DUE DILIGENCE
FORENSIC VERIFICATION & FRAUD RISK REPORT

Subject Entity: FAKHR ALARD TRADING L.L.C. (فخر الأرض للتجارة ذ.م.م) **-** Dubai, UAE
License No.: 1111966 | Register No.: 2674000 | Chamber No.: 425581
Report Date: 07 August 2026
Matter: Non-payment for goods, USD 16,000; invalid transfer advice; dishonoured/evasive counterparty

1. EXECUTIVE SUMMARY

Overall Risk Score: 81/100 - CRITICAL (fraud-consistent profile).

The subject entity is a genuinely registered Dubai LLC (its license record is corroborated by multiple independent registry aggregators and its own live web footprint), but the transaction file exhibits the classic anatomy of **a goods acquisition fraud executed through a registered shell**:

The payment instrument trail is fabricated or abusive. The "transfer confirmation" of 04/08/2026 lacks every security attribute of a genuine UAE bank remittance advice (no UETR, no MT103 reference, no bank branding), names a beneficiary ("NAVSER MARITIME LTD") different from the cheque payee (the Turkish seller "NAVSER MARINE ELEKTRONIK VE HABERLESME SISTEMLER"), and has been proven invalid-i.e., it is a **counterfeit bank document** used to induce release of goods.

The "**GUARANTEE**" cheque (AED 58,720) was drawn on a brand-new account - MICR cheque serial 000002 on a Mashreq neobiz (**Digital-Onboarding**) account, the typical low-friction account structure used to issue valueless security cheques.

The digital footprint is disposable: the corporate domain fatradingllc.com was registered only on **10 April 2026** with garbage/privacy WHOIS data and a third unexplained mobile number; the license's own contact is a free Gmail address; the business card pairs one employee's name with another person's e-mail ("h.kapur").

A prior market participant has already flagged the entity: a B2B platform record states, "We performed DD towards this company and suspected a scam buyer." The entity's real trade is onions/avocados/produce (customs data, Al Aweer Fruit & Vegetables Market address), the purchase of USD 16,000 of marine electronics from a Turkish marine-electronics firm is off-profile, a hallmark of scam-buyer solicitations, and the entity was actively soliciting further foreign suppliers (seafood, meat) on the same pattern.

Evasion after delivery completes the fraud: goods released → payment failed → contact ceased.

The owner identified on the license (100% owner/manager, Pakistani national, Emirates ID 784-1986-6811423-8) is the same person named on the Emirates ID provided, and his ID lists as employer a linked entity, Fakhr Alard IT Solutions Co. L.L.C., registered at the same office (1906, SIT Tower, Dubai Silicon Oasis) and appearing on MOHRE's restricted-employer list - a related-entity cluster useful for asset tracing and, potentially, veil-piercing

2. Verification Methodology

Corroborative OSINT exhibits company website live with license phone (+971 52 1275 092); LinkedIn "General Manager" page (21 followers); customs data showing produce imports (e.g., NEW RED ONION, 20/12/2025); B2B listings ("junior buyer… avocados… founded 2025"); **freshdi record: "We performed DD towards this company and suspected a scam buyer"**; further live solicitations for seafood/meat CIF Jebel Ali on the same pattern; victim entity Navser Marine verified as a genuine, established Istanbul marine-electronics company (est. 2013, MarineTraffic/industry listings) confirming the seller is legitimate and the cheque payee naming is accurate, which throws the advice's "NAVSER MARITIME LTD" beneficiary into sharper relief as a fabrication/misdirection (unless the client confirms it as a group entity-confirm immediately).

3. VERIFICATION FINDINGS BY CRITERION

3.1 License authenticity/status & registry match. The license is probably genuine as a registry record: third-party registry/credit data reproduce its key fields (name, Office 1906, POB 47809), the renewal receipt is internally consistent, and the entity has a real (if thin) operating footprint (produce imports; market shop). Official re-verification must be run via the DET "Search License Information" service / u.ae license-enquiry gateway / MoE company enquiry. Conclusion: **a real registered shell-genuineness of the license does not negate fraud; it identifies the perpetrator**.

3.2 Owner identity match. License owner (Person No. 1199381, 100%) = Emirates ID holder (name string identical). MRZ consistent. ICA e-verification required for court-grade confirmation. **Match: YES (provisional)**.

3.3 Signatory authority. The only natural person with stated authority is the owner/manager Sohail. The cheque signature is illegible and unverified against the bank's specimen (obtainable only via police/court). The negotiator "Muhammad Asif" (Purchase Executive) has no documented authority; the card's e-mail belongs to a different individual ("H. Kapur"); the WHOIS registrant ("pm", +971.582825679) is a fourth actor. **Authority chain is broken/multi-actor-procure the account mandate and the contract signatory's authorization (POA/mandate) via the criminal file**.

3.4 Cheque genuineness (MICR/endorsement). Physically coherent with the stated IBAN; serial 000002 indicates a newly opened account; no endorsement chain (payee-only instrument). Genuineness of stock/signature requires presentment + specimen comparison + (if contested) questioned-document examination**. Risk: Designed To Dishonour**.

3.5 Payment traceability. The "transfer" is untraceable by design: no UETR/MT103; proven invalid. The account …463 exists per the cheque IBAN, but funding status unknown until presentment/police subpoena. **Traceability: FAIL (Traceable Upon Presentment)**.

3.6 Timestamps. Sequence is fraud-consistent: cheque (24/07, security) → forged advice (04/08 09:14, inducement to release goods) → goods released → evasion → license PDF generated & sent via WhatsApp (06/08 19:39, reassurance) → silence. Domain created only 10/04/2026. Owner ID issued 12/12/2024 (recent sponsor switch to the linked IT company). **Sequence: COHERENT WITH PRE-PLANNED FRAUD**.

3.7 Tampering indicators. ①: format/branding/UETR/beneficiary anomalies (counterfeit indicators). ②: name/e-mail mismatch. address mismatch; Gmail vs corporate domain. ③: employer mismatch (cluster indicator, not tampering per se). On remote review; MRZ/IBAN mathematics are internally clean-consistent with genuine identity documents and genuine license being used as instruments of fraud, **which is the dominant UAE shell-fraud pattern**.

4. FORENSIC ANALYSIS PLAN (CHEQUE & TRANSFER ADVICE)

4.1 Cheque

- Immediate presentment through the client's bank via UAE clearing; obtain the dishonour/partial-payment record - this both evidences dishonour and converts the cheque into an executive instrument for direct execution before the execution judge (current post-2022 regime).

- Specimen-signature & mandate pull (Mashreq, via police/court order): confirms signatory authority and whether the account was closed/starved (bad-faith indicators that revive criminal liability).

- Questioned-document examination (if forgery is pleaded): ink, MICR toner, stock comparison with genuine Mashreq neobiz stock; latent fingerprints on the instrument (police lab).

- Account history subpoena: opening date (expect ≈ July 2026), inflows/outflows, signatory, KYC phone/e-mail (cross-match against WHOIS number +971.582825679 and card numbers).

4.2 Transfer advice

- Email/header forensics on the native message: SPF/DKIM/Return-Path, originating IP, Message-ID domain-to prove non-Mashreq origin and identify the sender infrastructure.

- PDF/metadata & typographic comparison against authenticated Mashreq advices (reference-format "033DBFG…" atypical; absence of UETR field decisive).

- SWIFT trace: written confirmation from Albaraka Turk (no receipt; no UETR) and from Mashreq that reference 033DBFG251992193 corresponds to no executed payment instruction-the foundational forgery evidence.

- Bank-impersonation referral to Mashreq's Fraud & Investigations Unit (the bank has independent interest in pursuing counterfeit advices naming its brand and a neobiz account).

5. Recommended posture:

treat this as a criminal fraud matter with a parallel executive-instrument (cheque) enforcement track. Given the modest claim size (AED 58.7–58.9k), the economics favour high-leverage, low-cost remedies (cheque execution + criminal complaint with travel ban) to force settlement, rather than full civil litigation. Act within 72 hours: the owner's residency/ID expires 11/12/2026 and the license lapses 25/10/2026 - both are natural exit/dissolution windows creating flight risk.

6. CONCLUSION

The subject is a genuine registration used as a fraud vehicle: a real license, a real (matched) owner, and a real produce-trading operation providing cover, combined with a counterfeit bank transfer advice, a new-account security cheque, a disposable digital footprint, a prior "scam buyer" flag, and post-delivery evasion. Risk score 81/100 (Critical). The file is strong for a criminal fraud complaint (Arts. 451 FDL 31/2021; FDL 34/2021) and for cheque execution, with the owner's residency (travel ban) as the decisive leverage. Initiate Phase 0 within 72 hours - the Oct-2026 license lapse and Dec-2026 ID expiry define the outer window of effective enforcement.

Prepared: 07/08/2026