Anti-Money Laundering Act 2018 (SAMLA) operates as a comprehensive civil-liability defense. Where a bank withholds payment in the *reasonable belief* that doing so is required to comply with UK sanctions, Section 44 shields the bank not only from statutory interest and legal costs, but from the underlying debt claim itself while the freeze persists. In London, statutory compliance now sits behind a reinforced bunker, leaving beneficiaries to absorb the financing cost of immobilized working capital while banks await ministerial licensing.

Singapore: Strict Scrutiny of Precautionary Compliance

Across the Indian Ocean, Singapore has drawn a far sharper

line in defense of mercantile certainty. In *Kuvera Resources Pte Ltd v JPMorgan Chase Bank, N.A. [2023] SGCA 28*, a confirming bank refused to honor complying drafts after internal screening flagged circumstantial evidence suggesting the carrying vessel had a Syrian beneficial ownership nexus.

The Singapore Court of Appeal reversed the High Court and ruled squarely against the bank. Delivering the judgment, Justice Steven Chong emphasized that contractual interpretation, not geopolitical risk aversion, governs a sanctions clause embedded in an irrevocable confirmation. The Court rejected the bank's reliance on subjective risk-management assessments and inconclusive circumstantial indicators, holding that a confirming bank must discharge an objective evidentiary burden demonstrating that payment would *actually* violate applicable sanctions. Precautionary de-risking, the exact reflex incentivized by Washington's enforcement posture, does not excuse non-performance under Singapore law.

Beijing: Turning Western Overcompliance into Civil Liability

If London shields precautionary freezes and Singapore constrains them, Beijing actively penalizes them. Following the State Council's March 2025 regulations implementing China's Anti-Foreign Sanctions Law (AFSL), Beijing expanded its legal counter-sanctions apparatus aggressively throughout 2026. On April 7, 2026, China promulgated State Council Order 835, establishing broad regulations to counter improper foreign extraterritorial jurisdiction. Less than a month later, on May 2, 2026, China's Ministry of Commerce invoked its 2021 Blocking Rules for the first time, issuing a formal prohibition order barring compliance with U.S. sanctions targeting five Chinese refineries accused of importing Iranian crude, as reported by Al Jazeera and Reuters.

The judicial enforcement mechanism followed swiftly. On June 24, 2026, China's Supreme People's Court released six

representative maritime cases of 2025, highlighted by China Law & Practice as the first Chinese court judgment applying the AFSL to reject foreign sanctions compliance as a defense for contractual breach. In that Shanghai Maritime Court ruling, a carrier that halted performance out of fear of U.S. restrictions was ordered to pay full cargo damages plus interest notwithstanding foreign choice-of-law terms. For an international bank confirming an LC involving a Chinese supplier or consignee, invoking a broad U.S.-centric sanctions clause to suspend reimbursement no longer merely invites a commercial dispute; it invites mandatory domestic statutory liability against onshore assets.

The Asymmetric Mechanics of Frozen Reimbursements

Examine the resulting vise from the seat of a global trade-finance bank operating across the Dubai–Singapore–Shanghai–London corridor. The incentives are hopelessly asymmetric:

1. **Pay against a shadow-sanctioned nexus:** Risk losing U.S. dollar correspondent clearing privileges under Operation Economic Outcast, an existential threat for any internationally active lender.
2. **Freeze payment on precautionary grounds:** Claim statutory immunity in London under *UniCredit* if UK sanctions are plausibly engaged, face a breach-of-confirmation judgment in Singapore under *Kuvera* if the evidence is merely circumstantial, and trigger statutory countermeasures and damages exposure in China under the AFSL and MOFCOM blocking orders.

Caught between these grinding tectonic plates is the exporter. A commodity trading house in Dubai or Singapore can load compliant physical cargo, present faultless UCP 600 documentation, and watch its reimbursement vanish into an indefinite compliance limbo, no formal dishonor, no statutory interest while a licensing application sits in a ministerial

queue, and no assurance that dollar clearing through New York will resume. The autonomy of the letter of credit has not been formally repealed; it has been hollowed out from within by the sovereign plumbing required to settle it.

The Wartime Playbook for Trade Finance

Wishing for a return to unipolar financial neutrality is not a risk-management strategy. For commodity traders, corporate treasurers, and financial institutions operating across high-friction corridors, protecting working capital requires redesigning trade-finance documentation for a multipolar order:

- **Audit Sanctions Clauses Before the Vessel Sails:** Beneficiaries must stop treating confirming-bank sanctions clauses as harmless boilerplate. Insist on objective, narrowly tailored wording tied strictly to *mandatory statutory illegality* in the place of payment, explicitly rejecting discretionary "internal bank policy" carve-outs in accordance with the ICC's revised Guidance.
- **Engineer Routing Resilience Into the Credit:** In active maritime conflict zones, single-port discharge terms and 14-day presentation windows are self-inflicted wounds. Structure credits with regional port ranges (permitting discharge across designated east-coast GCC or Red Sea gateways), explicit transshipment permissions, and extended presentation windows so wartime diversions do not gift counterparties a technical discrepancy defense.
- **Build Multi-Currency Fallback Mechanisms:** With 58% of surveyed banks reporting rising demand for local-currency trade finance, relying exclusively on single-correspondent USD clearing creates a fatal single point of failure. Embed pre-agreed fallback settlement rails (such as AED, EUR, or CNH) and alternative clearing banks in the underlying sales contract, triggered automatically if USD correspondent clearing is suspended

without a primary sanctions violation.

- **Ring-Fence Licensing Delays and Financing Costs:** Following *UniCredit v Celestial*, beneficiaries cannot assume statutory interest will accrue while a confirming bank awaits regulatory licensing. Negotiate express covenants requiring the applicant (buyer) to bear carrying costs, demurrage, and direct alternative-payment obligations if LC reimbursement is suspended due to regulatory screening delays unrelated to the seller's own conduct.
- **Isolate Conflicting Statutory Perimeters in Advance:** Where trade flows intersect both Western dollar clearing and PRC counterparties, treat the selection of confirming bank, governing law, and dispute-resolution forum as primary commercial pricing terms. Ring-fencing PRC-nexus facilities away from U.S.-dollar correspondent chains, rather than attempting to reconcile contradictory sovereign mandates inside a single LC, is increasingly the only durable hedge against bilateral legal exposure.

Takeaway

The documentary credit was engineered for an era in which sovereigns kept their geopolitical contests largely outside the clearinghouse. That era has closed. Between Washington's secondary-sanctions perimeter, London's statutory deference to sanctions freezes, Singapore's insistence on strict evidentiary proof, and Beijing's punitive enforcement of blocking statutes, the once-uniform language of UCP 600 now translates differently in every major financial hub.

Letters of credit remain indispensable to global commerce, but their promise of cash-like certainty can no longer be taken on faith. In a fragmented financial order, the party that controls the drafting of the sanctions clause, the flexibility of the shipping documents, and the redundancy of the settlement rail determines who gets paid, and who is left

holding paper while liquidity remains frozen in transit.

Wasel & Wasel advises on complex commercial disputes, international arbitration, and cross-border financial litigation. The firm represents commodity traders, financial institutions, and multinational corporations in high-stakes proceedings before courts and arbitral tribunals across the GCC, DIFC, ADGM, London, Hong Kong, and Singapore. Our practice includes litigating documentary credit and demand guarantee disputes, navigating conflicting international sanctions regimes and blocking statutes, structuring resilient trade-finance documentation, and enforcing cross-border payment obligations amidst geopolitical disruption.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

When the Bot Signs the Wire: Why US "own-risk" waivers for AI banking shatter against emerging rules in Abu Dhabi, London, Hong Kong, and Singapore.

November 26, 2026

Introduction: Follow the Net Interest Margin, Then Read the

Fine Print

In global banking, whenever chief executives invoke “customer safety” in unison on third-quarter earnings calls, prudent observers immediately check the net interest margin. Throughout October and November 2026, the largest financial institutions in the United States and Britain erected sudden technical and contractual barriers against third-party artificial intelligence agents, autonomous browser tools and personal assistants capable of logging into accounts, paying bills, and reallocating cash. Publicly, bank leadership framed the crackdown around rogue software and cybersecurity hygiene. Privately, the physics of modern bank balance sheets tell a simpler story.

Retail banking profitability rests on inertia. When households leave cash sitting in checking accounts yielding roughly 0.1%, banks lend or park those balances at 4% to 5% and pocket the spread. An autonomous agent programmed to optimize household yield does not suffer from human procrastination; it sweeps idle cash into higher-yielding treasury bills or money-market funds while its owner sleeps. Apollo Global Management chief economist Torsten Slok warned in September 2026 that synchronized balance-sweeping could trigger an “agentic bank run” at machine speed, with industry estimates placing annual US deposit-margin erosion near $47 billion. Across the Atlantic, McKinsey estimated that AI-driven switching threatens £700 billion in low-yielding British retail deposits, where moving just 5% to 10% of balances would slash UK bank deposit profits by a fifth or more.

Faced with software that threatens both authentication perimeters and deposit spreads, US banks split into two camps in late 2026. JPMorgan Chase, Bank of America, Citigroup, and Charles Schwab opted for perimeter prohibition, blocking credential-sharing agents like Meta’s Muse outright while funneling third-party apps toward read-only open-banking pipes that can view balances without moving money. Wells Fargo chose

a far more revealing path. Effective November 24, 2026, a newly minted Section 15 of Wells Fargo's *Online Access Agreement* leaves the door ajar for AI agents, provided the customer signs up for an extraordinary legal bargain: total assumption of operational, fraud, and manipulation risk, paired with an affirmative evidentiary duty to prove revocation when shutting an agent down.

For cross-border financial institutions, corporate treasurers, and sovereign wealth allocators operating across London, Dubai, Hong Kong, and Singapore, Wells Fargo's contractual experiment raises a decisive question. Can a regulated bank contractually blindfold itself to automated account activity while dumping the tail risk of machine error onto its depositors, or does that posture shatter against mandatory regulatory frameworks and emerging judicial precedent, exemplified by the Middle East's first AI liability ruling in **Abu Dhabi Commercial Court Case No. 762 of 2026**?

The Contractual Baseline: Dissecting Wells Fargo's Section 15 and the US Fault Line

Effective November 24, 2026, Wells Fargo's updated *Online Access Agreement* governs retail and commercial digital channels alike, spanning Wells Fargo Online, Wells Fargo Business Online, Wells Fargo Mobile, and Wells Fargo Advisors, all reinforced by mandatory binding arbitration and a class-action waiver. Rather than banning autonomous tools, Section 15, titled *"Third-Party Artificial Intelligence Agents or Agentic AI"*, constructs an eight-part liability shield from subsections 15(a) through 15(h):

- **Definitional Dragnet , Section 15(a):** Defines an "AI Agent" as *"any software, application, program, or other technology that takes autonomous, semi-autonomous, or non-autonomous action on behalf of any person or entity"*. Read literally, the inclusion of *"non-autonomous action"* sweeps in deterministic treasury

scripts, ERP reconciliation macros, and scheduled bookkeeping connectors alongside frontier language models.

- **Attribution Without Verification , Sections 15(b)–(d):** Disclaims bank control or vetting of third-party tools, strips bank privacy-policy protection from shared data, and decrees that every instruction transmitted by an authorized agent counts as the customer's personal act, with zero obligation on Wells Fargo to perform secondary verification. Under Section 2(d), if an account delegate or employee unleashes an agent, the primary account holder owns the resulting transactions, *"including those you did not want or intend"*.
- **Contractual Blindness , Section 15(e):** Declares in stark capitals that agent use is *"AT YOUR OWN RISK"*, covering software bugs and manipulated inputs such as third-party prompt injections, while stipulating: *"We do not monitor, screen, or review AI Agent activities"*.
- **The Revocation Burden , Section 15(f):** Places the entire mechanical and evidentiary burden of cutting off an agent on the customer. Account holders must revoke access *"properly and timely"*, rotate compromised Wells Fargo credentials, notify the bank via the channel specified in Section 17(d), and retain documentary proof, screenshots, vendor termination receipts, and call logs, to produce upon bank demand. Until Wells Fargo receives formal notice, the customer remains on the hook.
- **Unilateral Kill-Switch , Sections 15(g)–(h):** Bars use by minors under 18 and reserves Wells Fargo's right to mandate agent registration or block any tool overnight without notice or consequential liability.

Viewed through a commercial lens, Wells Fargo has drafted a free option on the agentic ecosystem. If fintech developers build sticky consumer workflows, Wells Fargo captures the transaction volume while JPMorgan and Citi block the door; if

a prompt-injected browser agent wires funds to a fraudster, Wells Fargo points to Section 15(d) and demands the customer's revocation screenshots.

The Institutional Mirror: Abu Dhabi Case No. 762 of 2026 and UAE Algorithmic Accountability

Step outside American arbitration clauses into the onshore courts of the United Arab Emirates, and the premise of Wells Fargo's Section 15(e), *"We do not monitor, screen, or review AI Agent activities"*, runs straight into a wall of institutional duty.

On June 11, 2026, the **Abu Dhabi Commercial Court of First Instance** delivered a landmark ruling in **Case No. 762 of 2026** (ABCFI 762/2026), establishing the first judicial precedent in the UAE and wider Middle East on institutional liability for AI-driven banking risk systems. The dispute arose from unauthorized credit card transactions executed via Apple Pay and one-time password (OTP) authentication channels. Despite the cardholder immediately notifying the bank of the fraud, the bank failed to halt the bleed and sought to hold the customer liable for the resulting card debt.

Evaluating the record under UAE Federal Decree-Law No. 35/2022 on Evidence and Federal Decree-Law No. 42/2022 on Civil Procedure, the Abu Dhabi Commercial Court discharged the customer's card liability and awarded compensation against the financial institution. Crucially, the Court treated structural deficiencies in the bank's artificial intelligence systems and architecture not as an excusable technological quirk, nor as a risk transferable by standard account terms, but as a fundamental institutional breach of the banker's duty of care.

The judgment does not stand in isolation. It operationalizes a dense UAE regulatory lattice governing automated finance:

1. **Capital Markets & SCA Rulebook Codification:** Under Securities and Commodities Authority Decision No.

13/RM/2021, as updated by Capital Market Authority Decision No. 13/RM/2026, UAE financial regulators explicitly require licensed institutions to govern four core algorithmic failure modes: *Model Drift*, *Hallucination* or illogical outputs, *Explainability Loss*, and *Algorithmic Bias*.

2. **Central Bank of the UAE (CBUAE) Supervisory Guardrails:** In February 2026, the CBUAE issued its *Guidance Note on Responsible Adoption of AI and ML*, mandating comprehensive AI model inventories, bias stress-testing, consumer human-review rights, and a strict boundary confining fully autonomous, unreviewed execution to low-risk, non-material processes.
3. **Civil Code Policing of Unfair Exclusions:** Under UAE civil transactions principles, AI possesses no independent legal personality, and onshore courts retain statutory discretion to pare back or nullify overbroad limitation-of-liability clauses in adhesion contracts that purport to absolve a regulated custodian from monitoring obvious fraud vectors.

Put bluntly: as case law stands, in Abu Dhabi or Dubai, a bank cannot deploy automated payment rails, pocket the operational cost savings of digitized servicing, insert a clause declaring *"we do not monitor or screen"* machine-driven transactions, and expect a commercial judge to enforce the disclaimer when an account is emptied in thirty seconds.

Global Financial Hubs Compared: Will London, Dubai, Hong Kong, and Singapore Adopt the Wells Fargo Playbook?

While banks across every major financial capital share Wall Street's hostility toward credential-scraping bots, **the four premier non-US financial hubs, London, Dubai, Hong Kong, or Singapore, can cleanly import Wells Fargo's "permit credentialed agents at the customer's sole risk" model.** Instead, regulatory physics in all four hubs is forcing banks toward a two-stage sequence: **block unverified credential-**

sharing today, then channel agents onto regulated, auditable API rails tomorrow.

Financial Hub	Current Bank Stance on AI Agents (Late 2026)	Governing Regulatory & Liability Architecture	Viability of Wells Fargo's "Sole Customer Risk" Model
London (UK)	**Precautionary Perimeter Block:** HSBC, Barclays, Lloyds, NatWest, and Nationwide moved in Nov 2026 to block/restrict transactional AI agents ahead of Meta Muse's UK rollout.	FCA Consumer Duty & Senior Managers Regime; UK Strong Customer Authentication (biometric app sign-off); PSR mandatory APP scam reimbursement; FCA developing trusted agentic finance framework.	**Low for Retail / Moderate for Corporate:** FCA treats failure to catch obvious fraud anomalies as a senior-management breach; biometric SCA physically blocks password-scraping agents anyway.
Dubai / UAE	**Controlled Sovereign Buildout:** Emirates NBD advocates bank-built agentic frameworks and hosts GPT models on onshore UAE servers; 53% of DIFC firms pilot agents, only 14% deploy live.	**ABCFI Case No. 762/2026** (institutional liability for AI fraud-detection failures); CBUAE Open Finance Regulation & Feb 2026 AI Guidance; SCA/CMA Decision 13/RM/2026; DFSA cyber/AI oversight.	**Rejected for Institutional Failures:** Courts hold banks liable for deficient fraud-detection models; third-party agent access is being routed into CBUAE-licensed Open Finance APIs rather than raw passwords.

Hong Kong	**Supervised Sandbox & Hard Human Gates:** Banks restrict external credential-sharing while testing agentic workflows inside regulatory sandboxes.	HKMA **ART Framework** & *Supervisory Guidance* (Ref. B1/15C, Oct 15, 2026); **Project SAGE** & *Discussion Paper on Agentic A.I. Governance* (Nov 2, 2026).	**Incompatible with Supervisory Expectations:** HKMA expects defined delegation scopes, deterministic fail-safes, real human approval windows, and immutable action logs, the exact opposite of "we do not monitor".
Singapore	**Phased Risk-Proportionate Governance:** DBS, OCBC, and UOB enforce strict anti-credential-sharing controls and app-bound cryptographic tokens.	MAS *Guidelines on AI Risk Management* (finalized Oct 7, 2026; phased Oct 2027 / Oct 2028) covering AI agents; MAS/IMDA *Shared Responsibility Framework* (SRF) for unauthorized/scam flows.	**Preempted by Waterfall Liability:** Under the SRF and MAS AI Guidelines, banks must fulfill real-time fraud surveillance duties first; blanket contractual disclaimers cannot override breached bank duties.

1. London: Biometric Friction and the £700 Billion Deposit Defense

On November 8, 2026, Britain's five largest lenders, HSBC, Barclays, Lloyds, NatWest, and Nationwide, confirmed precautionary restrictions blocking third-party AI agents from executing customer account transactions, despite zero reported incidents inside UK accounts to date. Structurally, London

differs from New York in two decisive respects. First, UK Strong Customer Authentication rules already force per-payment biometric approval inside a bank's native mobile app, breaking password-based screen-scraping agents before they reach the ledger. Second, under the FCA's Consumer Duty and Senior Managers and Certification Regime, if a bank's automated fraud-monitoring system misses glaring anomalies, regulators treat the lapse as an institutional governance failure rather than a retail user's tough luck. Rather than copying Wells Fargo's liability dump, the FCA is working with industry to construct a formal agentic finance framework built around verified **agent identity, scoped delegated authority, and clear institutional accountability**, keeping read-only open banking alive while gating payment initiation behind regulated rails.

2. Dubai and the UAE: Sovereign Infrastructure Over Password Scraping

Across the DIFC, ADGM, and onshore UAE banking markets, the regulatory ethos favors sovereign-grade infrastructure over laissez-faire credential sharing. The DFSA's *AI Survey 2026*, published November 2, 2026, revealed that while 71% of authorized DIFC firms now use AI and 53% are testing or piloting AI agents, only 14% have moved agents into production, reflecting cautious supervisory pacing on third-party concentration risk. Leading regional lender Emirates NBD has explicitly argued that banks must construct their own governed agentic frameworks rather than surrendering the interface to outside bots, going so far as to run OpenAI models on dedicated servers inside the UAE. Combined with the CBUAE's Open Finance Regulation, which standardizes tokenized API access, and the judicial warning shot of **Case No. 762 of 2026**, UAE banks have zero incentive to tolerate raw password-sharing agents while gambling on an untested contractual waiver.

3. Hong Kong: Project SAGE and Deterministic Guardrails

Hong Kong has moved faster than almost any peer jurisdiction to write an explicit architectural blueprint for agentic banking. Following its October 15, 2026 rollout of the **ART Framework** (Accountability, Resilience, and Trust) and updated *Supervisory Guidance* (Ref. B1/15C), the HKMA launched **Project SAGE** (*Securing Agentic Finance with Governance and Enablement*) alongside its *Discussion Paper on Agentic A.I. Governance in the Banking Sector* on November 2, 2026, with industry comments closing February 1, 2027. Four HKMA principles directly invert the Wells Fargo approach: agents must act strictly within bounded delegations of authority; failed deterministic checks must automatically block or escalate the transaction; human-on-the-loop approvals must afford genuine time to reject actions before settlement; and banks must preserve granular audit trails showing prompts, permissions, and approvals. Under Project SAGE, revoking or bounding an agent becomes a cryptographic infrastructure feature audited by the bank, not a screenshot scavenger hunt outsourced to the depositor.

4. Singapore: Waterfall Accountability and the October 2026 MAS Mandate

Singapore’s Monetary Authority closed Consultation Paper P017-2025 on October 7, 2026 by issuing final, binding-expectation *Guidelines on Artificial Intelligence Risk Management* applicable to all financial institutions and explicitly encompassing generative AI and AI agents. Phased into force on October 7, 2027 (governance, AI inventories, and materiality assessments) and October 7, 2028 (full lifecycle and infrastructure controls), with targeted MAS industry engagement on agentic AI slated for 2027, Singapore treats autonomous software as a supervised operational risk. Moreover, Singapore’s *Shared Responsibility Framework* (SRF) allocates digital fraud losses through a strict “waterfall” mechanism: financial institutions sit on the top rung and must prove they met real-time transaction-surveillance, cooling-off, and notification duties before passing losses downstream.

While deliberate password sharing by a retail user still breaches user-protection duties in Singapore, a bank that adopted Wells Fargo's *"we do not monitor or screen"* posture would fail the first rung of MAS's waterfall immediately.

The Legal Reality: Structural Issues Along the Fault Line

Beneath the immediate friction over blocked logins and updated terms of service lies a deeper set of structural problems that neither bank boilerplate nor developer optimism has yet resolved. The first is the **collapse between identity and delegation**. Legacy online banking was built on a binary premise: whoever presents valid credentials is the customer. Autonomous software breaks that assumption. As long as read-only data aggregation and payment-execution authority travel over the same shared credentials, account holders, particularly corporate treasurers operating outside retail consumer-protection caps, face asymmetric exposure whenever an automated workflow misinterprets an instruction or falls prey to external manipulation. Separating balance visibility from the power to move funds is no longer a mere technical preference; it is the boundary line where liability begins.

Closely tied to delegation is the **evidentiary mismatch around revocation**. Contractual terms that obligate a customer to cut off an agent and prove after the fact that termination was timely assume a clean, linear paper trail. Software permissions rarely fail so neatly. Persistent session tokens, cached credentials, and millisecond execution windows mean that future disputes will turn less on what a depositor intended than on which party holds verifiable, time-stamped records of when authority ended and whether the underlying rail actually honored the cutoff. Where revocation remains an informal tug-of-war over passwords rather than an instantaneous cryptographic switch, evidentiary ambiguity will consistently favor the party that drafted the agreement.

For institutions operating across borders, however, the

sharpest tension is the **territorial limit of contractual blindness**. A disclaimer stating that a bank neither monitors nor screens agent-driven activity may deter claims in domestic consumer arbitration, but it does not travel well. Across Abu Dhabi, London, Hong Kong, and Singapore, courts and supervisors increasingly treat anomaly detection, deterministic pre-settlement checks, and clear delegation boundaries as non-delegable institutional functions. Relying on passive "own-risk" waivers in jurisdictions that hold banks accountable for the blind spots of their own automated risk engines invites the worst of both worlds: operational complacency paired with unenforceable legal shelter.

Ultimately, neither blanket bans nor one-sided liability dumps represent a durable commercial equilibrium. Banks have every incentive to capture the transaction volume of automated commerce, provided they do not surrender low-cost deposits to unpoliced yield-sweeping along the way. The lasting resolution therefore points toward governed "Know Your Agent" infrastructure, dedicated rails where an agent's identity, spending ceiling, and counterparty permissions are verified before settlement, and where liability tracks actual operational control rather than fine print. Until those rails mature, the gap between what autonomous software can execute and what banking law will excuse remains the central risk on the ledger.

Mahmoud Abuwasel serves on the arbitral rosters of the American Arbitration Association (AAA), the Dubai International Arbitration Centre (DIAC), the Korean Commercial Arbitration Board (KCAB), and other international arbitral institutions, and is featured on the AAA-ICDR Blockchain and Web3 Disputes Panel. Advising extensively on high-stakes crypto, digital-asset, and algorithmic disputes, the earliest proving ground for litigation over autonomous execution, delegated credentials, and cryptographic revocation, he is the author of UAE Crypto Litigation and a contributing author to

Kluwer Law International's Crypto Asset Disputes. Operating across the fault line between international arbitration and mandatory onshore judicial supervision, including before the UAE courts and major global financial centers, Wasel & Wasel counsels clients on the governance, enforcement, and liability architecture of automated and cross-border finance.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Sovereign Heists, Stablecoin Freezes, and the ADGM Proprietary Injunction: Inside the $6.3 Billion Binance Recovery Architecture

November 26, 2026

The Abu Dhabi Global Market (ADGM) Courts' issuance of a proprietary injunction ordering 18 major cryptocurrency companies to freeze billions of dollars in stolen digital assets marks a pivotal moment in cross-border digital asset recovery [Reuters]. Following the October 29, 2026 cyberattack on wallets operated by Binance, a $6.3 billion breach attributed by United States authorities to North Korea and standing as the largest heist in cryptocurrency history [Reuters; Arabian Business], the world's largest cryptocurrency exchange turned to the courts of its global

operational hub in Abu Dhabi to restrict the movement of stolen tokens [Reuters]. Counsel from Gibson Dunn representing Binance described the relief in a statement as *"one of, if not the, largest publicly known freezing orders ever made"* [Reuters]. Applying to stablecoin issuers Circle (operator of USDC) and World Liberty Financial (operator of USD1), alongside 16 other firms, none of which were accused of wrongdoing by the court [Reuters; Arabian Business], the interim order sets the stage for a key return hearing scheduled for December 1, 2026 [Reuters].

For practitioners handling high-stakes Digital Asset Claims and cross-border enforcement, the ADGM Court's order represents a live test of the legal, custodial, and regulatory infrastructure developed across the United Arab Emirates in recent years. Drawing on the analysis of over one hundred UAE digital asset judgments in *UAE Crypto Litigation* and Wasel & Wasel's ongoing Intelligence coverage of global Web3 jurisprudence, four core legal dimensions define this proceeding: the jurisdictional shift to ADGM's common law framework, the legal mechanics binding non-wrongdoer intermediaries, the operational distinction between issuer-controlled stablecoins and native tokens, and the intersection of sovereign cyber operations with institutional risk frameworks.

Why Abu Dhabi? From "Binance Operators" to the ADGM Common Law Hub

Binance previously disclosed that the ADGM financial center serves as its global hub and that Abu Dhabi's Financial Services Regulatory Authority (FSRA) is its primary regulator [Reuters; Arabian Business]. In a January 9, 2026 briefing, *The Cost of Clarity: Inside Binance's 2026 Terms and the New Dispute Resolution Regime*, Wasel & Wasel examined Binance's transition, effective January 5, 2026, into a regulated corporate structure within the ADGM.

Prior to 2026, Binance's legacy user terms relied on an overarching counterparty construct termed "Binance Operators," an arrangement that faced judicial criticism for corporate opacity in *CFTC v. Zhao* and in *Lochan v. Binance Holdings Limited*, 2023 ONSC 6714, which Wasel & Wasel analyzed in *Crypto Disputes in Arbitration or Court? Impact of the Lochan v. Binance Judgment*. Under the 2026 restructuring analyzed in *The Cost of Clarity*, Binance segregated its operations across three distinct ADGM-licensed entities: **Nest Exchange Limited** (Recognized Investment Exchange), **Nest Clearing and Custody Limited** (Recognized Clearing House and digital asset custodian), and **Nest Trading Limited** (Broker-Dealer).

Alongside shifting user-facing disputes to three-member ICC arbitral tribunals seated in the ADGM, anchoring the platform's primary regulatory and custodial nexus in the ADGM carried significant substantive consequences under property law. As examined in the Introduction to *UAE Crypto Litigation*, while the UAE's onshore federal and local courts adjudicate digital asset claims within a civil law statutory framework, the ADGM and the Dubai International Financial Centre (DIFC) operate as autonomous common law jurisdictions. As H.E. Justice Michael Black KC noted in the Foreword to *UAE Crypto Litigation*, this pluralistic legal architecture places specialized common law courts alongside the onshore judiciary, equipping the UAE to address complex transnational blockchain disputes.

In *The Cost of Clarity*, Wasel & Wasel specifically noted that because ADGM law directly incorporates English common law, which recognizes crypto-assets as property capable of being the subject of proprietary claims (*AA v Persons Unknown* [2019] EWHC 3556 (Comm)), digital assets tied to the ADGM structure may be subject to **proprietary injunctions**. In the wake of the October 29 breach, Dugan Bliss, Deputy General Counsel at Binance, stated: *"We will continue using every lawful tool available to trace, freeze and recover stolen assets, support*

our partners in returning funds where possible, and keep those assets out of the hands of the attackers" [Reuters; Arabian Business]. Establishing its global hub in the ADGM positioned Binance within a common law jurisdiction empowered to issue proprietary freezing relief directed at tracing and immobilizing misappropriated assets across international markets.

Anatomy of the Proprietary Injunction: Innocent Intermediaries and Procedural Exposure

It was announced that the 18 companies named in the legal action are **not accused of any wrongdoing** [Reuters; Arabian Business]. Several market participants had already intercepted or frozen stolen tokens shortly after the October 29 incident, with Binance previously reporting that approximately **$2.85 billion** (roughly **45.2%** of the $6.3 billion stolen) had been frozen or intercepted by third parties [Reuters]. David Wachsman, spokesman for World Liberty Financial, stated: *"As the security incident unfolded in real time, World Liberty received an alert from onchain data identifying the issue. We acted decisively to protect our users and our partners"* [Reuters]. Similarly, a spokesperson for Circle stated that the company continues to coordinate with Binance and law enforcement, while declining to comment on specific legal proceedings [Reuters].

From an asset-recovery and Major Litigation perspective, formalizing pre-existing voluntary freezes through an ADGM proprietary injunction serves four concrete legal functions:

Proprietary Relief vs. Personal (*Mareva*) Freezing Orders: In cross-border fraud recovery, where Wasel & Wasel advises on obtaining *Mareva* injunctions and has represented respondents in USD 88 million worldwide freezing order (WFO) proceedings, a critical distinction separates a personal freezing injunction from a **proprietary injunction**. Whereas a *Mareva* order restrains a defendant from dealing with their own assets

to preserve a future judgment sum, a proprietary injunction attaches to specific claimed assets in which the claimant asserts a proprietary interest [Reuters]. As Wasel & Wasel examined in *Piercing the Blockchain Veil: The Ontario Court's Novel Pushback on Crypto Norwich Orders (Compared with the UK and DIFC)*, citing *Techteryx Ltd v Aria Commodities DMCC* [2025] DIFC DEC 001, common law courts in the UAE apply the "Enforcement Principle" to prevent the court's jurisdiction from being thwarted by rapid on-chain dissipation.

Prohibiting Lending, Swapping, and Mixing to Preserve Traceable Title: Under the ADGM Court's order, Circle, World Liberty Financial, and the 16 other named companies must maintain the freeze pending further court proceedings and are expressly **barred from lending, swapping, or mixing** the tokens with other assets [Reuters]. In *Misappropriated Mining Hardware and Newly Minted Tokens: Analysis of Yimiao v 3V (Supreme Court of Victoria) — Opportunity Loss, Unjust Enrichment, and Constructive Trusts*, Wasel & Wasel examined how common law courts treat stolen property as held on an institutional constructive trust from the moment of theft, whereas downstream derivative proceeds can complicate third-party "knowing receipt" claims if direct proprietary lineage is broken. Likewise, as detailed across *UAE Crypto Litigation*, UAE Virtual Asset Service Provider (VASP) regulations strictly prohibit commingling and unauthorized rehypothecation of virtual assets in order to preserve an auditable, one-to-one ownership record. Enjoining lending, swapping, and mixing prevents the claimed corpus from being absorbed into omnibus liquidity pools where proprietary tracing could be contested.

Judicial Safe Harbor Against Third-Party Holder Claims: When an issuer or exchange unilaterally freezes a wallet address without a court order or law-enforcement directive, it faces potential litigation from downstream wallet holders alleging breach of contract or tortious interference, a tension highlighted in Wasel & Wasel's August 2026 analysis, *A Reading*

of the High Court of Australia Transcript on the Nature of Cryptocurrency in Poulton v Conrad, regarding strict-liability conversion and good-faith purchaser defenses. As analyzed in Chapter 68 of *UAE Crypto Litigation* (examining Dubai Court of Appeal Case No. 233/2023), compliance with a binding legal freeze order from a competent authority negates the element of "fault" required to establish civil liability against a financial intermediary. A formal ADGM injunction converts voluntary blacklisting into compliance with a judicial mandate.

Divergent Enforcement Sanctions Across UAE Forums: For global VASPs served with court orders in the UAE, compliance risks differ sharply between common law free zones and mainland execution courts. In the ADGM and DIFC, non-compliance with an injunction engages **contempt of court** powers, an area in which Wasel & Wasel acted in the first contempt proceedings before the DIFC Courts and provided expert UAE law evidence to the UK High Court in *Commercial Bank of Dubai v. Al Sari* on cross-border WFO disclosure liabilities. By contrast, as Wasel & Wasel detailed in *The Seven-Day Trap: Dubai Courts Impose Strict Liability on Non-Debtor Third Parties — A Comparative Warning for Global Crypto Exchanges*, if parallel recovery actions lead to onshore UAE third-party garnishment notices under Articles 256 and 259 of Federal Decree-Law No. 42 of 2022, a non-debtor exchange that fails to file a formal declaration within seven days can be held **personally liable for the entire underlying debt**.

Stakeholder / Asset Category	Reported Scope in the $6.3B Breach	Legal & Operational Status	Primary Procedural Mechanism
Binance (ADGM Global Hub / FSRA Regulated)	Wallets breached on Oct. 29 for $6.3B; stated it absorbed financial impact and made customers whole [Reuters]	Pursuing recovery via ADGM Courts; return hearing set for Dec. 1, 2026 [Reuters]	Proprietary injunction to prevent transfer and support law enforcement [Reuters]
Circle (USDC), World Liberty Financial (USD1) & 16 Other Firms	Named among 18 respondents not accused of wrongdoing; part of ~$2.85B (45.2%) frozen/intercepted [Reuters]	Required to maintain freeze; barred from lending, swapping, or mixing tokens [Reuters]	ADGM Court proprietary order pending Dec. 1 continuation terms [Reuters]
Tether (USDT – El Salvador)	Previously disclosed freezing $1.5B of stolen funds; not included in ADGM court order [Reuters]	Direct bilateral coordination with Binance in consultation with authorities [Reuters]	Token reissuance workflow achieving functional restitution *in specie*
Remaining Unintercepted Assets (~$3.45B)	~54.8% of total stolen tokens outside reported $2.85B third-party interceptions [Reuters]	Subject to ongoing on-chain tracing and law-enforcement tracking [Reuters]	Forensic ledger screening and targeted freezes at VASP off-ramps

Centralized Stablecoin Control, Token Reissuance, and

Restitution *In Specie*

The division between the **$2.85 billion** (**45.2%**) already frozen or intercepted and the **$3.45 billion** (**54.8%**) remaining outside initial third-party freezes [Reuters] underscores the structural difference between centralized stablecoins and decentralized native protocols.

In *Universal Jurisdiction and the Situs of Centralized Digital Assets: An Analysis of Crypto Server Location in Iakovlev v. Epayments Systems Ltd. (Ontario Superior Court of Justice)*, Wasel & Wasel analyzed how courts increasingly look past the "borderless" narrative of blockchain networks when adjudicating centralized digital asset structures, anchoring control to identifiable corporate entities and infrastructure. Fiat-pegged stablecoins such as USDC, USD1, and USDT [Reuters] incorporate smart-contract administrative controls enabling their corporate issuers to freeze specific addresses on-chain. Functionally, that protocol-level authority operates much like the tripartite Account Control Agreements and "Notices of Sole Control" examined in *UAE Crypto Litigation*, which enable a secured or authorized party to halt unauthorized dispositions without the wallet holder's cooperation.

Equally noteworthy is the distinct path taken with El Salvador-based Tether. Although Tether previously disclosed that it had frozen **$1.5 billion** worth of stolen USDT, Tether was not included among the 18 companies in the ADGM Court order [Reuters]. Bliss stated that Binance was working directly with Tether on the return of those frozen assets, and a Tether spokesperson stated: *"In consultation with the relevant authorities, we will work directly with Binance in respect of reissuing the tokens"* [Reuters].

From a remedies standpoint, burning or permanently immobilizing compromised stablecoins and reissuing replacement tokens to the rightful holder achieves the functional equivalent of **restitution *in specie***. As examined in Chapters

42 and 63 of *UAE Crypto Litigation* and in Wasel & Wasel's February 2026 briefing, *UAE Crypto Litigation: Specific Performance and the Return of the Asset In Specie*, the Dubai Court of Cassation (Judgment of 14 November 2024 in Case No. 433/2024) has affirmed under Article 386 of the UAE Civil Transactions Law that the primary remedy for misappropriated digital assets is specific performance, returning the exact digital asset in kind, resorting to monetary valuation at the time of judgment only where *in specie* return is impossible. Where token reissuance is not resolved bilaterally alongside law enforcement, a court-sanctioned proprietary determination provides the formal legal basis that regulated issuers and custodians require before extinguishing or transferring frozen balances.

For the remaining **$3.45 billion** not yet captured in reported freezes, recovery confronts the evidentiary realities of decentralized networks. As detailed in Chapter 11 of *UAE Crypto Litigation* (analyzing Dubai Court of First Instance Case No. 2915/2023), when misappropriated assets are dispersed across dozens or hundreds of unattributed wallets, raw blockchain immutability proves asset movement but does not by itself establish legal attribution in court. Intercepting those flows requires combining real-time distributed ledger tracing software, a mandatory technical control for licensed VASPs under UAE regulatory rulebooks, with rapid injunctive and disclosure applications at the centralized off-ramps where laundered clusters eventually seek fiat or stablecoin liquidity.

Geopolitical Attribution, Balance-Sheet Protection, and Strategic Imperatives Ahead of December 1

The attribution of the October 29 heist to **North Korea** by US authorities [Reuters; Arabian Business] situates this recovery squarely at the intersection of Major Litigation and Sensitive Geopolicy. In *War Series: The Cyber-Kinetic Blur , 27+ Data Center Strikes in Active Conflicts, the NotPetya Precedent,*

and "Acts of War" in Arbitration and *The Private Sector's Increasing Control on National Security*, Wasel & Wasel analyzed how private digital infrastructure increasingly sits on the frontline of state-sponsored cyber operations, and how Lloyd's Market Association Bulletin Y5381 (the LMA5564 clauses) shifted systemic state-backed cyber risks away from standalone insurance policies and onto corporate balance sheets.

In its blog post, Binance stated that while it had absorbed the financial impact of the stolen funds and made customers whole, it had a duty and responsibility to pursue the stolen assets and support law enforcement [Reuters; Arabian Business]. Within the UAE's virtual asset regulatory architecture, where Wasel & Wasel has arbitrated and litigated complex exchange disputes involving platform security, liquidation engines, and insurance fund deployment, maintaining 100% one-to-one reserve backing for client liabilities is a foundational regulatory requirement. Where customer balances are made whole, downstream recovery litigation focuses directly on the platform's proprietary claims to trace, freeze, and reclaim stolen assets from attackers and intermediary pools.

With the ADGM Court scheduled to consider on **December 1, 2026** whether the proprietary injunction should continue and on what terms [Reuters; Arabian Business], institutional market participants, OTC desks, and global VASPs face three immediate operational priorities:

Enforce Contractual Provenance Warranties and Compliance Rejection Rights: US attribution of the breach to North Korea [Reuters] creates acute sanctions and secondary-freeze exposure across OTC and DeFi liquidity pools. Institutional counterparties should review master trading and custody agreements to exercise **Compliance Rejection Rights** and enforce express warranties that delivered tokens carry clean, unencumbered title free from unlawful provenance or regulatory

freezes, as detailed in *UAE Crypto Litigation*.

Isolate Flagged Balances from Automated Treasury Sweeps: VASPs and issuers bound by, or put on notice of, the ADGM proprietary order must ensure that technical wallet architectures disable automated lending sweeps, liquidity rebalancing, or omnibus commingling on flagged addresses to comply strictly with the court's prohibition against lending, swapping, or mixing [Reuters].

Coordinate Multi-Forum Procedural Responses Within Statutory Windows: Where cross-border tracing extends across the ADGM, DIFC, onshore UAE courts, and foreign jurisdictions, legal and compliance teams must map response protocols to each forum's exact procedural thresholds, distinguishing common law return hearings and contempt standards from the strict seven-day declaration window applicable to onshore UAE execution attachments.

As the December 1 return hearing approaches [Reuters], the ADGM Court's proprietary freeze demonstrates how far digital asset dispute resolution has evolved. While cryptographic exploits can move billions of dollars across ledgers in minutes, the ultimate recovery of institutional capital turns on regulatory foresight, forensic on-chain tracing, and the decisive deployment of common law equity.

Mahmoud Abuwasel is a Disputes Partner at Wasel & Wasel, with offices across Abu Dhabi, Dubai, Melbourne, Toronto, and Washington D.C., and is the author of UAE Crypto Litigation. For urgent inquiries regarding ADGM or DIFC freezing injunctions, VASP compliance protocols, or cross-border digital asset recovery, contact Wasel & Wasel's Digital Asset Claims and Crypto Fraud Protection team at **business@waselandwasel.com**.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

The Cost of Construction Expedience: Undocumented Variations and Arbitral Jurisdiction in Miller v Monaghan

November 26, 2026

In the physical execution of capital projects, there is a persistent friction between the rigid administrative mechanics of a written contract and the urgent, on-the-ground necessity to maintain operational momentum. When site conditions evolve or project scopes expand, the formal machinery of written notices, cost estimates, and countersignatures is frequently abandoned in favor of verbal approvals. It is a pragmatic, operational shortcut designed to save time, but one that almost inevitably invites a legal reckoning when the final invoices are issued. When a dispute arises over these undocumented variations, a critical jurisdictional question frequently emerges: If the parties completely ignored the strict variation procedures mandated by their contract, does the dispute over that "off-the-books" work still fall under the contract's arbitration agreement? Or does the procedural failure sever the dispute from the contract entirely, stripping the arbitrator of jurisdiction? This precise tension

was recently adjudicated by the Supreme Court of Western Australia in *Miller v Monaghan* [2026] WASC 441. The judgment provides an instructive framework for capital allocators, general counsel, and construction professionals regarding the breadth of standard arbitration clauses and the limits of contractual non-compliance in establishing arbitral jurisdiction. **The Factual Matrix: Expedience Over Procedure** The dispute in *Miller* centered on a standard form residential building contract executed in April 2024 for a sum of $675,910. The contract contained a highly prescriptive mechanism for variations under cl 12, requiring a written request from the owner, the preparation of a formal variation document by the builder detailing the cost, and the explicit, signed agreement of the owner before the work commenced. As is common in the industry, the paperwork fell behind the physical reality of the build. The plaintiff builder issued an invoice for $106,773.52 for additional work carried out on a "cost-plus" basis. The builder openly conceded that the formal variation procedure in cl 12 was not followed for every item of additional work. Instead, the builder justified the departure through an alleged verbal agreement driven by timeline pressures. As Justice Lundberg noted in the judgment, the plaintiff deposed:

> *"[45] In that context, to keep the Works progressing and to allow Mr and Mrs Monaghan to have their variations, I said to Mr Monaghan, at a meeting at 10 Sabina Drive in late-September 2025, 'All these changes are getting too complicated to keep up with the paperwork with, so all these additional works will need to be carried out at cost plus a reasonable margin and reconciled as we go, if we 're to get you in before Christmas'. Mr Monaghan said to me: 'That's fine'."*

When the defendant owner disputed the invoice, citing the absence of signed variations alongside invoicing errors, the builder sought to invoke the contract's arbitration clause (cl

18). Following a refusal by the contractual appointing authority (the Housing Industry Association) to appoint an arbitrator, the builder applied to the Supreme Court under s 11(4) of the *Commercial Arbitration Act 2012* (WA) to force the appointment. **The Jurisdictional Question: Are Non-Compliant Variations Arbitral?** For the Court to exercise its power to appoint an arbitrator, it first had to be satisfied that the dispute actually fell within the parameters of the arbitration agreement. This raised a formidable jurisdictional argument: if the builder completely bypassed the mandatory contractual procedure for raising variations, is the resulting dispute still subject to the contract's arbitration clause? The vulnerability of this position was addressed by Justice Lundberg:

> *"[26] The questions of whether the Variations were carried out, the value of the Variations and Mr Miller's entitlement are all matters falling for determination within the scope of the foreshadowed arbitration proceedings. It would not be appropriate to determine such matters in the context of the current hearing.*
>
> *[27] There is an argument potentially available as to whether the Variations-dispute falls within the ambit of the arbitration agreement because the Parties do not appear to have complied with the procedure for the raising of variations under cl. 12 of the Contract. Whilst it is accepted that neither party complied, that does not preclude the dispute from being arbitral."*

The Determination: The "Widest Import" of the Bargain

The Court rejected the premise that procedural non-compliance negates arbitral jurisdiction, relying heavily on the broad drafting of the arbitration clause itself. Clause 18 of the Building Contract dictated that "any dispute, disagreement or

difference… relating to this Contract" must be referred to arbitration.

Applying established principles of commercial construction, the Court noted that phrases such as "relating to" are heavily favored by the judiciary to capture precisely this kind of administrative deviation. Quoting the precedent set by Martin CJ in *Fitzpatrick v Emerald Grain Pty Ltd*, the Court reaffirmed that the phrase is "properly construed as a term of the widest import which should not, in the absence of compelling reasons, be read down."

Justice Lundberg concurred with the plaintiff's submission, determining verbatim:

> *"I respectfully agree, bearing in mind the breadth of the arbitration agreement in this case, as objectively assessed.*
>
> *That is, the court can be presently satisfied that, subject to the findings which might be made on the evidence, the subject matter of the variations claimed by the plaintiff is a dispute relating to the Building Contract and capable of being referred to arbitration."*

Crucially, the Court recognized that while the paperwork was flawed, the legal remedies to rectify that flaw, such as relying on the owner's verbal consent, are inherently tied to the contract's execution and remain the exclusive domain of the arbitrator:

> *"It is at least arguable that, although there was non-compliance with the variation procedure in cl 12 of the Building Contract, the plaintiff may be able to rely on the conduct of the parties to make good his contentions, relaying on some species of estoppel. Whether that will be the case requires a trier of fact to assess the competing evidence and*

> *credibility of the witnesses, which is beyond the scope of this application. It is enough to say that the plaintiff's claims for payment of the works undertaken as variations, which form the basis of the dispute between the parties, are matters relating to the Building Contract."*

Finding that the dispute squarely fit within the arbitration agreement, the Court exercised its statutory power to formally appoint the arbitrator. Furthermore, the Court ordered the defendant to pay the plaintiff's legal costs for the application on a party/party basis, noting that the plaintiff's conduct "involved nothing more than an adherence to the parties' bargain" and that the application "was necessary and appropriate in order to overcome the stalemate in the arbitral process." **Pragmatic Imperatives for the Construction Sector** The *Miller v Monaghan* decision offers stark, practical guidance for stakeholders in the construction industry. Courts will read phrases like "relating to this Contract" with a broad and flexible approach. A mutual or unilateral failure to comply with the administrative mechanics of a variation clause will unlikely sever the dispute from the arbitral tribunal. Skipping the paperwork may prejudice a party's chances of actually winning the arbitration on the merits, forcing them to rely on complex, evidence-heavy arguments like estoppel. However, as the Supreme Court of Western Australia has clearly signaled, that arduous evidentiary battle will unequivocally be fought in arbitration, exactly as the contract originally intended.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

The Right of Angary in Low Earth Orbit – Requisitioning Commercial Space Assets in Contemporary Armed Conflict

November 26, 2026

Capital is relentlessly pragmatic. It flows toward predictable legal frameworks and flees unquantifiable risk. For the past decade, the consensus narrative surrounding the commercialization of Low Earth Orbit (LEO) was remarkably straightforward: driven by plummeting launch costs and rapid advancements in commercial off-the-shelf technology, private enterprise would seamlessly expand the global economy into space. With institutions projecting the orbital economy to approach $1.8 trillion over the next decade, institutional capital poured billions into commercial satellite constellations. The fundamental premise was that these assets would operate much like terrestrial fiber-optic networks; as neutral, sovereign-agnostic infrastructure, safely insulated from geopolitical friction.

That premise has violently collided with reality. As active international conflicts vividly demonstrate, modern military operations are now irrevocably dependent on private space infrastructure. From high-resolution synthetic aperture radar (SAR) to decentralized broadband communications, commercial LEO assets are actively functioning as the nervous system for tactical battlefield logistics. This dual-use reality introduces a profound, largely unpriced risk for space-focused capital: the threat of sovereign requisitioning, wartime expropriation, and direct orbital interference. For the legal counsel and capital allocators underwriting this new frontier, the governing legal frameworks will not be found in utopian space treaties. They will be dictated by ancient maritime doctrines of warfare, modern orbital tracking data, and the fierce arenas of international commercial arbitration.

The Erasure of Orbital Neutrality

The theoretical risk of dual-use infrastructure has definitively transitioned into observable reality. In October 2026, an unprecedented event fundamentally altered the risk profile of commercial space operators. Independent orbital trackers suggest that *Cosmos 2612*, a Russian military satellite, executed a highly deliberate series of fuel-intensive maneuvers to rendezvous within a few hundred meters of *ICEYE-X36*, a U.S.-registered commercial SAR satellite operated by the Finnish firm ICEYE.

This maneuver was not a random convergence. It was the culmination of weeks of precise orbital repositioning. According to independent aerospace analyses, the Russian spacecraft altered its orbit by nearly 47 kilometers to match the commercial satellite's orbital plane, utilizing approximately 57 meters per second of velocity change to sustain unapproved close proximity with the 90-kilogram commercial payload. According to veteran orbital trackers, this incident represents the first known rendezvous between two active satellites in low Earth orbit without mutual owner approval.

The strategic context of this encounter is critical. Under an agreement formalized in 2022 and expanded in 2026, ICEYE provides dedicated SAR imagery and constellation access directly to Ukraine for military reconnaissance, leveraging the technology's unique ability to pierce cloud cover and operate at night. While it remains publicly unconfirmed whether the *ICEYE-X36* payload specifically services those operations, the geopolitical message was absolute. Sovereign adversaries are aggressively targeting Western commercial space assets utilized for military support.

This fulfills the stark warnings previously issued by the Russian defense apparatus: commercial satellites utilized to assist military operations in armed conflicts constitute "indirect participation" and are therefore "legitimate targets for retaliation." Whether the *Cosmos 2612* approach was an act of electronic espionage, a kinetic threat simulation, or a hostile inspection, the financial implications are immediate.

When a sovereign military physically intercepts a commercial asset and paints it as a legitimate target, traditional “war exclusion” clauses in property insurance predictably void coverage. This leaves private operators and their financial backers exposed to total systemic loss, confirming that the neutrality of commercial space hardware has functionally evaporated.

The Ghost of *The Zamora* and Orbital Angary

If adversaries are willing to actively target commercial infrastructure, host nations will be equally willing to forcibly commandeer it. In the brutal calculus of geopolitics, when national survival is threatened, the sanctity of private commerce is routinely subordinated to military necessity.

To understand how states will legally justify this requisitioning, international litigators must look backward. Customary international law has long recognized the “Right of Angary” (*ius angariae*); a sovereign prerogative allowing a belligerent state, in times of urgent public necessity, to lawfully requisition, commandeer, or destroy neutral foreign commercial property located within its jurisdiction, provided adequate compensation is ultimately paid.

This principle was definitively stress-tested during World War I in the landmark Privy Council Prize Court case, *The Zamora* (1916). The English court affirmed that the Crown possessed the prerogative right to requisition neutral cargo, in that instance, a shipment of copper, provided the seizure was absolutely necessary for the defense of the realm. Today, that copper is encrypted SAR data, and the cargo ship is a commercial LEO constellation. Under Article VIII of the 1967 Outer Space Treaty, a state retains jurisdiction and control over any space object on its registry. If a geopolitical flashpoint escalates and a host state urgently requires exclusive bandwidth, immediate geospatial intelligence, or the denial of that intelligence to an adversary, the Right of Angary provides a viable legal mechanism to simply commandeer

a private commercial network.

The military establishment is actively pricing in this reality. The U.S. Space Force has formally detailed the Commercial Augmentation Space Reserve (CASR), a framework designed to seamlessly scale military access to private space bandwidth and imagery during wartime. While CASR is currently framed as a voluntary peacetime contractual arrangement, voluntary frameworks are a luxury of peace. If a commercial operator attempts to geofence its network to preserve its civilian neutrality during a hot war, host states will inevitably bypass commercial contract law and invoke emergency national security statutes to seize operational control.

The Arbitration Battlefield: *CC/Devas* and the National Security Exception

When a sovereign state commandeers, nullifies, or inadvertently triggers the destruction of a commercial space asset, the ensuing financial fallout bypasses domestic courts and flows directly into Investor-State Dispute Settlement (ISDS). In these arbitral tribunals, aggrieved foreign investors collide with the most formidable defense in international law: the National Security Exception.

The arbitration saga of *CC/Devas (Mauritius) Ltd. v. Republic of India* (PCA Case No. 2013-09) serves as the definitive structural precedent for space-bound capital. In 2011, the Government of India abruptly annulled a highly lucrative S-band satellite spectrum lease held by private firm Devas Multimedia. India's justification was rooted entirely in sovereign prerogative: the state declared the orbital spectrum was urgently required for "strategic national security use."

The Mauritian investors brought claims under the Mauritius-India Bilateral Investment Treaty (BIT), arguing unlawful expropriation. An international arbitral tribunal ultimately ruled against India, concluding that while a state possesses the sovereign right to protect its essential security interests, it cannot utilize the cloak of national security to

arbitrarily expropriate commercial rights without executing full reparations. The resulting awards, ordering India to pay in excess of $1.1 billion in damages, established a vital precedent: international tribunals will aggressively scrutinize a blanket “national security” defense in space-related expropriations to ensure capital is adequately compensated.

Pragmatic Imperatives for Capital Allocators

Hope is not a viable legal strategy, and proceeding into the modern space economy with commercial contracts drafted for a benign, purely civilian operational environment is a severe dereliction of fiduciary duty. As the ongoing shadowing of the *ICEYE-X36* satellite unequivocally demonstrates, the commercialization of space has functionally privatized military logistics, dissolving the traditional boundaries between commercial hardware and sovereign weaponry. Adversarial nations possess both the capacity and the intent to contest this infrastructure physically. For legal counsel and executives structuring orbital investments, managing this unprecedented sovereign risk requires ruthless contractual mechanics executed long before launch.

The immediate priority for capital allocators is pricing the requisition risk directly into the foundational legal framework. When commercial payload and service contracts are signed with sovereign or quasi-sovereign entities, the agreements must mathematically quantify the state’s absolute financial liability. If a host state triggers an emergency seizure, commandeers satellite bandwidth under the Right of Angary, or invites hostile orbital harassment by utilizing the commercial asset for active military operations, there must be no ambiguity regarding who assumes the financial loss. This operational reality simultaneously demands a structural evolution in corporate design. Operators can no longer comfortably commingle neutral commercial logistics data with wartime intelligence on the same physical satellite bus.

Blending these services severely compromises the asset's neutral status under the laws of armed conflict, effectively turning the entire platform into a legitimate military target and guaranteeing the voiding of commercial insurance policies. The technical and legal bifurcation of civilian and military services is a necessary market response to ring-fence civilian liability.

Ultimately, the deployment of capital for space infrastructure must be subjected to intense geopolitical scrutiny regarding treaty routing. Capital must be rigidly channeled through jurisdictions with robust Bilateral Investment Treaties that provide actual mechanisms for international arbitration. Investors must analyze the specific language of a treaty's essential security interests clause. Treaties featuring self-judging national security exceptions offer commercial operators virtually zero legal protection against arbitrary state expropriation. In an orbital economy where military payloads actively stalk commercial satellites, the strength of the underlying investment treaty is the only viable firewall between commercial survival and total, uncompensated loss.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

War Series: The Cyber-Kinetic Blur – 27+ Data Center Strikes in Active Conflicts,

the NotPetya Precedent, and "Acts of War" in Arbitration

November 26, 2026

In the architecture of global commerce, risk is fundamentally priced against historical precedent. For decades, that precedent dictated a clearly defined paradigm: warfare was kinetic, geographic, and overt. Standard *force majeure* provisions and property insurance "war exclusions" were meticulously calibrated for a world of naval blockades, physical destruction, and formal declarations of hostility. If a sovereign state committed an act of war, the evidentiary threshold was unmistakable, and the contractual remedies were clear. That framework is now structurally obsolete. As highlighted by a recent *NBC News* analysis documenting at least 27 direct attacks on data centers across active global conflicts, the civilian digital infrastructure that underpins the global economy is no longer merely collateral damage; it has become a primary military target. This escalation signals a definitive new front in modern warfare, where state-sponsored operations, whether kinetic strikes on centralized data nodes or the deployment of weaponized malware, routinely serve as the vanguard of geopolitical friction. This reality erases sovereign borders, transforms neutral corporate supply chains into active conflict zones, and exposes how systematically the broader market is mispricing the associated legal risk.

For multinational capital and the legal counsel tasked with its preservation, the 2017 *NotPetya* cyberattack remains the definitive baseline. Generating an estimated $10 billion in total global economic damage according to U.S. White House assessments, the event exposed a critical vulnerability: commercial contracts drafted for twentieth-century physical hostilities are highly susceptible to twenty-first-century

digital contagion.

The Second-Order Effects of Insurance Risk Transfer

NotPetya was initially deployed against Ukrainian tax software, but the malware rapidly broke containment, paralyzing the operations of non-combatant commercial entities globally. When pharmaceutical conglomerate Merck & Co. suffered severe operational downtime, it sought relief under its "all-risk" property insurance policies. Underwriters denied the claim, invoking standard "war exclusion" clauses on the grounds that *NotPetya,* widely attributed to Russian military intelligence, was an uninsurable act of war.

The resulting litigation, *Merck & Co., Inc. v. Ace American Insurance Co.* (N.J. Super. Ct. App. Div., 2023), culminated in a ruling that standard "hostile action" exclusions applied exclusively to traditional, kinetic warfare. Merck and its insurers ultimately reached a confidential settlement in early 2024, reportedly resolving the $1.4 billion claim. Similarly, food and beverage giant Mondelez International settled a high-profile $100 million claim with Zurich Insurance in late 2022 following a comparable dispute.

However, viewing these settlements as definitive corporate victories ignores the second-order effects on the market. Recognizing the existential threat to systemic capital, the London insurance market, the historical epicenter of global risk allocation, fundamentally re-engineered its exposure. Effective March 31, 2023, the Lloyd's Market Association (LMA) issued Bulletin Y5381, mandating that all standalone cyber policies explicitly exclude liability for state-backed cyberattacks that "significantly impair the ability of a state to function" (standardized under the LMA5564 series of clauses).

With insurers successfully transferring the liability of digital warfare back onto corporate balance sheets, the legal battleground has permanently migrated. Disputes over supply chain failures, data center outages, and operational downtime

have shifted from insurance subrogation into the realm of business-to-business breach-of-contract and *force majeure* arbitrations.

A Seamless Global Contagion, Localized Liability

The primary danger for the modern enterprise is that digital supply chains and data center networks are hyper-integrated, yet the legal mechanisms to defend them remain fiercely localized. A single piece of malicious code, or a kinetic strike on a regional data center, can ripple across the global economy, intersecting with fundamentally different statutory frameworks in real time. Instead of neatly separated jurisdictions, legal departments must now navigate a seamless global threat vector that cascades across regional legal doctrines.

Consider the lifecycle of a modern digital disruption. If a state actor breaches an EU-based logistics network, the commercial dispute instantly morphs into a regulatory crisis. Authorities evaluate the breach against the stringent strictures of the NIS2 Directive (Directive (EU) 2022/2555). It is insufficient to merely claim geopolitical *force majeure* to excuse non-performance; if a corporate victim failed to implement baseline cybersecurity risk-management measures, they face regulatory fines of up to €10 million or 2% of their global annual turnover. Domestically, European tribunals may reasonably conclude that this prior compliance negligence renders any contractual *force majeure* defense void, as the disruption could have been prevented or mitigated.

Tracing those supply arteries further east, the hardware powering this global system is manufactured by the highly integrated tech conglomerates of Japan and South Korea. According to IBM’s 2024 X-Force Threat Intelligence Index, the Asia-Pacific region remains one of the most heavily targeted geographic areas globally. When commercial entities are disrupted by regional Advanced Persistent Threats (APTs), they confront rigid domestic civil codes. Seeking relief under the

strict unforeseeability requirements of the Japanese Civil Code or the South Korean Civil Act is legally complex. In these jurisdictions, state-sponsored cyber hostility is increasingly scrutinized not as an unforeseeable act of war, but as a quantifiable, baseline operational risk that should have been priced into the contract.

This commercial vulnerability is accelerating rapidly in the Middle East. As the Gulf Cooperation Council (GCC), a regional cybersecurity market projected to exceed $13 billion by 2027, executes some of the most digitally integrated infrastructure megaprojects in history, legacy energy grids are evolving into hyper-connected smart cities. If state-sponsored malware targets a regional desalination plant or paralyzes automated port logistics, developers and sovereign wealth funds face immediate contractual deadlock. They must litigate whether the disruption constitutes a valid "extraneous cause" (*cause étrangère*) under statutes such as Articles 273 and 287 of the UAE Civil Transactions Law, or a fundamental failure of the contractor to secure the digital perimeter.

When these high-stakes, cross-border disputes inevitably rupture, they frequently flow into premier neutral arbitration hubs like Singapore. Institutions such as the Singapore International Arbitration Centre (SIAC) are increasingly tasked with adjudicating massive supply chain defaults caused by digital sabotage. Concurrently, Singapore's Cybersecurity (Amendment) Bill 2024 has expanded regulatory oversight to cover entities of "special cybersecurity interest," demonstrating how intimately commercial arbitration is becoming entangled with national security statutes. The traditional boundaries between private commercial disputes and sovereign regulatory regimes have vanished.

The Evidentiary Abyss of Attribution

Whether seated in Singapore, London, or Dubai, arbitral tribunals handling these disputes face a singular, paralyzing hurdle: the legal standard of attribution.

In kinetic warfare, attributing a physical strike on a facility to a sovereign state relies on observable fact. Cyberspace operates through proxies, criminal syndicates, and false-flag code. If a data center provider or logistics firm defaults on a major GCC infrastructure contract and invokes an "act of war" clause following a cyber event, establishing definitive state sponsorship before a private commercial tribunal is an immense evidentiary burden.

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* outlines strict thresholds for attributing cyber operations to a state, but private commercial tribunals lack the investigative authority of sovereign intelligence agencies. Arbitrators must distinguish between a state military operation and financially motivated cybercrime on a balance of probabilities. Parties often attempt to introduce unclassified intelligence from national cyber authorities to bridge this gap. However, under frameworks like the IBA Rules on the Taking of Evidence, relying on classified or highly redacted state intelligence within private commercial disputes introduces significant procedural complexities and questions of geopolitical bias.

Pragmatic Imperatives for Capital Protection

As the recent targeting of data centers illustrates, the intersection of military strategy and civilian data infrastructure is no longer a theoretical risk; it is an active operational reality. Relying on century-old boilerplate language for modern infrastructure and supply chain agreements presents a severe fiduciary vulnerability. In an environment where code deployed in one hemisphere can trigger a multi-billion-dollar default in another before the market opens, commercial structures must adapt.

For legal counsel and executives structuring multi-jurisdictional agreements, risk mitigation requires precise contractual mechanics:

- **Decouple Cyber from Kinetic Warfare:** Contracts should

identify whether state-sponsored cyberattacks, physical strikes on data centers, and ransomware constitute a distinct *force majeure* event, rather than relying on legacy "war, hostilities, or acts of foreign enemies" clauses. The contractual language must be as specific as the threat vector.

- **Price the Collateral Damage:** Supply chain agreements should mathematically quantify liability and delay damages for instances where a party is not the primary target of a cyber-hostility but suffers operational paralysis due to global digital contagion.
- **Hardwire Attribution Mechanisms:** To prevent evidentiary stalemates in arbitration, contracts should establish a pre-agreed standard for attribution. For example, parties may stipulate that a formal, public declaration from a recognized national authority (such as the U.S. CISA, the UK NCSC, or the Cyber Security Agency of Singapore) serves as *prima facie* evidence of a state-backed attack for the purposes of the agreement.

Geopolitical conflicts are increasingly executed across the physical and digital assets of private enterprises. Until the mechanics of international commercial law fully adapt to the realities of asymmetric warfare, the imperative lies with the private sector to strictly define, price, and contractually ring-fence its digital liabilities. In the modern commercial theater, an ambiguous contract is a quantifiable liability.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Arbitration Standing for Non-Controlling Shareholders: Lessons from 1171757 Ontario v. 1171758 Ontario with Global Perspectives

November 26, 2026

Introduction

In complex corporate structures involving holding companies, trusts, and family-owned enterprises, identifying precisely who is bound by, and who is entitled to invoke, an arbitration agreement remains a persistent source of jurisdictional friction. When a dispute arises, can a minority shareholder of a corporate partner, bereft of management control over that partner, qualify as a "party" to the underlying partnership agreement and initiate arbitration?

The Ontario Superior Court of Justice recently addressed this critical issue in *1171757 Ontario Limited et al v. 1171758 Ontario Limited et al*, 2026 ONSC 4414. Ruling that a non-controlling shareholder of a corporate partner did indeed possess standing to arbitrate, the Court delivered a compelling decision on contractual interpretation and commercial reasonableness.

For international practitioners and stakeholders across common law jurisdictions, from the United Kingdom to the United States, this judgment offers a robust blueprint for how courts balance strict privity of contract with the economic realities of indirect stakeholders.

The Factual Matrix: A Family Enterprise Divided

The dispute centered on a family-owned enterprise holding two hotels and a fitness centre in trust for a partnership. The partnership units were divided between corporate partners, including a company named 1171757 Ontario Limited ("757").

The partnership agreement relied on distinct defined terms: "Partner" (the corporate entities) and "Principal" (the natural persons with the ultimate right to direct and control a corporate partner). Crucially, the arbitration clause mandated that any dispute "between the parties hereto" must be resolved by arbitration, yet the term "party" was left undefined.

Following the death of the family patriarch, his shares in 757 were bequeathed equally to his two grandsons, Jason and Jonathan. The bequest, however, required Jonathan to execute a Power of Attorney ("POA") granting Jason absolute authority to vote Jonathan's shares and manage 757. Consequently, Jason became a "Principal" of 757, while Jonathan remained a 50% shareholder devoid of control rights.

When Jason initiated an arbitration to adjust compensation for a management company he controlled, Jonathan subsequently sought to participate to protect his own service contract with the enterprise and to request dissolution of the partnership. Jason challenged Jonathan's participation, arguing that because Jonathan was neither a "Partner" nor a "Principal," he was not a "party" to the agreement, meaning the arbitrator lacked jurisdiction over his claims.

The Court's Reasoning: Text, Context, and Commercial Logic

Justice E. Iacobucci of the Ontario Superior Court of Justice reviewed the arbitrator's preliminary jurisdictional ruling *de novo*. The Court rejected the argument that "parties" must be strictly limited to Partners and Principals, anchoring Jonathan's status in the agreement's recitals and enurement clause, guided by commercial logic.

1. Standard of Review: De Novo

Establishing the standard of review under the Ontario *Arbitration Act, 1991*, the Court confirmed its mandate to evaluate the jurisdictional question without deference to the arbitrator:

"This application is a hearing de novo, not a review of or an appeal from the arbitrator's decision. The principle of competence-competence does not require that any deference be paid to an arbitrator's determination of her own jurisdiction… I am simply to 'decide the matter'…" (para. 51).

2. Distinguishing Partners, Principals, and Parties

The Court found the agreement deliberately used the terms distinctly. While certain restrictive covenants applied exclusively to Principals and Partners (aligning with their managerial control), the arbitration clause did not contain such a restriction:

"The arbitration clause requires disputes between 'parties' to be decided in arbitration. It does not restrict the operation of the clause to 'partners' or 'principals'… Nothing in the wording of Article 18.1, or other clauses that use principals, partners and parties, detracts from the conclusion that a 'party' may be neither a principal nor a partner." (paras. 66, 74).

The Court found Jonathan's status anchored in the agreement's recitals and enurement clause. The original patriarch signed the agreement in his individual capacity, identified in the recitals expressly as a *"beneficial and registered shareholder."* Because the enurement clause bound and benefited his heirs, Jonathan inherited this "party" status alongside his equity.

3. Commercial Sensibility

Underlining the commercial pragmatism of the decision, the Court observed that granting a shareholder party status makes inherent business sense:

"A shareholder in a partner has a financial interest in the operations of the partnership. Including that shareholder as a party to the partnership agreement provides the shareholder with protection of that financial interest… Just as non-voting shareholders do not have control rights over the corporation, yet have standing to seek corporate law remedies, the partnership agreement in this case confers on non-principal, non-partner parties standing to participate in arbitration protecting their rights and interests." (para. 80).

4. The Power of Attorney Did Not Extinguish Standing

Jason argued that the POA stripped Jonathan of party status by transferring all governance rights. The Court wholly rejected this, holding that the loss of operational control does not extinguish underlying contractual rights tied to beneficial ownership:

"That Jonathan has no control rights in 757 does not affect the implications of the wording of the agreement, nor the commercial logic of allowing shareholders without control rights to protect their financial interests in the partnership through party status (and rights to arbitrate) pursuant to the agreement." (para. 93).

Comparative Global Perspectives: UK, US, and Beyond

The Ontario Court resolved this issue through direct textual interpretation; finding the shareholder was an actual "party" to the contract based on inherited shares and enurement clauses. How do other major common law jurisdictions approach minority shareholders and non-signatories seeking to invoke an arbitration clause?

United Kingdom: Statutory Gateways and Third-Party Rights

In England and Wales, the strict doctrine of privity of contract traditionally poses a high hurdle for non-signatories. However, Section 82(2) of the English *Arbitration Act 1996* provides that a party to an arbitration agreement includes any person *"claiming under or through a party to the agreement."* Furthermore, under Section 8 of the *Contracts (Rights of Third Parties) Act 1999*, a third-party beneficiary (such as a shareholder explicitly granted rights or protections in an agreement) can enforce an arbitration clause. Much like the Ontario court's reliance on the enurement clause to recognize Jonathan's inherited status, English courts will allow stakeholders to arbitrate if the contractual machinery clearly intended to benefit them or if their claims are entirely derivative of a signatory's rights.

United States: Equitable Doctrines and Pro-Arbitration Policy

The United States operates under the Federal Arbitration Act (FAA), embodying a strong national policy favoring arbitration. Rather than strictly interpreting the word "party," US federal and state courts frequently allow non-signatories to invoke arbitration clauses using common law equitable doctrines (*e.g., Arthur Andersen LLP v. Carlisle*, 556 U.S. 624). Doctrines such as *third-party beneficiary*, *alter ego/veil-piercing*, and *equitable estoppel* are routinely deployed. Had this case been litigated in New York or Delaware, Jonathan might have successfully compelled arbitration by arguing that his claims were heavily "intertwined" with the underlying partnership agreement, and that as an equity holder, he was an intended third-party beneficiary of the enterprise structure.

Other Common Law Hubs (Singapore, Australia, DIFC)

Courts in leading global arbitration hubs have adopted highly commercial, purposive approaches to arbitration clauses. Like the Ontario Court's emphasis on the "commercial logic" of allowing stakeholders to protect their financial interests,

jurisdictions like Singapore and Australia frequently look at the substantive economic reality of corporate structures. They are reluctant to elevate strict corporate formalism over practical business sense, especially if a restrictive interpretation leads to a commercial absurdity where a beneficial owner is left without an arbitral remedy despite having a clear, contractually recognized financial stake.

Key Takeaways for International Practitioners

The Ontario judgment in *1171757 Ontario Limited et al v. 1171758 Ontario Limited et al* serves as a powerful reminder that "control" and "standing" are distinct concepts in dispute resolution. For corporate drafters and commercial litigators globally, the takeaways are clear:

Define "Party" Explicitly: The entire jurisdictional battle in this case stemmed from defining "Partner" and "Principal" but leaving "Party" undefined. If the intention is to limit dispute resolution mechanisms strictly to controlling principals or specific corporate signatories, the arbitration clause and the definitions section should state this unambiguously.

Beware Recitals and Enurement Clauses: "Boilerplate" clauses enuring benefits to heirs and successors, combined with recitals identifying stakeholders as beneficial owners, can act as a backdoor entry into an arbitration agreement, unintentionally widening the pool of individuals with standing to arbitrate.

Control Does Not Equal Standing: Divesting a shareholder of voting or management control (e.g., via a proxy or POA) prevents them from directing the company, but it does *not* automatically strip them of their underlying contractual rights to seek arbitral remedies to protect their economic interests.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

The Seven-Day Trap: Dubai Courts Impose Strict Liability on Non-Debtor Third Parties – A Comparative Warning for Global Crypto Exchanges

November 26, 2026

Introduction: The Historical Opacity of Onshore Asset Tracing

In traditional commercial disputes, pre-execution asset tracing in onshore jurisdictions has long been hindered by structural opacity. Outside of public shareholding disclosures, corporate registries for mainland and free zone limited liability companies do not publicly disclose banking relationships, intercompany receivables, or granular asset holdings. Strictly enforced banking secrecy laws prevent judgment creditors from independently identifying where a debtor holds accounts or receivables prior to opening an execution file. Consequently, creditors historically relied on broad, court-driven inquiries routed through the UAE Central Bank, land departments, and licensing authorities, rarely possessing independent proof of assets held by private non-bank third parties.

Faced with these onshore hurdles, creditors navigating complex fraud or asset recovery cases frequently looked toward the Dubai International Financial Centre (DIFC) Courts. In that offshore jurisdiction, common law tools like *Norwich Pharmacal* and *Bankers Trust* disclosure orders are readily available and historically favored. These orders are highly effective largely because they carry the severe and coercive threat of contempt of court proceedings for non-compliance.

However, a profound shift in UAE mainland jurisprudence has fundamentally altered the asset recovery paradigm. The Dubai Court of Cassation, in a series of recent landmark judgments, including Cassation No. 1665/2025 and combined appeals No. 1773 & 1826 of 2025, has established a stringent interpretation of the UAE Civil Procedures Law. The newly affirmed standard is absolute: non-debtor third parties ordered to disclose a debtor's assets who fail to formally respond within exactly **seven days** can be held personally and directly liable for the entirety of the original judgment debt.

While this use of disclosure orders provides a powerful theoretical tool for creditors, it creates a formidable compliance challenge for third parties. This is particularly true for cryptocurrency exchanges and Virtual Asset Service Providers (VASPs) operating in the UAE, whose operations could face severe financial exposure under these newly established procedures.

The UAE Framework: From Procedural Default to Substantive Liability

The recent Dubai Court of Cassation judgments clarify the strict application of Articles 255, 256, and 259 of the UAE Civil Procedures Law (Federal Decree-Law No. 42 of 2022).

Under these procedures, when a creditor executes a judgment, the execution judge can issue a garnishee or attachment order

directing a third party to disclose any funds or assets it holds belonging to the debtor. Under Article 256, the third party has exactly seven days from the date of notification to formally declare what it holds. Crucially, the law explicitly dictates that a third party is *not exempt* from the duty to report even if they do not hold any assets for the judgment debtor; they must still formally submit a negative declaration.

As affirmed by the General Assembly of the Dubai Court of Cassation (Decision No. 10 of 2025) and applied in the recent Cassation judgments, if the third party ignores the notice, refuses to accept it, provides insufficient information, or conceals documents, their inaction constitutes a severe procedural fault. Under Article 259, this procedural failure allows the creditor to file a substantive civil claim directly against the third party.

The Court of Cassation decisively clarified that this is not a mere execution dispute under the purview of an execution judge. Instead, the failure to submit the report transforms the execution claim into a direct, personal, and substantive civil lawsuit against the third party for the full value of the original debt. By missing the court’s deadline, the third party effectively assumes the debtor’s liability.

The Virtual Asset Context: Transparency Meets Strict Liability

This development is of acute importance to the digital asset sector. While a debtor could traditionally hide fiat currency or private shares behind structural opacity, cryptocurrency fundamentally changes the investigative reality. Because blockchains function as public ledgers, forensic investigators can trace diverted funds directly to deposit wallets hosted by centralized cryptocurrency exchanges.

Armed with a blockchain tracing report, a creditor could bypass the reliance on broad Central Bank inquiries and

present independent proof of digital asset locations directly to a UAE execution judge. Under the newly established procedures, a creditor could then obtain a targeted disclosure and attachment order against the local offices of a global crypto exchange. This potentiality presents significant operational and legal risks for international VASPs, particularly where internal compliance protocols are modeled on the more extended response timelines typical of other jurisdictions:

Jurisdictional Friction (ADGM/DIFC vs. Onshore Dubai): Many crypto exchanges operating in the UAE are licensed within financial free zones, such as the Abu Dhabi Global Market (ADGM) or the DIFC. If an onshore Dubai Court execution order is served on a free-zone domiciled entity, there may be a legal question regarding whether the mainland execution judge holds direct jurisdiction over the offshore-licensed entity. Even if the mainland court lacks jurisdiction, under the new Cassation precedent, a failure to formally submit this jurisdictional defense to the ordering court within the seven-day window could allow the creditor to invoke Article 259 and pursue the local exchange for the entire crypto-traced debt.

Fragmented Corporate Structuring (The Sister Entity Defense): Global crypto exchanges frequently utilize highly fragmented corporate structures. A localized UAE entity might operate solely as a marketing, support, or advisory branch, while the actual user wallets, customer funds, and private keys are custodied by a sister entity in another jurisdiction. If a mainland court’s seven-day disclosure notice is received by the local branch, the fact that the UAE entity does not technically hold the funds does not negate the reporting obligation. Under Article 256, the entity must still formally reply to the execution court, detailing its corporate structure and clarifying its non-custodial status. Failing to legally articulate this reality within the tight statutory timeframe could result in the onshore entity absorbing the

debtor’s financial liability.

A Striking Divergence: Comparing Global Crypto Hubs

To fully appreciate the gravity of the UAE’s approach, it is vital to contrast it with how third-party disclosure is enforced in other major jurisdictions favored by the crypto industry.

United Kingdom, Singapore, Hong Kong & DIFC (The Contempt Paradigm): In traditional common law hubs, tracing digital assets typically relies on *Norwich Pharmacal* Orders (NPOs) or *Bankers Trust* Orders (BTOs). Courts in the UK (e.g., *Fetch.ai Ltd v Persons Unknown*), Singapore (e.g., *CLM v CLN*), and Hong Kong routinely issue these orders to major VASPs. If an exchange fails to comply, much like in the offshore DIFC Courts, the remedy is typically **Contempt of Court**. While contempt is highly coercive, risking asset sequestration, heavy fines, or the committal of corporate directors, it does not automatically mutate the underlying commercial debt onto the exchange’s balance sheet simply for a missed administrative deadline. Historically, DIFC disclosure orders have been favored because this threat of penal sanctions ensures swift compliance, but they operate fundamentally differently from the UAE mainland’s strict financial liability mechanism.

United States (The Garnishment Default Parallel): Interestingly, the UAE’s Article 259 mirrors some of the strictest elements of US post-judgment enforcement. Under US Federal Rule of Civil Procedure 69, which defers to state law for execution, creditors may serve writs of garnishment on banks and VASPs. In certain strict state jurisdictions, if a garnishee fails to file a timely answer, the court may enter a default judgment against the garnishee for the *full amount of the underlying judgment*, regardless of how much crypto the exchange actually held. The UAE Court of Cassation has effectively solidified this similarly unforgiving standard

onshore.

Conclusion

The Dubai Court of Cassation has sent a definitive message: mainland disclosure orders are strict legal mandates bounded by rigid statutory deadlines. While common law crypto hubs rely on the coercive power of contempt to enforce third-party disclosure, the UAE mainland leverages the threat of immediate, substantive financial liability.

For crypto exchanges, financial institutions, and major commercial entities operating in the UAE, internal compliance protocols must be urgently reviewed to account for what could occur under these newly established procedures. Any notification from a UAE court regarding a third-party attachment should trigger an immediate, formal legal response. The seven-day clock is absolute. Jurisdictional objections, corporate veil defenses, or factual denials must be actively pleaded before the Execution Judge within this critical window. In the modern landscape of UAE litigation, a failure to respond is no longer just a procedural misstep, it could act as a total assumption of liability.

We invite corporate leadership, in-house counsel, and VASP compliance departments to engage with our specialist dispute resolution team at Wasel & Wasel to audit, strengthen, and, where necessary, systematically defend their positions in this exacting regulatory environment.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com