The Supplier Was Genuine. The Payment Wasn't.

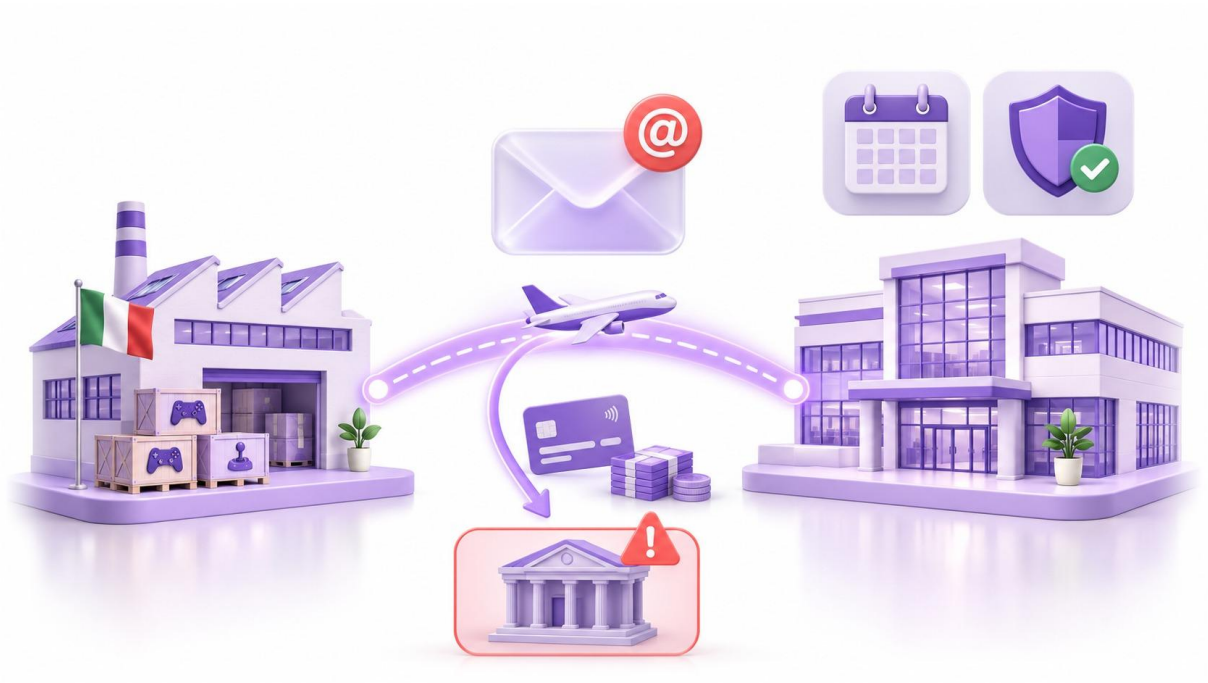
What the LuLu Group fraud teaches businesses about supplier verification and payment security

By 10xDS - Exponential Digital Solutions



A legitimate supplier. An apparently genuine invoice. An established business relationship. Yet approximately US$175,000 was reportedly diverted to fraudsters.

The recently reported fraud involving LuLu Group highlights a vulnerability in how businesses manage supplier relationships and payments.

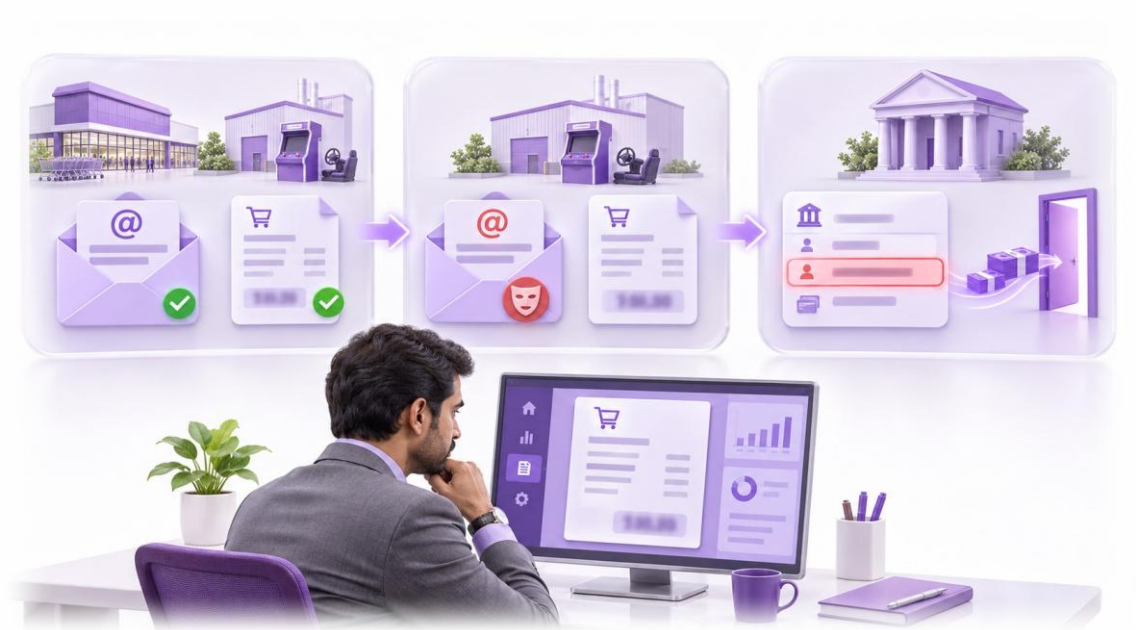


According to media reports published in October 2026, fraudsters allegedly impersonated IE Park S.R.L., an established Italian supplier of gaming equipment to LuLu Group. Using email addresses resembling those of the genuine supplier, the perpetrators reportedly sent fraudulent payment instructions that resulted in **approximately €150,500 (around US$175,000)** being transferred to accounts supplied by the impersonators.

Kochi Cyber Crime Police registered a case on 23 October 2026. The incident remains subject to investigation. The key question for every business is **whether it verifies only that its suppliers are genuine, or also verifies the people requesting payments and the accounts receiving them**.

How Supplier **Impersonation Fraud Works**

Supplier impersonation is a form of Business Email Compromise (BEC), in which criminals exploit established commercial relationships to redirect payments. The attacker may not need to break into a banking system. Instead, the attacker sends an email that resembles legitimate supplier correspondence and references an expected transaction.



The invoice may appear consistent with a genuine purchase order. The amount may be correct. The critical difference is a changed beneficiary bank account. If finance processes the request without independent confirmation, the payment may reach an attacker-controlled account.

This is the broad mechanism alleged in the LuLu case; the actual internal approval process and source of the attacker's information have not been publicly established.

The Real Weakness: **Trust Without Continuous Verification**

Many organizations check registration documents, tax information, bank details and contacts when onboarding a supplier. Subsequent invoices may then pass through routine workflows. But supplier legitimacy at onboarding does not prove that every future message and payment instruction is authentic.



Three different questions matter:

1. Is the supplier a genuine, active business?
2. Is this communication from an authorized supplier representative?
3. Does the payment beneficiary actually belong to the approved supplier?

> A company can answer the first correctly and still lose money on the second or third.

Introducing 10xVerify: **From Supplier Verification to Payment Protection**

10xDS is developing 10xVerify as a supplier and business verification platform. Its direction is to move beyond one-time due diligence toward continuous monitoring and payment-related verification. The objective is simple: **verify the supplier, verify the communication and verify the payment instruction.** The payment-specific capabilities described below are proposed extensions and should not be interpreted as already deployed functionality.

1

Supplier Identity and Background Verification

10xVerify can help assess legal existence, registration status, operating history, directors and ownership information where available, registered address, digital footprint, domain history, financial indicators and relevant adverse or sanctions information. Such checks can reveal inconsistencies before a supplier is approved.

2

Detecting Supplier Impersonation

A proposed communication-authenticity module would inspect sender domains, email authentication signals, unusual changes in correspondence and approved supplier contacts. A lookalike domain may differ by just one character. Automated detection can flag anomalies for human review, complementing rather than replacing existing email-security controls.



3

Invoice and Bank Account Verification

A proposed payment-verification module would compare invoices against purchase orders, approved supplier records and previously verified bank accounts. A newly introduced beneficiary or changed bank account would trigger an exception. The finance team would independently confirm the change through a previously authenticated contact channel, not the email requesting it. Where supported, regulated account-verification services could provide additional evidence.

4

Risk-Based Payment Screening

A proposed risk engine could examine new beneficiaries, suspicious domains, unusual amounts, changes in contact information, unexpected destinations and deviations from payment history. Low-risk items would follow normal approvals; medium-risk items would receive additional review; high-risk items could be held pending verification. Authorized personnel, not AI alone, should retain payment-release authority.

5

Continuous Supplier Monitoring

Supplier ownership, directors, domains, contact details and financial circumstances can change. Continuous monitoring can alert organizations to material changes and prompt targeted reviews. The purpose is not to treat every change as fraud, but to ensure that significant changes are verified.

What Would a Safer **Payment Process Look Like?**

1	An invoice arrives from a familiar overseas supplier.
2	The workflow checks the sender, matches the invoice to the purchase order and compares beneficiary details with approved records.
3	If the details match, it proceeds through normal approval.
4	**If the beneficiary has changed, payment is held until independent verification and authorization are documented.**
5	Every exception and decision is retained for audit.



This model reduces exposure, but no tool can guarantee that fraud will never occur.

Why This Matters
Beyond Retail

Hotels, manufacturers, healthcare groups, professional-services firms and shared-service centers process large volumes of supplier payments. Manual verification becomes demanding as volume rises. Technology can perform repeatable checks and surface exceptions; finance professionals can focus on judgment, independent confirmation and approval. **The goal is better information before money is released, not removal of people from financial controls.**



Five Questions Every **CFO Should Ask**

01	Do we independently verify every new or changed supplier bank account?
02	Can we detect impersonation through lookalike email domains?
03	Are supplier master-data changes approved separately from payment authorization?
04	Can we flag unusual payments before funds are released?
05	Do we retain an audit trail of verification, exceptions and approvals?

Moving From Reactive Investigation to **Preventive Verification**

Payment fraud creates costs beyond the immediate loss: investigation, bank coordination, evidence preservation, legal obligations and disrupted supplier relationships. The reported LuLu case illustrates why supplier verification should be an ongoing financial control rather than a one-time administrative step.



> **A genuine supplier does not automatically mean a genuine payment instruction. An invoice that looks correct does not prove the beneficiary is legitimate.** Before the next supplier payment, ask: are we sure who is receiving the money?

10xVerify by 10xDS

Don’t just verify who you’re buying from. Verify who you’re paying.

10xDS can help organizations assess supplier verification processes, identify control gaps and explore verification and monitoring capabilities. Request a Supplier Payment Fraud Exposure Assessment.

Sources and editorial note

Public reporting includes The New Indian Express (24 October 2026), The Economic Times and other Indian media. The reported amount was €150,500 (approximately ₹1.64 crore); US$175,000 is an indicative conversion, not a confirmed USD settlement amount. The attack remains under investigation. Internal control failures, system compromise, perpetrators and recovery status have not been independently established. Proposed 10xVerify controls are not a claim that the platform was involved in, or would certainly have prevented, this incident.

Reference:

https://www.newindianexpress.com/cities/kochi/2026/Oct/24/lulu-group-loses-rs-164-crore-in-alleged-email-impersonation-fraud



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