Conflict-Driven Fraud

Guidance For Businesses — April 2026

The current conflict environment is creating a materially elevated fraud risk landscape across the Gulf. Rapid operational shifts, heightened geopolitical sensitivity, and increased regulatory activity are being actively exploited by fraudsters through impersonation, social engineering, and supply chain manipulation.

For businesses operating in or exposed to the region, this is not a theoretical threat: it requires immediate, practical adjustments to controls, awareness, and decision-making processes. Themis Powered by Tathabbat has put together the following guidance to help businesses navigate the current fraud risk landscape.

1. Treat Conflict-Linked Communications as High Risk by Default

Fraudsters are systematically exploiting the language of crisis — urgency, disruption, sanctions, and security — to bypass standard controls.

Apply heightened scrutiny to any communication referencing:

- [ ] Sanctions updates, regulatory directives, or compliance changes
- [ ] Urgent payment requests or capital reallocation
- [ ] Supply chain disruption or rerouting

Independently verify all such requests using pre-existing, trusted contact details

- [ ] Reinforce a “pause and verify” culture across finance, legal, and operations teams

2. Conduct Enhanced Network and Counterparty Due Diligence

In a conflict environment, financial crime risks can often be embedded in counterparties, intermediaries, or cross-border operations.

- [ ] Map ownership and control structures across counterparties and their affiliates
- [ ] Identify indirect exposure to high-risk jurisdictions, sanctioned actors, or intermediaries

Use network-based analysis to detect:

- [ ] Hidden beneficial ownership
- [ ] Shared directors, addresses, or service providers
- [ ] Unusual transaction patterns across linked entities
- [ ] Reassess existing relationships — not just new ones — as risk exposure may have shifted

3. Strengthen Payment and Transaction Controls

Business Email Compromise (BEC), vishing, and executive impersonation attacks are increasing in both volume and sophistication.

- [ ] Enforce dual authorisation for all payment instructions and changes to bank details

Require out-of-band verification (e.g. phone call to known contact) for:

- [ ] Payment amendments
- [ ] New counterparties
- [ ] Urgent or time-sensitive transactions
- [ ] Introduce escalation thresholds for high-value or conflict-linked transactions

4. Tighten Third-Party and Supply Chain Due Diligence

Fraudsters are inserting themselves into disrupted supply chains — particularly in logistics, energy, and security services.

- [ ] Treat new intermediaries offering "conflict solutions" (e.g. alternative routing, security support, expedited services) as high risk

Independently verify:

- [ ] Corporate registration and beneficial ownership
- [ ] Physical presence and operating history
- [ ] Links to known logistics providers

Scrutinise invoices referencing:

- [ ] Fuel surcharges
- [ ] Security premiums
- [ ] Emergency routing or insurance costs

5. Prepare for Brand Impersonation and Investor Targeting

Gulf-based firms — particularly high-profile entities such as sovereign wealth funds, financial institutions, and large corporates — are being used as lures in fraud schemes.

Monitor for unauthorised use of your brand in:

- [ ] Fake investment opportunities
- [ ] Forged term sheets or co-investment proposals
- [ ] Spoofed domains and email addresses
- [ ] Alert clients, partners, and stakeholders to known impersonation risks
- [ ] Establish rapid takedown and response processes for fraudulent content

6. Enhance Cyber and Social Engineering Defences

The convergence of cyber threats, fraud, and disinformation is accelerating.

Issue targeted internal alerts on:

- [ ] Phishing and vishing campaigns linked to the conflict
- [ ] Deepfake-enabled impersonation attempts
- [ ] Conduct refresher training for high-risk functions (finance, HR, senior executives)

Test incident response plans against:

- [ ] Ransomware or account compromise

- [ ] Fraudulent payment scenarios
- [ ] Reputational attacks driven by false information

7. Monitor Sanctions and Regulatory Developments Closely

Fraudsters are exploiting confusion around rapidly evolving sanctions regimes and regulatory expectations.

Track updates from:

- [ ] UN, OFAC, OFSI, EU, and relevant Gulf regulators
- [ ] Treat unsolicited "compliance notifications" or "regulatory directives" with caution
- [ ] Verify all regulatory communications through official channels

Ensure internal teams understand:

- [ ] Sanctions obligations
- [ ] Escalation procedures
- [ ] Red flags for circumvention or fraud

8. Train Staff and Raise Awareness Across the Organisation

Human vulnerability remains one of the most exploited entry points for fraud.

Deliver targeted training on:

- [ ] Conflict-linked fraud typologies
- [ ] Impersonation and social engineering techniques
- [ ] Red flags specific to your sector and region
- [ ] Run scenario-based exercises (e.g. simulated BEC or phishing attacks)
- [ ] Ensure staff understand escalation pathways and feel empowered to challenge suspicious requests
- [ ] Reinforce awareness regularly — not as a one-off exercise

Bottom Line

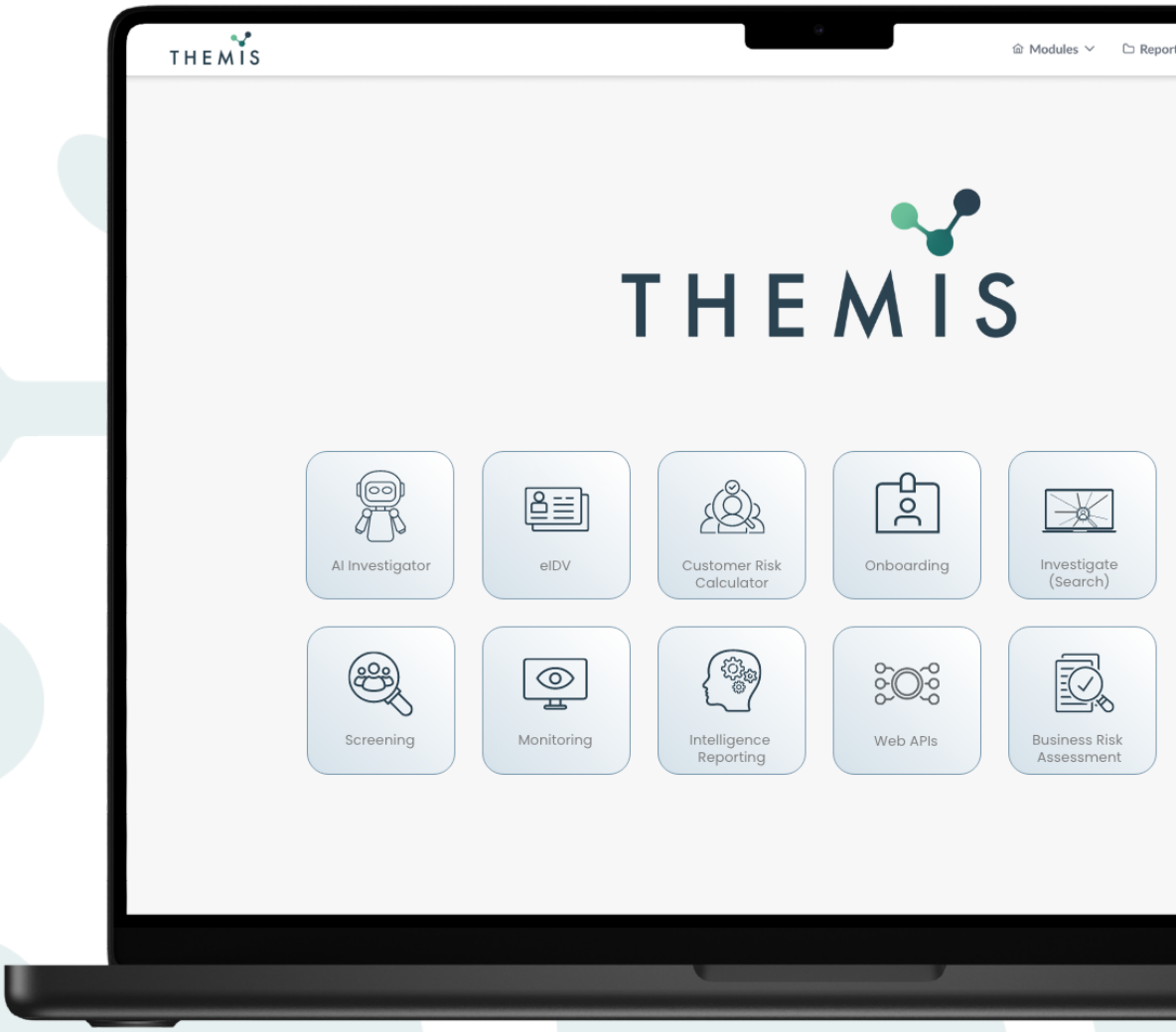
Businesses are facing a dual risk: being directly targeted by fraud, and having their brand, infrastructure, or market position exploited to target others.

In this environment, traditional controls are necessary but no longer sufficient. What is required is a shift toward **threat-aware operations and an investment in tech defences** — where conflict dynamics, fraud typologies, and geopolitical developments are actively integrated into day-to-day decision-making.

As ever, Themis Powered by Tathabbat is on hand to offer support as we all navigate our way through the conflict. If you are concerned about any of the threats outlined in this note, please contact us. Themis Powered by Tathabbat offers tailored Board-level and Senior Management threat intelligence briefings.

Get in Contact
click here

Your Complete Financial Crime Defence Platform



TATHABBAT

Manama | Riyadh | Abu Dhabi | Dubai | London

UK: +44 (0) 20 8064 1724 | UAE: +971 (0)2 676 7453

info@tathabbat.ai

tathabbat.ai