FISCAL TECHNOLOGIES

Executive Brief

Fraud prevention in the ECCTA Era

If your board asked, *"Can you demonstrate systematic fraud prevention?"* how confident would you feel?

In today's era of ECCTA, where failure to prevent fraud is an offence that could land your organisation a hefty fine and considerable reputational damage, this question is more important than ever.

DESPITE INCREASED REGULATIONS, FRAUD PERSISTS:

GLOBAL BUSINESSES LOSE

7.7%

OF THEIR REVENUE TO FRAUD EACH YEAR

TransUnion, H2 2025 Update to the Top Fraud Trends Report

£629.3M

UK REVENUE WAS LOST TO PAYMENT FRAUD AND SCAMS WITHIN 6 MONTHS

UK Finance, Half Year Fraud Report, 2025

58%

OF AP TEAMS EXPERIENCED FRAUD ATTEMPTS IN THE LAST 6 MONTHS

IOFM, February 2026

UK INVOICE AND MANDATE SCAM LOSSES TOTALLED

£32.4M

LAST YEAR FOR BUSINESSES

UK Finance, Annual Fraud Report 2025

SUPPLIER IMPOSTER FRAUD

INCREASED 11%

IN 2024

AFP, Payments Fraud Survey, 2025

Recorded Future's 2026 Payment Fraud Report notes that fraudsters are increasingly accessing industrialised support services and tooling to maximise effectiveness at scale.

Fraudsters are getting smarter, and they're targeting areas where they know organisations are vulnerable.

Existing fraud controls need improvement.

Modern finance teams are under pressure to perform to a high standard already. But identifying fraud is tricky, and there are more plates to spin with staff shortages, larger supplier files and a growing number of invoices to check. Controls are getting more difficult to perform at the level required by legislation, and some technologies aren't as sophisticated as you need them to be.

While ERPs can catch some issues that indicate a fraud attempt, the reality is that there are some things it wasn't designed for:

- ERPs excel at entity-level controls, but fraud often exploits the gaps between systems, across entities and over time.
- Fraudsters often circumvent processes, identifying loopholes in your systems. 3-way matching, for example, flags if items exactly match one another. But what if a digit or two were purposefully changed across all your documents? A duplicate invoice may never get flagged if that is the only control.
- Some ERPs also don't check for changes, dormancy or duplication in the master supplier file, making it easy for fraudsters to create opportunities for themselves.
- Smaller invoices, too, can fly under the radar. Automatic approvals under a spend threshold happen in many organisations. Couple this with automated payments and fraudsters can take advantage, accumulating large amounts over time.

Unfortunately, that makes ERPs alone sub-optimal as a control measure, especially if ECCTA legislation applies to you. The legislation states that organisations need to have 'reasonable fraud prevention procedures in place', with 'proportionate' fraud prevention procedures. So, if your organisation is complex with multiple entities, you need to cover off the gaps between those entities.

ECCTA legislation – a breakdown.

An organisation will be liable where a specified fraud offence an employee or agent commits the offence, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place'.

This also applies to subsidiaries or other 'associated persons' who provide services for, or on behalf of the organisation, for example, outsourced payroll personnel and contractors.

Specifically, the offence applies to:

- All large, incorporated bodies, subsidiaries and partnerships.
- Large not-for-profit organisations such as charities (if they are incorporated).
- Incorporated public bodies.
- Bodies, incorporates and partnerships formed outside UK, with a UK nexus.

ECCTA shifts the burden of proof.

It requires the organisation to prove they had reasonable prevention procedures in place when fraud has occurred.

Your organisation doesn't need to be aware of, or order, the fraudulent activity to be liable. It just needs to happen and benefit the organisation.

THE DEFENCE, THEREFORE, IS:

"We had reasonable procedures in place."

THE METHOD:

Demonstrable evidence

Strengthening your fraud controls.

It's essential to monitor these areas regularly to stay compliant.

The supplier master file.

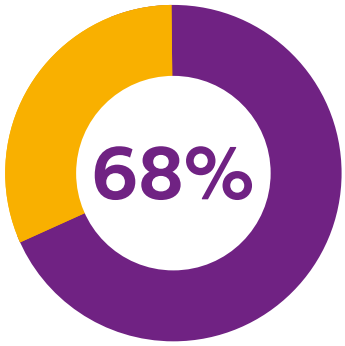
Using our own aggregated, anonymous data which spans 21 sectors, we've identified that on average:

68% of supplier records are dormant

Per 100 suppliers, duplicated records vary between 6% and 40%

The ACFE Report states organisations lose 5% of their annual revenue to occupational fraud, some of which can be traced back to supplier file tampering.

Those figures point to substantial exposure within the supplier master file. With their constant state of change and growth, ECCTA legislation places the onus on your organisation to keep up.



of supplier records are dormant

Transactions.

Seeking trends in invoice data can allow your team to investigate potential fraud before payment. AI can reveal changes to invoices and supplier actions, like a higher value invoice than the rest, a spike in the number of transactions, or an invoice sent at an unusual time. Transaction analysis also reveals duplicate invoices, which are worth 1% of spend on average.

Supplier statement reconciliation.

1 in 3 supplier statements contain discrepancies.

These range from differing invoice values to missing invoices, some of which indicate potential fraud. If the figures don't line up, if there are a few too many invoices, regular statement reconciliation finds them and allows your team to follow up.

What does good look like?

Compliance looks like thorough controls that you are confident fill in the gaps between systems and identify human-made errors.

BEST IN CLASS TEAMS HAVE:

- Specialist continuous risk monitoring tools with advanced forensic analysis.
- Master supplier file monitoring for dormant and duplicate suppliers, changes to the supplier file and employee-supplier file data matches.
- Transaction monitoring for a wide range of fraud indicators, including duplicate invoices, and unusual data patterns.
- Automated statement reconciliation looking for discrepancies across the whole supplier base.
- Human-level oversight, augmented with AI, ensuring the net is wide and very little slips through.
- Systematic procedures with audit evidence to demonstrate compliance.

CASE STUDY

The organisation

A leading global publisher with 5000+ employees and £160million+ revenue.

The problem

- Large volumes of invoices with increased the risk of duplicate and fraudulent payments.
- No way to identify them before the payment run.
- Difficulty managing and cleansing the master supplier file.

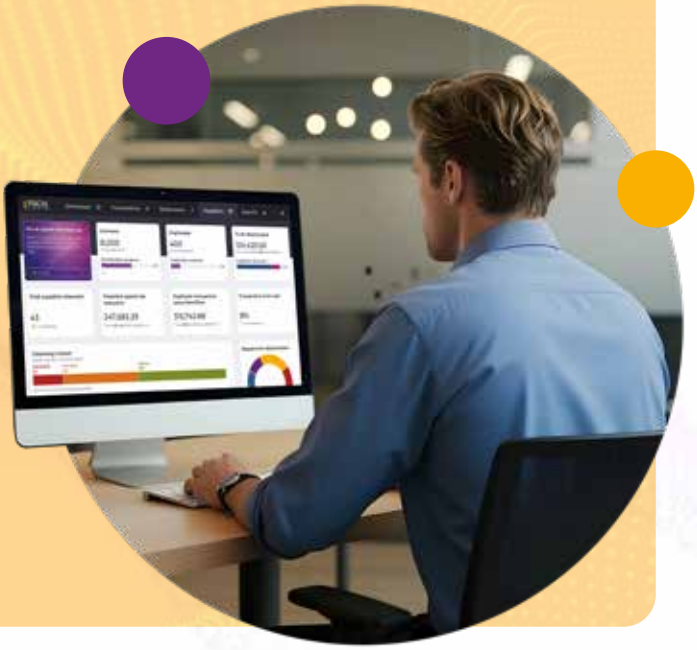
The solution

FISCAL Transaction and Supplier Risk Intelligence provided an automated analysis of every invoice and supplier risk. It found fraud indicators, exceptions, and duplicate or dormant suppliers, allowing the finance team to investigate before payments were made.

Having FISCALs software in place created strong fraud controls across transactions and supplier file monitoring. The organisation now has peace of mind not only that fraud is being caught and prevented, but that if it does occur, they have a strong defence against the failure to prevent fraud offence.

Benefits

- Prevented incidents of fraud with the platform.
- Prevented over £617,000 in overpayments.
- Effective cleansing and maintenance of the master supplier file.
- Time savings for the team thanks to automated, accurate controls, thereby reducing costs.



Our solution for best-in-class fraud controls.

FISCAL's P2P risk management software helps finance teams protect spend and strengthen risk controls, including in fraud prevention. It's backed by our expert consultancy and support teams.

The AI-powered software analyses every supplier and invoice, finding risks for your team to investigate and resolve. It augments your team's capabilities, strengthening controls before and after payment.

Specifically, it helps your team to:

- Monitor invoices for irregularities which could be fraudulent, including invoices entered or paid at unusual times, transaction spikes, round amounts and Benford's analysis.
- Check the master supplier file in real-time for duplicate or dormant suppliers.
- Examine the employee file and supplier file for data matches.
- Investigate or monitor changes to transactions and the master supplier file
- A full audit trail and reports to demonstrate compliance and assess controls.
- Complete statement reconciliation 12 times faster than manual methods.

Find out how FISCAL fits your fraud prevention framework. Talk to our team.

FISCAL TECHNOLOGIES

We protect your spend.

Every invoice. Every supplier. Every day.

t: +44 (0) 845 680 1905
e: smarter@fiscaltec.com
w: www.fiscaltec.com

FISCAL's P2P risk management platform helps finance teams protect spend and strengthen risk controls. It's backed by our expert consultancy and support teams.

The AI-based software analyses every supplier and invoice, finding risks for your team to investigate and resolve. It augments your team's capabilities, strengthening controls before and after payment.

FISCAL reduces fraud and compliance breaches, prevents duplicate payments, decreases supplier risk and automates statement reconciliation 12x faster. It integrates smoothly into your systems and processes, improving efficiency, and streamlining pay runs.

Since 2007, we have overseen 450+ implementations across sectors including local government, healthcare and retail. We now protect over £300 billion each year with proven, data-driven intelligence.

Document ID: Fraud Protection in the ECCTA Era 2026.