10xDS / 10xVerify

One Payment Change.
A Product was Born.

Case Study 001 | UAE office rental | May 2026



AED 12,845

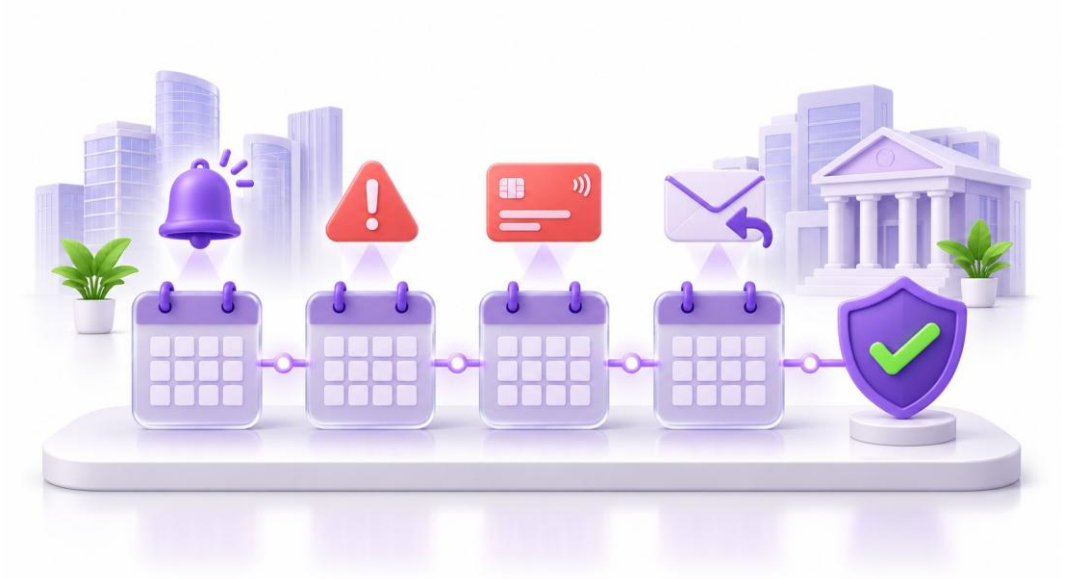
Payment potentially at risk

No Payment made

Suspected attempt, not proven fraud

WHAT HAPPENED

- **04 MAY:** Rental payment reminder received
- **08 MAY:** Instruction not to use the usual bank account
- **18 MAY:** New Emirates NBD account details supplied
- **18 MAY:** Internal reply proposed replacing existing bank details



WHY IT MATTERED

- A genuine commercial relationship can carry an unverified payment instruction.
- A different email domain is a warning sign, not proof of compromise.
- A changed beneficiary requires independent verification before approval.

THE 10xVERIFY RESPONSE

VERIFY THE BUSINESS:

Registration, directors and business identity

VERIFY THE CHANNEL:

Domain, email and communication signals

VERIFY THE CHANGE:

Independent bank-detail confirmation and approval

10xVerify: Born from a Real Attempted Payment Fraud

One suspicious payment instruction. One changed bank account. One important lesson.

In May 2026, Transformation Technology Services, associated with the 10xDS business group, encountered a suspected payment-diversion attempt involving a routine office rental payment in the UAE. The payment amount was AED 12,845. The rental relationship was genuine, the payment was expected and the correspondence appeared within an established conversation with the service provider.



But the payment instructions changed. The sender directed the company to use a new bank account, while messages in the chain involved an email domain different from the supplier's established business domain. This raised a critical question: **was the requested beneficiary change genuinely authorized?**

No payment was made to the questioned account. The available correspondence does not establish that the bank account was fraudulent or that an email account was compromised. It does, however, illustrate a payment-control risk that businesses face every day.

The incident: what the records show

4 May: An established supplier contact sent a reminder for the rental installment due on 22 May 2026.

8 May: A message advised that the usual bank account should no longer be used.

18 May: A new Emirates NBD account was provided, with a request to transfer the funds that week. An internal response indicated an intention to update beneficiary records.

No payment was subsequently made to the questioned account.

The alternative email domain appeared in correspondence as early as January 2026. This matters: its presence is a reason to verify the communication channel, but not evidence on its own that a criminal introduced it in May.

The weakness was not necessarily the supplier. **It was the change.**

Organizations often check a vendor at onboarding, then treat later invoices and messages as routine. But a genuine supplier relationship can be used as the setting for a false payment instruction. A real invoice, familiar conversation or plausible sender name cannot independently prove that a new beneficiary account belongs to the intended payee.



For this reason, bank-detail changes should trigger a fresh control: verify through a trusted contact channel already on file, confirm the legal beneficiary using reliable banking or documentary evidence, and require a separate approval before changing payment instructions. Email replies within the same thread are not an independent confirmation.

From internal problem **to product**

This incident became the starting point for 10xVerify, conceived as a way to help organizations verify vendors and sensitive payment instructions before releasing funds. The idea expanded from a single use case into a wider business verification and risk assessment product.



10xVerify is intended to bring together checks on corporate existence, registration, directors, address, digital footprint, domain signals, legal and financial risk indicators, and ongoing changes in vendor records. Its most important control is not simply producing a risk score: it is **routing unusual changes for independent validation, human review and documented approval**.

How 10xVerify would **approach this case**

1. **Establish a trusted baseline.** Record the approved supplier identity, official domains, known contacts and previously verified beneficiary details.

2. **Detect the exception.** Identify a request to change banking instructions and flag differences between the sender domain and established supplier records.

3. **Verify independently.** Contact the supplier using a previously validated phone number or channel, rather than details supplied in the change request. Validate the beneficiary name and account information using available authorized methods.

4. **Require approval.** Place the proposed change on hold until the evidence is reviewed and an authorized person approves it.

5. **Preserve an audit trail.** Record the request, verification evidence, decision, approver and any follow-up monitoring.

⚠ These are proposed controls, not a claim that 10xVerify was deployed during the May 2026 incident or that it could guarantee prevention of every fraud attempt.

A wider **business lesson**

The immediate potential exposure was AED 12,845, assuming the instruction was fraudulent. **The larger exposure is systemic**: businesses may make repeated payments to suppliers whose details change over time. Verification should therefore be a continuing process, especially when bank accounts, ownership, contact details or payment instructions change.



Verify the business. Verify the identity. Verify the change. Before you pay.

10x DS

Let’s build what’s next.

Partner with us to accelerate transformation and deliver measurable impact.

www.10xds.com

www.10xds.ai

Connect@10xds.com

