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 23, 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 23, 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]

Stakeholder / Asset Category	Reported Scope in the $6.3B Breach	Legal & Operational Status	Primary Procedural Mechanism
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 23, 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 23, 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 23, 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 23, 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 23, 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

Code and Copyright: The UAE's First NFT Judgment

November 23, 2026

As the digital asset economy matures, the legal infrastructure governing it is inevitably tested. Commercial disputes in the Web3 space, spanning breach of contract, intellectual property, and licensing, are transitioning from theoretical debates to practical litigation.

In a recent sequence of rulings, the Dubai Courts issued what is understood to be the first judgment in the United Arab

Emirates, and potentially the wider MENA region, addressing the application of copyright law to Non-Fungible Tokens (NFTs). Our firm acted for the plaintiff in this matter. The resulting judgments across the Court of First Instance, the Court of Appeal, and the Court of Cassation provide a structural framework for how work-for-hire agreements, the transfer of economic rights, minting rights, and joint authorship operate within the digital asset sector.

The Factual Baseline

A work for hire agreement had been entered into between a digital artist (the plaintiff) and a Web3 enterprise (the defendant). The objective of the project was accurately defined by the courts, demonstrating judicial recognition of generative NFT mechanics as:

"…designing tens of thousands of digital artistic elements, including three-dimensional characters for different creatures…in addition to background designs, bodies, faces, and accessories, to be used cumulatively in the project, and the creation of a massive library of elements that provide the required diversity for more than ten thousand digital editions."

The contract stipulated a six-figure amount for the transfer of the financial rights to the artworks, structured with an upfront payment and the balance due upon the public launch of the project.

The plaintiff delivered the digital assets, and the project launched. However, citing liquidity constraints, the defendant failed to remit the remaining balance. Despite the lack of full payment, the enterprise proceeded to mint the NFTs and commercialize the digital characters.

The plaintiff initiated litigation to recover the unpaid balance and requested an injunction to halt further commercial use and minting of the digital works until the financial

obligations were settled.

Copyright Application and Digital Delivery

A threshold issue was whether the digital files and generative elements qualified as protected works. The courts did not treat the assets as a legal anomaly, firmly situating them within the ambit of UAE copyright law, specifically Federal Decree-Law No. 38 of 2021 on Copyrights and Neighboring Rights.

The courts also addressed the mechanics of digital delivery. To prove fulfillment of the contract, the Court of Cassation evaluated electronic evidence and validated cloud storage transfers as a completed handover, stating:

"…the respondent delivered the digital artistic works subject of the agreement, and notified the company of the readiness of the final high-resolution copies, and requested the provision of storage space to upload approximately 70 gigabytes of files, and the company replied confirming the granting of access permissions… which makes it clear that the respondent uploaded and delivered the works and their possession transferred to the company…"

Specific Performance and Injunctions

A primary legal tension revolved around the status of the economic and minting rights, given the defendant's failure to complete payment. The plaintiff sought to halt the ongoing use and minting of the artwork.

Establishing the baseline mechanics of the IP transfer, the court-appointed intellectual property expert concluded that the enterprise did not inherently secure the copyright merely by possessing the digital files. The expert report, cited by the courts, explicitly stated:

"…the transfer of intellectual property rights to the first

defendant is linked to the payment of the full agreed fees to the plaintiff.”

However, the courts identified a structural contradiction in the plaintiff’s approach to enforcing this default rule.

By suing for the remaining payment, the plaintiff was fundamentally demanding the specific performance of the contract. Under contract law, a party cannot enforce a contract’s payment terms while simultaneously attempting to enjoin the transfer of the very rights that the payment purchases.

The Court of First Instance articulated this clearly, ruling:

“The court points out that this request contradicts the claim for the outstanding balance under the contract, as that request is a demand for the validity and enforceability of the contract, and therefore, by granting that request, the rights to the works and drawings transfer to the first defendant, and it has the right to use them.”

The Court of Appeal noted:

“…the latter has become the owner of the rights to those drawings sold to it by the appellant, and the intellectual property rights to those drawings transfer to it upon the payment of the appellant’s dues.”

This logic also addressed the plaintiff’s attempts to claim moral damages for the unauthorized tokenization of the art. Because the plaintiff elected to pursue the financial balance, the Court of Appeal ruled that the enterprise’s subsequent minting of the NFTs could not be considered an abusive exploitation or a breach of the artist’s moral rights, stating:

“…the appellant, by obtaining the consideration for his sale of those drawings to the first respondent, which necessarily

leads to the latter having the right to use those drawings in the manner it sees fit."

In the context of Web3, this confirms that once economic rights transfer under an enforced agreement, the creator cannot rely on moral rights to dictate or restrict the buyer's choice to mint the assets on a blockchain.

The Court of Cassation finalized this framework regarding the transfer of intellectual property under a work-for-hire agreement, stating:

"…the financial and intellectual property rights for the artistic works subject of the contract transferred to it considering them as completed works within the framework of a work for hire agreement."

A Procedural Note: To legal practitioners accustomed to other litigation hubs in Asia and Europe, such as Singapore, Hong Kong, London, Germany, or Paris, this finding may require procedural contextualization. In those jurisdictions, courts issue interim injunctive orders to temporarily freeze the minting or commercialization of a disputed digital asset while a substantive payment claim proceeds to trial. However, in the UAE, substantive trial courts generally do not issue interim injunctive relief within the primary merits claim itself; such interim relief is the purview of separate, urgent applications. Consequently, the UAE trial court consolidated the issues, ruling on the matter definitively in a single, final judgment. Because the court was adjudicating the final merits, its simultaneous confirmation of the debt owed and denial of the injunction were intrinsically linked. The court recognized that it could not finalize the financial execution of the contract while simultaneously blocking the transfer of the very commercial rights that the payment purchased.

The Adverse Position: Securing an Injunction Against Minting

The court's observation that a claim for the outstanding

balance contradicts a request for an injunction provides a clear roadmap for future Web3 litigation. By dictating that enforcing payment perfects the transfer of minting rights, the judgment identifies the specific legal posture required to successfully halt an unauthorized mint.

To secure an injunction against a Web3 enterprise, a creator must adopt the adverse position. Rather than suing for specific performance (the unpaid balance), the plaintiff must seek the rescission or termination of the contract due to a material breach, such as non-payment.

By petitioning the court to dissolve the agreement, the transfer of economic rights is nullified. The copyright reverts to or remains entirely with the creator. In this posture, any subsequent minting of the digital assets by the enterprise transforms into an actionable copyright infringement under UAE law, potentially satisfying the prerequisites for injunctive relief.

Global Jurisdictional Comparatives

This ruling places the UAE in direct dialogue with other major litigation hubs actively defining the intersection of copyright and digital assets.

In the United States, federal courts would look to 17 U.S.C. § 204(a) of the US Copyright Act, requiring a signed written instrument to transfer exclusive rights. US litigation frequently turns on contractual scope. In *Miramax v. Tarantino*, the core issue was whether legacy rights transfers implicitly included the right to exploit derivative works via NFTs. The UAE judgment bypasses medium-specific debates by recognizing that where a contract's factual purpose is the creation of an NFT collection, the general transfer of "economic rights" under Article 28 of the UAE Copyright Law inherently encompasses blockchain exploitation and minting, provided the financial terms are enforced.

In common law hubs like London, Singapore, and Hong Kong, courts have issued landmark rulings recognizing NFTs as legal property capable of being subject to proprietary injunctions. Cases such as *Osbourne v. Persons Unknown* in the UK and *Janesh s/o Rajkumar v. Unknown Person* in Singapore largely focused on the theft of the tokens themselves. These courts draw a strict distinction between the token as personal property and the underlying copyright, which is governed by statutes like the UK's Copyright, Designs and Patents Act 1988 or Singapore's Copyright Act 2021. The UAE judgment complements this global consensus by directly addressing the contractual transfer of the underlying generative art layers *before* they are minted onto the blockchain.

Joint Authorship in Decentralized Teams

The creation of the digital assets involved a co-creator who was not a named plaintiff in the lawsuit. Consequently, the Court of First Instance initially reduced the awarded payment.

The Court of Appeal overturned this reduction by applying Article 26 of the UAE Copyright Law, which governs joint works. The court relied on the statute, quoting:

"If several persons participate in the authorship of a work in such a way that the share of any of them cannot be separated from the other, all partners shall be considered equal authors of the work, unless otherwise agreed in writing… and each of them has the right to file lawsuits when an infringement occurs on any of the copyright rights protected by this Decree-Law."

This confirmed the NFT assets as an inseparable joint work and validated the plaintiff's standing to claim the entire financial balance on behalf of both authors, accommodating the decentralized reality of Web3 collaborations.

Furthermore, the litigation addressed a critical procedural hurdle common to Web3: the informal, cross-border nature of

decentralized collaborations. The defendants challenged the plaintiff's standing to claim his global co-creator's share, arguing that the written authorization between different artists was executed abroad and lacked official diplomatic legalization or state notarization, a traditional requirement in UAE litigation.

Recognizing the borderless reality of digital asset creation, the Court of Cassation dismissed this defense. Distinguishing between official state documents and private contracts, the court established a highly Web3-friendly precedent:

"…customary documents drawn up by individuals among themselves outside the State do not require authentication by official authorities in the country where they were issued to be accepted as evidence before the State's courts."

This vital procedural clarification ensures that international Web3 teams are not barred from enforcing their joint IP rights in the UAE merely because their internal governance agreements lack traditional, paper-based consular notarizations.

The Legal Reality

The sequence of judgments establishes a definitive baseline for the digital asset sector in the UAE. The rulings confirm that decentralized assets operate predictably within the established boundaries of copyright and contract law. The transfer of economic and minting rights in a work-for-hire context is directly linked to the remedy pursued by the claimant. Seeking the monetary enforcement of an agreement effectively validates the transfer of the underlying digital intellectual property. For developers, investors, and creators, the legal mechanics governing Web3 are proving to be just as critical as the underlying code.

Wasel & Wasel advises on complex commercial disputes, international arbitration, and digital asset litigation. The firm possesses deep expertise in navigating cross-border

fraud, tracing misappropriated funds, and securing interim equitable relief such as worldwide freezing injunctions and disclosure orders. By bridging the gap between local procedural frameworks and global common-law standards, Wasel & Wasel provides robust representation for corporate entities, tech developers, and international investors operating within the digital economy.

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: Paper Barrels and Physical Constraints – The Limits of Force Majeure in the 2026 GCC Energy Shock

November 23, 2026

"In the inevitable collision between paper contracts and physical supply chains, physical reality ultimately dictates the terms."

The Divergence of Paper and Physical Energy A recurring theme in macroeconomic and energy analysis is the fundamental disconnect between financial abstractions and physical reality. The modern economy operates on the assumption of uninterrupted primary energy flows. As the 2026 Iran War destabilizes the Arabian Gulf, the region is experiencing a severe, real-world stress test of that assumption.

While the Gulf Cooperation Council (GCC) remains the

undisputed epicenter of global hydrocarbon production, the intense militarization of shipping lanes and sudden refining bottlenecks have severely constrained the downstream supply of refined products. Diesel and bunker fuel are the master resources of the physical economy. Without them, the sprawling infrastructure pipelines in Saudi Arabia, the logistics hubs in the UAE, and the massive backup generators required for the region's data centers simply grind to a halt.

For years, procurement teams at major regional contractors managed their energy exposure through long-term, fixed-price diesel supply agreements. These contracts were viewed as ironclad hedges against market volatility. However, this strategy relied on the flawed premise that a paper contract can indefinitely command physical delivery, regardless of macroeconomic or geopolitical conditions. Paper barrels do not power generators.

Today, those fixed-price contracts are deeply out of the money. Spot prices for refined products have spiked dramatically, and commercial fuel suppliers are operating at severe losses with every truck they dispatch. Predictably, these suppliers are issuing sweeping "Force Majeure" notices, unilaterally suspending deliveries, and demanding immediate price renegotiations.

Within the region's commercial sectors, there is a growing misconception that extreme market volatility automatically excuses contractual performance. It is critical to examine this through the lens of established GCC civil law, which takes a highly structured, unsentimental approach to separating economic friction from true contractual impossibility.

The Unified GCC Legal Framework: Impossibility vs. Hardship When a fuel supplier unilaterally halts deliveries during a regional conflict, their primary defense is Force Majeure. However, the civil codes across the entire GCC, which share a deeply intertwined jurisprudential DNA heavily influenced by the Sanhuri model, draw a strict, unforgiving line between *absolute impossibility* and *extreme financial*

hardship.

Across the region, Force Majeure requires an unforeseeable event that renders the performance of a contract physically or legally impossible. Only then is the obligation extinguished. Conversely, the doctrine of *Exceptional Circumstances* (or Hardship) applies when an unforeseeable public event occurs and performance remains physically possible, but has become so economically burdensome that it threatens the supplier with "grave loss." Crucially, this doctrine does *not* allow the supplier to unilaterally terminate the agreement.

This vital duality is explicitly codified across the major Gulf jurisdictions:

- **The United Arab Emirates:** Article 273 of the Civil Transactions Law governs Force Majeure (impossibility), while Article 249 governs Exceptional Circumstances (hardship).
- **Kingdom of Saudi Arabia (KSA):** Under the recently enacted KSA Civil Transactions Law (Royal Decree M/191 of 2023), Article 125 dictates Force Majeure, whereas Article 97 provides for judicial intervention when unforeseeable circumstances make performance "oppressive" to the debtor.
- **Qatar:** The Qatari Civil Code (Law No. 22 of 2004) mirrors this structure precisely in Articles 258 and 171.
- **Oman and Kuwait:** Similar structural divides exist in the Omani Civil Transactions Law (Arts. 172 and 159) and the Kuwaiti Civil Code (Arts. 215 and 198).

Price Shocks Are Not Force Majeure To understand how regional courts apply these codes during commodity shocks, we can look to historical precedents. Following the 2008 global financial crisis and subsequent commodity supercycles, suppliers of highly volatile industrial materials faced catastrophic price spikes. Bound by fixed-price contracts, many claimed Force Majeure and halted deliveries.

The regional courts, setting a jurisprudential standard widely respected and cited across the GCC, have generally established a definitive rule: **A massive, unexpected increase in procurement costs, even if triggered by an unforeseeable geopolitical black swan, does not render a contract "impossible" to perform.**

If the physical molecules of diesel exist in the spot market, the supplier can technically procure and deliver them. The fact that doing so erodes profit margins and threatens the supplier's balance sheet constitutes a *relative* impossibility (hardship), not an *absolute* one (Force Majeure). Therefore, any supplier who unilaterally halts fuel deliveries based solely on market price surges is in material breach of contract.

The Judicial Pressure Valve The legal system, however, recognizes that rigidly enforcing economically ruinous contracts can trigger systemic cascading defaults across the supply chain. Bankrupting regional logistics providers serves neither the project owners nor the broader economy.

This is where the doctrine of Exceptional Circumstances acts as a vital pressure valve. It grants the presiding judge or arbitral tribunal the exclusive authority to intervene. By reviewing forensic financial data, a tribunal can equitably distribute the "grave loss." The judge may force the buyer to absorb a calculated percentage of the price surge, while mandating that the supplier continues deliveries at a newly adjusted rate.

The key legal distinction is procedural: the supplier cannot simply stop pumping fuel while demanding higher rates. They must maintain physical performance while formally petitioning the court to restore the economic balance of the contract.

When Sovereign Rationing Intervenes While market price surges do not trigger Force Majeure, the 2026 Iran War introduces a variable that absolutely does: Sovereign Energy Rationing.

If a GCC Ministry of Energy, national oil company, or sovereign military command issues a formal decree limiting commercial diesel allocations, perhaps capping them at 40% of

pre-war volumes to preserve strategic reserves, the legal paradigm immediately shifts.

A direct sovereign rationing order is a true “foreign cause.” It creates an absolute legal impossibility. If a supplier fails to deliver the remaining 60% of the contracted fuel because the state redirected the refinery output, they are completely shielded under the Force Majeure provisions across all GCC civil codes. The buyer cannot claim delay damages or demand the supplier procure fuel on the grey market to circumvent a sovereign mandate. When physical constraints are enforced by state power, the commercial contract must yield.

The Wartime Playbook for Energy Logistics For EPC contractors, heavy logistics operators, and energy suppliers navigating the supply constraints of the 2026 conflict, adhering strictly to regional legal frameworks is essential for mitigating risk:

- **For the Buyers – Audit the Notices:** Do not accept blanket Force Majeure notices at face value. If the supplier’s inability to deliver stems entirely from spot-market price inflation, issue a formal Notice of Breach. Regional jurisprudence makes it clear that market volatility is not a valid basis for unilateral termination.
- **For the Suppliers – Maintain Supply While Seeking Relief:** Unilaterally suspending fuel deliveries is a critical error that exposes the firm to substantial delay damages. Suppliers must continue physical performance while simultaneously invoking the Exceptional Circumstances provisions in local courts or tribunals to seek a formal, judicially mandated price adaptation.
- **For All Parties – Document Sovereign Intervention:** If fuel deliveries are halted due to state-imposed rationing, informal communications from downstream distributors are legally insufficient. To successfully invoke Force Majeure, the impacted party must formally serve the counterparty with the published government

decrees, ministry circulars, or military orders demonstrating that the shortfall was dictated by sovereign mandate rather than commercial preference.

Takeaway The 2026 Iran War has profoundly disrupted the fundamental inputs of regional commerce. Businesses find themselves navigating a narrow corridor between severe price surges and the reality of state-level resource rationing. The assumption that fiat agreements can entirely insulate operations from physical supply chain shocks is no longer viable.

The GCC civil law frameworks provide a pragmatic, structured mechanism for managing this disruption. The law rigorously protects the sanctity of contracts against mere market panic, while allowing for judicial intervention to prevent systemic economic collapse. Companies cannot use geopolitical volatility to unilaterally walk away from unprofitable agreements, but they can leverage statutory doctrines to ensure an equitable sharing of the wartime burden. Ultimately, success requires aligning legal strategy with physical market realities.

Wasel & Wasel advises on complex commercial disputes, international arbitration, and cross-border financial litigation. The firm represents major corporate entities, regional contractors, and energy suppliers in high-stakes proceedings before various courts and tribunals across the GCC. Our practice includes navigating complex force majeure claims, litigating the application of exceptional circumstances and contract adaptation, managing multi-jurisdictional supply chain disputes, and enforcing contractual rights amidst geopolitical crises and sovereign interventions.

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

Secondary Market Misrepresentation in Crypto: Insights from the Ontario Superior Court of Justice

November 23, 2026

A recent decision by the Ontario Superior Court of Justice in *Banach v. Galaxy Digital Holdings Ltd., 2026 ONSC 4534* is emerging as a critical reference point for digital asset investors, class actions, and corporate disclosure obligations. The judgment establishes decisive principles regarding secondary market misrepresentations, the assessment of materiality for cryptocurrency disclosures, and the liability associated with the promotion of algorithmic stablecoins. The ruling also sheds light on the broader implications for the permissibility and opportunity of class action crypto disputes globally. **Background**The precedent case arose from a class action against Galaxy Digital Holdings Ltd. ("Galaxy"), an investment company heavily engaged in the digital asset industry, and its senior management. The plaintiff alleged that Galaxy failed to disclose material risks associated with its core digital asset holdings, specifically Luna and its associated algorithmic stablecoin, TerraUSD. Between May 2021 and May 2022, Galaxy's CEO heavily promoted Luna. However, in May 2022, Luna and TerraUSD entered a "death spiral," wiping out $40 billion in market value globally, which resulted in a 42.9% drop in Galaxy's share price and a $300 million quarter-to-date loss.

The plaintiff claimed that Galaxy's public disclosures during the class period contained misleading omissions regarding the

operation and inherent risks of the Terra blockchain and algorithmic stablecoins, particularly the risk of a "death spiral," whilst simultaneously selling their Luna holdings.

The Court's Key Findings The Ontario Superior Court granted the plaintiff leave to proceed under the Ontario Securities Act and certified the action as a class proceeding. The Court's detailed judgment provided several critical findings:

- **Materiality Exceeds Strict Percentages:** The defendants argued that Luna was a relatively small portion of Galaxy's total portfolio during most of the class period and was therefore not legally material. The Court rejected this quantitative defense in full. It held that the test for materiality is whether the omitted information would significantly alter the "total mix of information" available to a reasonable investor. The intense promotional campaign by Galaxy's CEO made Luna fundamentally material to the company's valuation in the eyes of the market, demonstrating that risks cannot be ignored based on percentage alone.
- **Public Corrections:** Following the collapse of Luna, the CEO issued public statements acknowledging the risks of algorithmic stablecoins and the resulting losses. The defendants dismissed these as *ex post facto* musings. However, the Court categorized these statements as actionable "public corrections," revealing to the market the material facts and risks that Galaxy was obligated to disclose all along.

Comparing Permissibility of Class Action Crypto Disputes in Global Jurisdictions The *Banach* decision highlights Canada's permissive "opt-out" class action regime, which seamlessly aggregates massive retail investor claims. For digital asset issuers and exchanges operating globally, the permissibility of class action crypto disputes varies drastically across other major jurisdictions:

- **London (England & Wales):** The English legal system does

not possess a direct equivalent to the North American opt-out class action for securities fraud. Claimants generally rely on Group Litigation Orders (GLOs) under the Financial Services and Markets Act (FSMA) or representative actions. GLOs operate on an "opt-in" basis, requiring upfront funding from each claimant. Representative actions require all claimants to share the "same interest," making it exceedingly difficult to aggregate the claims of retail investors who purchased digital assets at varying times and prices.

- **Hong Kong & Singapore:** Neither Hong Kong nor Singapore currently supports a statutory class-action regime. Mass claims are limited to traditional representative proceedings, which mandate a rigid "same interest" test. Consequently, mass retail actions over crypto market misrepresentations face significant procedural hurdles. These jurisdictions heavily favor bilateral commercial litigation and institutional arbitration for digital asset disputes, limiting the threat of plaintiff-driven mass securities torts.
- **DIFC (Dubai) & ADGM (Abu Dhabi):** As leading offshore common law jurisdictions in the Middle East, the DIFC and ADGM provide highly sophisticated courts capable of handling complex digital asset disputes. While they offer mechanisms for group litigation, these operate on an opt-in basis. Neither jurisdiction permits the sweeping, opt-out class actions seen in Ontario, thereby providing an efficient venue for organized institutional investors but inherently shielding token issuers from the asymmetric exposure of North American retail class actions.

Looking Ahead The Ontario Court's decision serves as a definitive warning that generic risk disclosures are insufficient for complex digital assets and that public promotional activities can elevate an asset's legal materiality. Categorizing bespoke digital assets under generic

umbrellas constitutes a material misrepresentation if unique structural risks are omitted. For global practitioners and stakeholders operating in this space, navigating the distinct procedural realities of global financial hubs will be essential for effective collective redress and mitigating exposure to class actions.

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