The Supplier Is Genuine. So How Can the Payment Still Be Fraudulent?

Description

When a Genuine Invoice Leads to a Fraudulent Payment

A supplier may be completely genuine.

The invoice may be genuine.
The goods or services may have actually been received.
The purchase may have been properly approved.
And the payment amount may exactly match the invoice.

Yet, the payment can still be fraudulent.

How?

The risk is not always the supplier. It can be the bank account.

Consider a simple situation.

A company regularly purchases goods from a genuine supplier. The supplier's name, GST details, invoices and transactions all appear legitimate.

At some point, the supplier's bank account details are changed in the company's records.

The new bank account may have been inserted or changed by someone within the accounts or finance process.

The payment is then made to the new account.

From the accounting records, everything may appear normal:

- Genuine supplier
- Genuine invoice
- Genuine purchase
- Correct invoice amount
- Proper approval
- Payment recorded against the supplier

But the money has gone to a different bank account.

In some cases, that account may belong to an employee, an employee's relative, or another person connected with the fraud.

This is why **verifying the supplier is not enough. The payment destination also needs to be verified.**

Why can this be difficult to detect?

Most accounting controls focus on whether the transaction itself is genuine.

For example:

Purchase Order ? Goods Received ? Invoice ? Approval ? Payment

If all these documents match, the transaction may appear completely legitimate.

But there is another question that is often overlooked:

Who actually owns the bank account to which the payment was made?

If the supplier's bank details were changed without independent verification, a genuine transaction can become a fraudulent payment.

A simple control that can reveal a serious problem

One practical review is to compare supplier bank-account information with employee-related bank-account information.

For example, take:

1. The list of active supplier bank accounts.
2. The list of employee salary bank accounts.
3. Compare the bank account numbers.
4. Where appropriate, also compare IFSC codes and account-holder names.
5. Investigate any unusual matches.

Suppose a supplier's bank account happens to be the same as an employee's salary account.

That does **not automatically prove fraud**.

There could be a legitimate explanation. For example, the employee may have a genuine business relationship with the supplier or may have been authorised to receive payments in a particular arrangement.

However, such a match is certainly a **red flag that deserves investigation**.

The same principle can be extended to other unusual relationships, such as supplier bank details matching accounts associated with employees or their related parties.

The bigger control: independently verify changes in bank details

The most important control is not simply comparing account numbers.

It is having a proper process whenever supplier bank details are changed.

For example:

Supplier requests change in bank details
?
Change request is documented
?
Supporting bank details are obtained
?
Independent verification is performed using previously known contact details
?
Change is approved by an authorised person
?
Bank details are updated in the accounting system
?
Payment is released

The key word here is **independent**.

If the same person who receives the bank-change request can also update the master data and release the payment, the control is considerably weaker.

What businesses should consider implementing

A few simple controls can significantly reduce this risk:

1. Maker-checker control

The person who changes supplier bank details should not be the same person who approves the change.

2. Independent verification

Do not rely solely on the email or message requesting the change.

Verify the change through an independent communication channel, such as a previously registered supplier contact number.

3. Maintain an audit trail

Every change to supplier master data should leave a record showing:

- Who requested the change
- Who made the change
- Who approved it
- When it was changed
- What the previous bank details were
- What the new bank details are

4. Review unusual matches

Periodically compare supplier bank details with employee and other relevant master data to identify unusual overlaps.

5. Review recently changed bank accounts

Payments made shortly after a supplier's bank details have been changed can receive additional scrutiny, particularly where the transaction is large or unusual.

What about the auditor?

This distinction is important.

The existence of a genuine supplier and genuine invoice does not, by itself, establish that the payment was made to the correct beneficiary.

At the same time, an auditor cannot be expected to detect every fraud simply because a fraud has occurred.

The nature and extent of audit procedures depend on the applicable auditing standards, the circumstances, the assessed risks and the controls in place.

For businesses, the practical lesson is therefore not to rely on the audit alone.

Fraud prevention starts with the company's internal controls.

The question every finance team should ask

When a supplier's bank details are changed, ask:

Does someone independent verify that the new bank account actually belongs to the genuine supplier before the payment is released?

If the answer is no, there may be a control gap worth addressing.

Because sometimes the supplier is genuine.

The invoice is genuine.

The purchase is genuine.

The approval is genuine.

And yet the money still goes to the wrong person.

That is why supplier verification and payment verification should be treated as two separate controls.

Final takeaway

A genuine supplier does not automatically mean a genuine payment.

The risk can sit between the invoice and the bank transfer, particularly when supplier master data can be changed without adequate verification.

A simple, well-designed process for **supplier bank-account changes, independent verification, maker-checker approval and periodic data analysis** can help businesses identify and prevent potentially costly payment fraud.

The real question is not only, “Is this supplier genuine?”

It is also:

“Are we certain that the money is going to the genuine supplier?”

Disclaimer:

This article is for general informational purposes only and should not be considered professional advice. Please consult a qualified expert for advice tailored to your specific situation. The author and website owner are not liable for any errors or actions based on this content.

Date
22/09/2026
Date Created
07/09/2026
Author
meetsoni