creditsafe

REPORT

THE BUSINESS FRAUD OUTLOOK 2026

UK business perspectives in the current fraud landscape.

EXECUTIVE SUMMARY

UK businesses are at a crossroads when it comes to fraud. Rapid advancements in technology have changed the threats that we face entirely, allowing fraudsters to become more sophisticated and penetrate deeper into business systems and data. Techniques that once required significant effort or specialist knowledge have now been automated and are far harder to spot.

At the same time, economic conditions are challenging. Over the past decade, the UK has been hit hard by the COVID-19 pandemic, spiralling energy prices, and the fallout of global crises, all leading to slow growth. Businesses are battling budget constraints, resulting in outdated software systems and internal skill gaps. Long-term transformation initiatives have fallen by the wayside in favour of immediate operational priorities, or “quick wins”.

The result is a vulnerability gap that continues to get wider. While the general consensus is that fraud is a significant threat, responses to it are inconsistent.

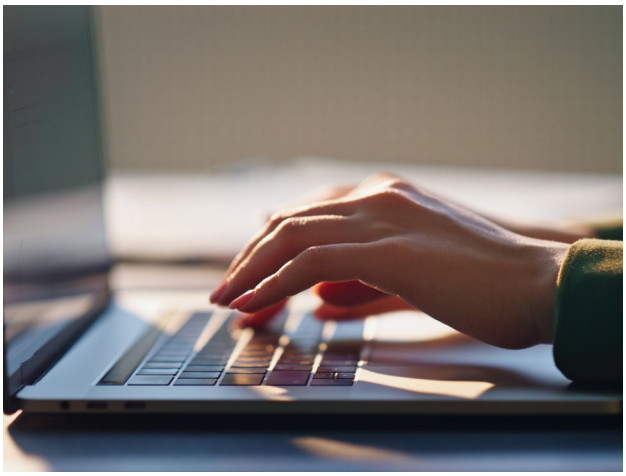
Investment lags behind threat levels and responsibility for fraud risk is often unclear or spread across multiple teams. Many businesses are leaving themselves exposed to risks that they simply cannot afford.

There are clear patterns in what UK businesses are experiencing and what they are doing in response. Understanding the sentiment towards fraud is what is going to help us put ourselves in the best position to tackle it.

The findings of this report make obvious that this is not a problem of indifference, but of constraint and complexity. Businesses are balancing fraud prevention against multiple competing priorities, often without the insight needed to quantify return on investment (ROI).

For UK businesses, the path forward is not just recognising the threat, but taking action before it is too late.

Chris Robertson, CEO at Creditsafe UK



Survey Methodology

Creditsafe surveyed 108 UK businesses between February and March 2026, spanning businesses with 1-250+ employees. Respondents were asked about fraud experiences, risk perceptions, approaches to prevention and operational challenges.

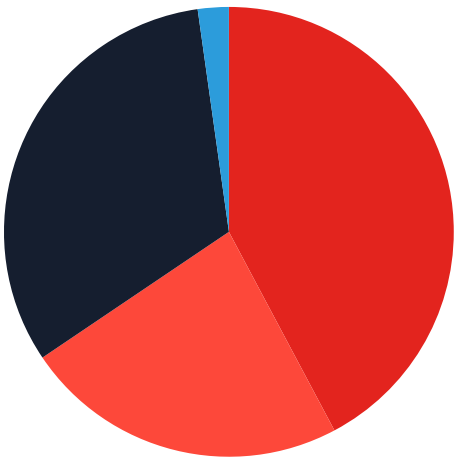
THE CURRENT FRAUD LANDSCAPE

Fraud is escalating, and businesses know it

In 2024, fraud accounted for 41% of all crime in England and Wales[1], making it the biggest risk to organisations today. It's also one of the costliest crimes – the social and economic cost of fraud to UK businesses, including anticipation, consequence and response, was estimated to be £5.2bn in the same year.[2]

Have you seen an increase in fraud attempts over the past 3 years?

38%	31%	29%	2%
Significant Increase	Minor Increase	No Change	Decrease



There is little indication that fraud attempts will decrease anytime soon. In fact, UK businesses are reporting the opposite. Almost 70% of UK businesses have experienced an increase in fraud attempts over the past three years, with over a third reporting a significant rise.

This sharp increase suggests that fraud is accelerating at a rapid pace, likely driven by automation and AI tools that allow fraudsters to work at scale. AI has also lowered the barrier to entry for criminals, making it easier to impersonate customers or other trusted individuals, forge documents, access more businesses and adapt when attacks fail.

However, it's not only criminals that are using AI; businesses are speedily adopting generative AI tools, driving the market to grow from 0 in 2021 to over $43bn by 2024.[3] A rapid roll-out of new tools can often come with technology and security gaps, which fraudsters can exploit.

As for the 29% who experienced no change, this should not be interpreted as unaffected by fraud. In some cases, this can reflect a lack of visibility rather than a lack of activity. Organisations operating without real-time monitoring or cohesive data are often unaware of how frequently they are being targeted, or how close some attempts come to succeeding.

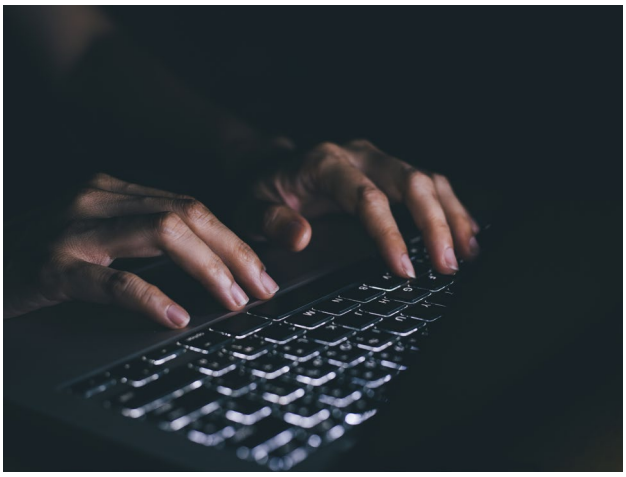
The future of fraud is digital

It's estimated that almost 70% of fraud reported in the UK is cyber-enabled.[4] Phishing attempts account for over half of fraud experienced, but compromised emails and payment fraud are also at significant levels.

What type of fraud has your business experienced? (Select all that apply)

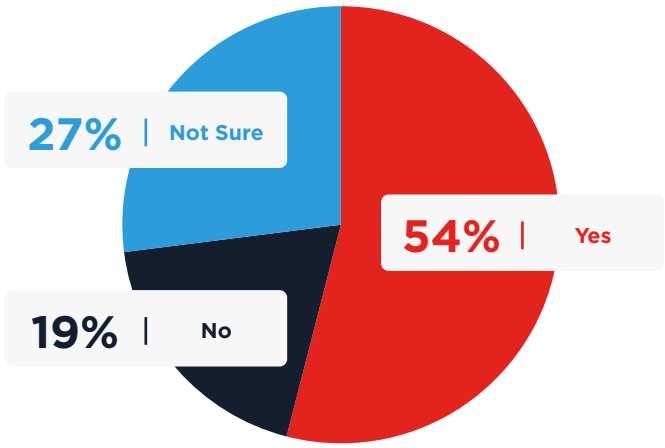
37% Payment Fraud	28% Invoice Fraud	59% Phishing Attempts	40% Compromised Emails
12% Identity Theft	12% None	12% Other	

These types of attacks are cheap and easy to conduct, making them attractive to fraudsters. They are also highly scalable and thrive in busy environments where manual workflows make it easier to overlook unusual activity. Additionally, phishing is so successful as it exploits human behaviour and trust. If the process is automated rather than manual, this adds a layer of protection as human input isn't required.



Not all businesses are certain about the future

Do you expect the risk of fraud on your business to increase in the next 1-3 years?



As fraud attempts increase, it's to be expected that over half of businesses believe fraud risk will continue on the same trajectory over the next one to three years. However, a more striking figure is that over a quarter of respondents said they were unsure whether fraud risk would rise. This number suggests that many businesses lack a clear understanding of their exposure.

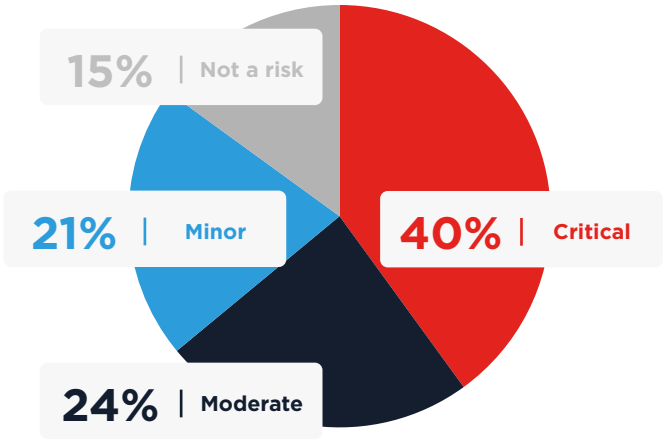
What causes this lack of clarity? It may stem from:

- Fragmented or siloed data
- Weak risk assessment processes
- Manual processes that cannot keep up with modern attack strategy
- Lack of analytic capability

With all these challenges facing UK businesses, it can be impossible for some to spot concerning trends or determine where their weak spots are. As a result, a significant proportion are reacting to fraud after it happens, rather than anticipating it.

Fraud is a concern, but not always a priority

Business Threat



On the surface, fraud awareness is high. 85% of businesses acknowledge fraud as a threat to some level, with 40% classifying it as a critical risk. However, when drilled down by company size, the perception changes vastly, revealing structural differences in how they manage risk.

Medium and large businesses (50-250+ employees) display heightened concern, with up to 39% viewing fraud as a critical threat. Larger organisations often have more complex operations and larger customer and supplier networks, which results in more entry points for fraudsters, so a higher level of concern is to be expected.

Small businesses (10-49 employees), on the other hand, are less concerned, with only 11% viewing fraud as a critical threat. Often this is because they have experienced fewer incidents, being less attractive to fraudsters looking to win big. As smaller businesses encounter fewer incidents, this can translate to lower perceived risk, meaning that fraud prevention is not a priority.

However, despite the lessened concern, smaller companies are often more vulnerable to risk. This is due to:

- Fewer internal controls
- A lack of dedicated team for fraud
- Outdated systems
- Less training around fraud awareness

Those least prepared are often least concerned, creating a paradox.

Despite the variations by company size, the overall results are clear: UK businesses definitely perceive fraud as a business threat.

Confidence does not always mean capability

How confident are you in your ability to prevent fraud as a business?

64%	25%	11%
Very confident	Somewhat confident	Not confident

89% of businesses report feeling confident in their ability to prevent fraud. On paper, this suggests that they feel they have the systems in place to combat fraud. However, the reality is more complex.

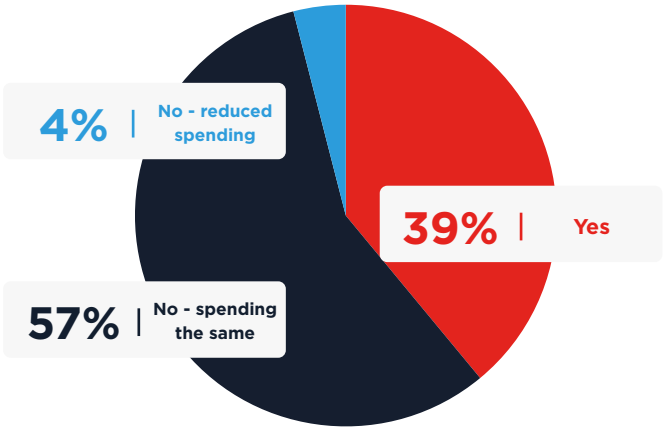
Confidence is not evenly distributed between business sizes. Small businesses are the least confident, which could be a reflection of their limited resources. Large firms show a wider divide in opinion, with many very confident but a notable minority not confident at all.

Nonetheless, spending trends do not align with this sentiment.

THE TRUE COST OF FRAUD

Spending and levels of concern are mismatched

Have you increased spending on fraud prevention in the past 3 years?



Despite the level of concern reported, the majority of businesses are stagnant when it comes to fraud prevention spending. Over half of businesses have not increased fraud prevention spending at all, with an additional 4% reducing their spend. In real terms, accounting for inflation, flat spend results in comparatively less spend year-on-year.

This misalignment could be for a few reasons:

- High inflation and rising operational costs mean businesses are struggling to ringfence funds for fraud prevention
- Investments that are made are often reactive rather than proactive
- Fraud is seen as a cost rather than an investment

When broken down by business size, mid-sized firms (50-249 employees) are the most likely to invest (56%). Businesses of this size have a higher exposure to fraud and stricter compliance requirements, alongside higher budgets.

Smaller businesses (<50 employees) were far less likely to increase spend, with up to 64% of companies spending the same across the past three years. Tighter budgets and a smaller workforce to take charge of fraud risk are the most likely reasons. Unfortunately, these same constraints make recovery from fraud far more difficult if it does happen.

Standing still in this environment means falling behind. It's clear that many UK businesses are relying on the systems they already have in place to combat future threats, which is not a sustainable approach as criminals become more sophisticated in their methods.

The cost goes beyond financial

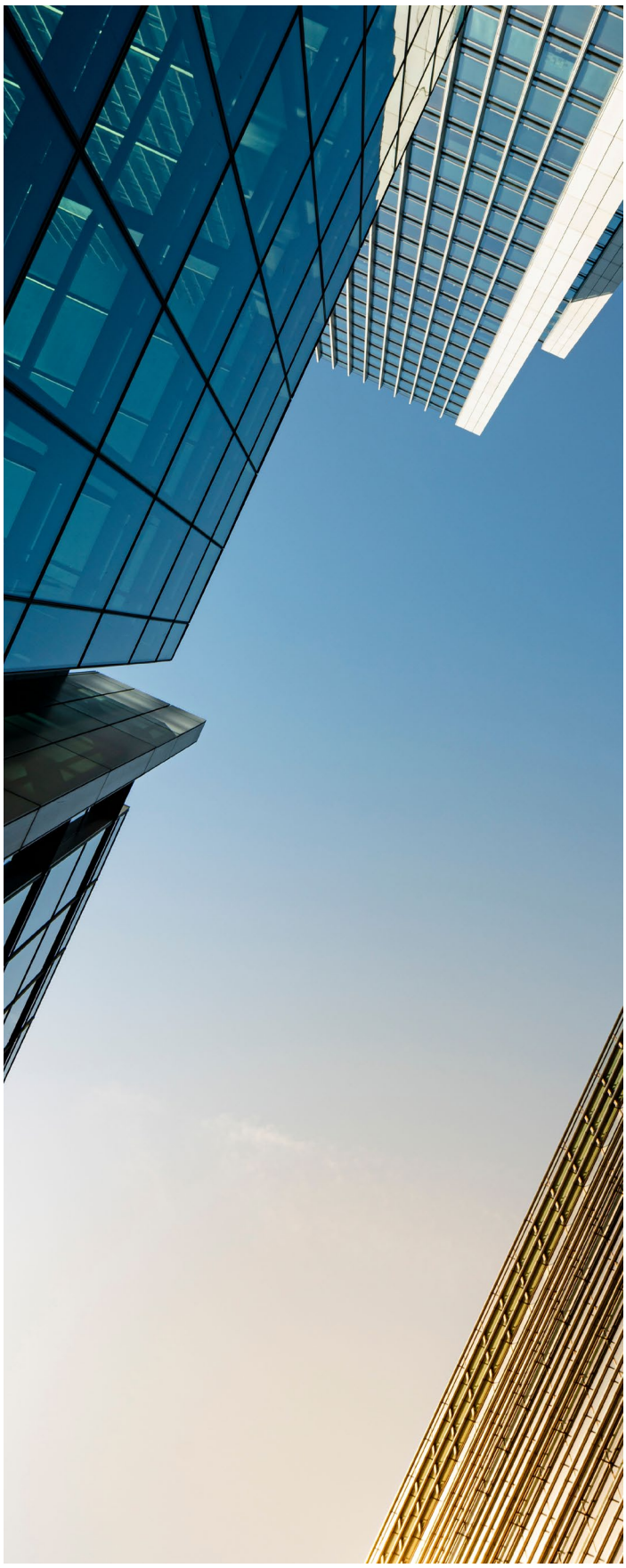
What are your biggest fraud concerns?

44%	Cash Flow Disruption
44%	Reputational Damage
22%	Credit Rating Impact
24%	Increased Insurance Premiums
41%	Operational Downtime
14%	Staff Productivity
91%	Financial Loss

Unsurprisingly, financial loss remains the number-one concern for the majority (91%) of businesses. The average amount lost to fraud by SMEs annually is almost £4,000[5], which is not an insignificant figure. However, the data shows that businesses see fraud as a multi-dimensional threat.

Cash flow disruption and operational downtime are main concerns for over 40% of respondents. This serves as a reminder that even relatively small fraud incidents can be a major disruption, whether that's payroll delays, supplier disputes, or having to stop services all together.

Reputational damage is of equal concern. Trust is fragile, and once it's lost, it's difficult to rebuild. In B2B environments especially, fraud incidents can jeopardise long-term, high-value contracts. Ultimately, fraud touches every corner of a business' health.



BARRIERS TO FRAUD PREVENTION

Action lags behind awareness

What is your biggest barrier to improving your fraud prevention activities?
(Select all that apply)

38% Cost	**36%** Lack of expertise	**15%** Limited access to data
30% Technology gaps	**37%** Other business priorities	**20%** Hard to measure ROI

A clear contradiction has emerged: fraud attempts are rising and concern is widespread, but businesses aren't taking action. To understand why, we need to look at the barriers that businesses say are holding them back.

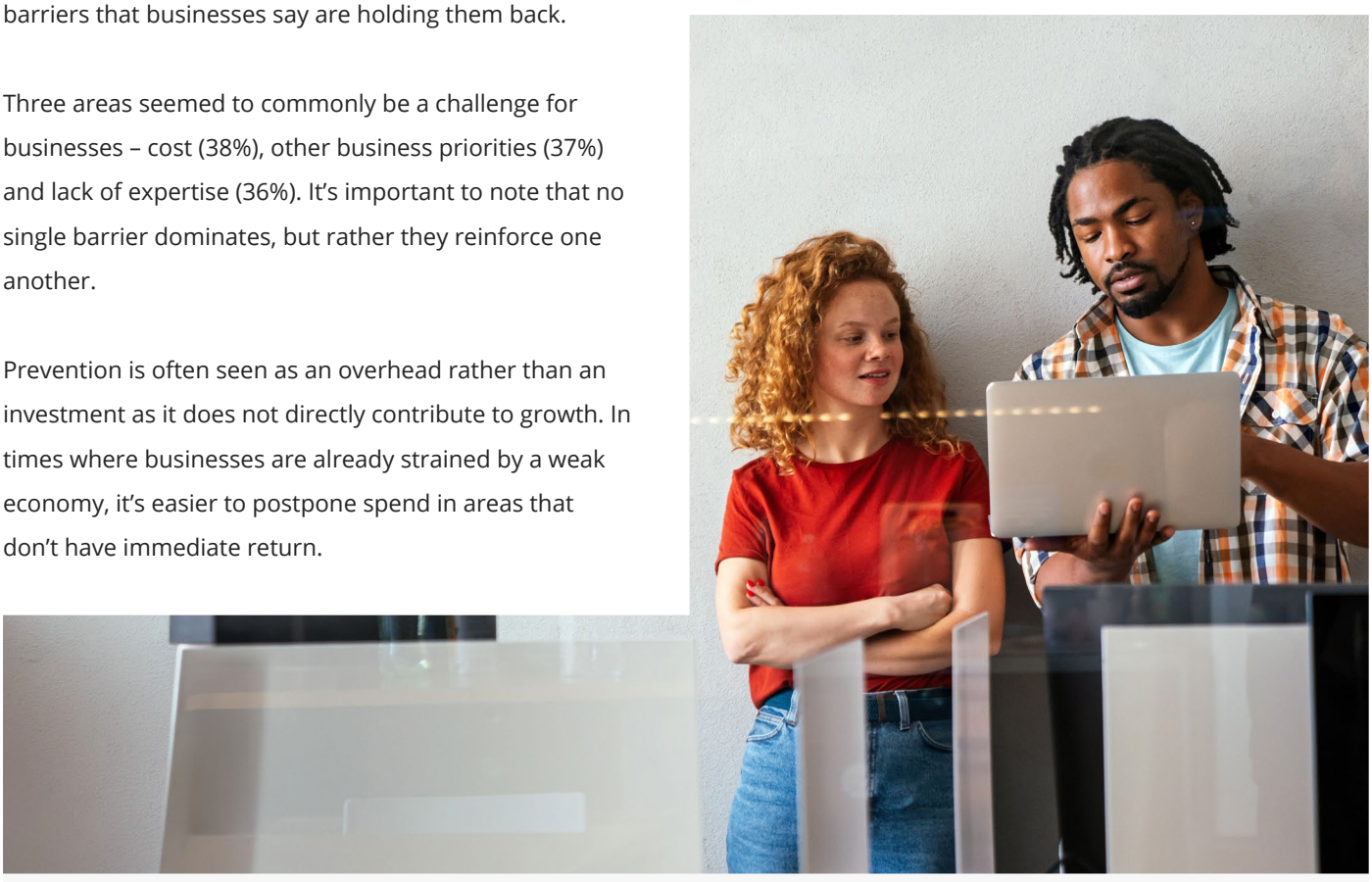
Three areas seemed to commonly be a challenge for businesses – cost (38%), other business priorities (37%) and lack of expertise (36%). It's important to note that no single barrier dominates, but rather they reinforce one another.

Prevention is often seen as an overhead rather than an investment as it does not directly contribute to growth. In times where businesses are already strained by a weak economy, it's easier to postpone spend in areas that don't have immediate return.

Directly linking to other business priorities, fraud prevention is competing with wider digital transformation, customer experience developments, operational firefighting, and regulatory changes. If budgets are limited, then businesses must decide where is most important to spend. It's less likely to go towards fraud prevention, as businesses will take the risk and react after a fraud attempt happens rather than prevent it in the first place.

A lack of expertise becomes central in this problem. Without internal fraud skills, businesses struggle to create a strategy to understand what tools they need. Consequently, this leads to a delay in investment decisions or a lack of consensus within the business.

Together, these barriers explain why many organisations worry about fraud yet struggle to act.



EARLY WARNING SIGNALS

Data is central to fraud prevention

Despite the differences in opinions between SMEs, there is one point they all agree on: data is key.

What data helps you the most in preventing fraud?

62%	Director/Shareholder/UBO Information
58%	ID & Address Verification
56%	Payment History/Finance Agreement Data
25%	CIFAS/Third-party Fraud Data
4%	Other

When asked which data sources help the most, respondents consistently wanted information on owners and key people with a business, ID and address verification and financial history.

Businesses are keen to discover early warning signals so that they can prevent fraud before it impacts them. Ownership changes, unusual appointments or addresses, payment irregularities or a lack of payment altogether all provide context that would be hard to get without the data.

However, there is a clear gap between recognising the value of data and fully operationalising it. Many businesses still rely on outdated software and manual checks, which means critical signs are often missed or identified too late.

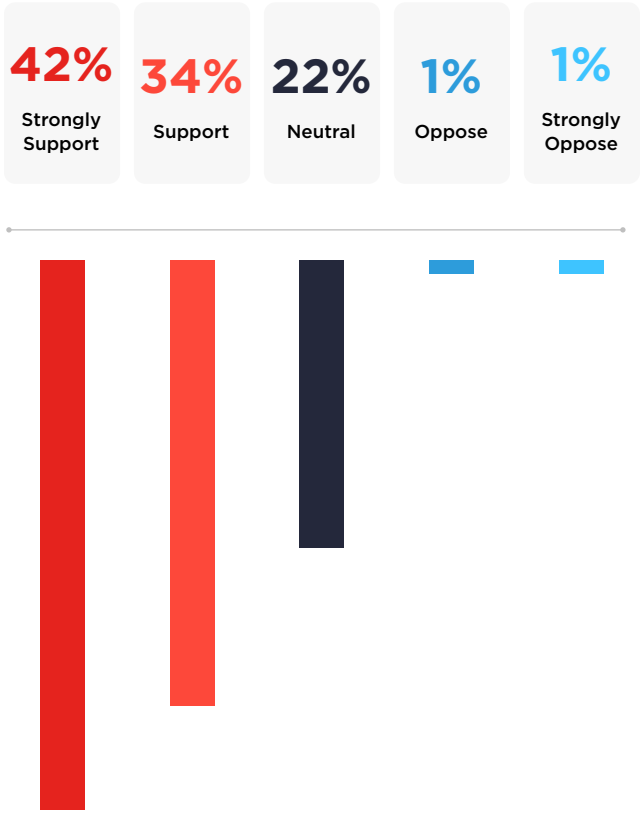
How can businesses operationalise fraud prevention? One way is to incorporate credit reporting tools into a wider digital transformation strategy.

Support for data collaboration is strong

Between 2023 and 2024, overall fraud reporting volumes increased by up to 19%.[6] Data on fraud continues to grow and it's clear that UK businesses are keen to share it.

With over three-quarters of organisations in support of reporting fraud risk, it's being seen as a collective problem. Criminals reuse identities and tactics, so when businesses operate in isolation, fraudsters aren't easily spotted.

Would you support reporting possible risk/ fraud anonymously with other businesses?



Of the 2% of businesses that opposed data sharing, their main concerns were complexity, regulatory compliance and governance. For some organisations, the perceived legal and operational challenges outweigh the benefits.

Businesses want to be alerted of unusual activity

Real-time alerts dominated when asked what would help the most in preventing fraud. Businesses want to know when there is unusual activity on their accounts in real time, without having to trawl through all their data. This way, they can act quickly.

What would help your business the most in preventing fraud?

33% Better access to data	**69%** Real-time alerts	**39%** Employee training
26% Regulatory guidance	**38%** Better technology	**44%** Data sharing

Training and technology also rank highly because they address the root causes identified earlier: lack of expertise and technology gaps. Making fraud prevention as easy and as streamlined as possible is what businesses want the most.

With the right tools, businesses can build fraud prevention directly into their existing workflows.

WHAT ARE THE TRENDS TO LOOK OUR FOR?

One of the reasons fraud prevention stalls is because it can be challenging to determine what is a struggling business and what is a fraudulent one. However, there are a few areas that while don't directly suggest fraud, can be a sign that further monitoring is required.

The following exceptions were found during a 12-month period between* ***March 2025 – March 2026.***

**Exceptions are unique warning indicators used by Creditsafe to highlight unusual company activities that could negatively affect business operations. These alerts are updated daily using information from official local and global sources.*

Unusually high first-year turnover

High turnover early on can be legitimate, but typically, a new business needs time to build its operations and establish itself. If profits are higher than the industry average, it should raise questions around if the stated business activity really took place and whether the figures are correct.

There are non-fraudulent reasons for this. For example, administrative errors, such as a misunderstanding of accounting rules, incorrect cut-off dates, invoicing errors, or revenue recognised before the goods or service has been delivered can inflate turnover.

However, they may be conducting circular transactions, where funds or goods are moved through a series of entities (often shell companies or partners), either to inflate financial results or to launder money.

***752** companies reported an unusually high first-year turnover.*

A director has been disqualified

There are a few reasons for a director to be disqualified. These include:

- Financial mismanagement: Failing to keep proper accounting records or submitting false statements
- Insolvent trading: Continuing to trade even when a company cannot repay its debts
- Non-payment of tax
- Misuse of company funds: Using company money or assets for personal benefit

Not all directors who are disqualified are committing fraud, so this alone isn't a sign of fraud. However, working with a company where a director has been disqualified can put the business at risk, especially when paired with other warning signs.

***468** companies had at least one Director appointed who is disqualified, without exemption.*

Companies House is their default address

Sometimes, a business' registered address will change to Companies House. There are a few reasons this happens:

- Mail sent to their registered address is undeliverable
- The address doesn't exist
- Companies House receives a complaint that the address is being used without permission

Companies cannot operate without a real and valid office. Sometimes, an administrative error can result in Companies House holding an invalid address for a company.

It can also be the case that a company is simply inactive.

However, fraudulent companies will often use addresses without permission or give false contact information. If a valid address isn't provided quickly, Companies House can initiate strike-off proceedings and dissolve the company.

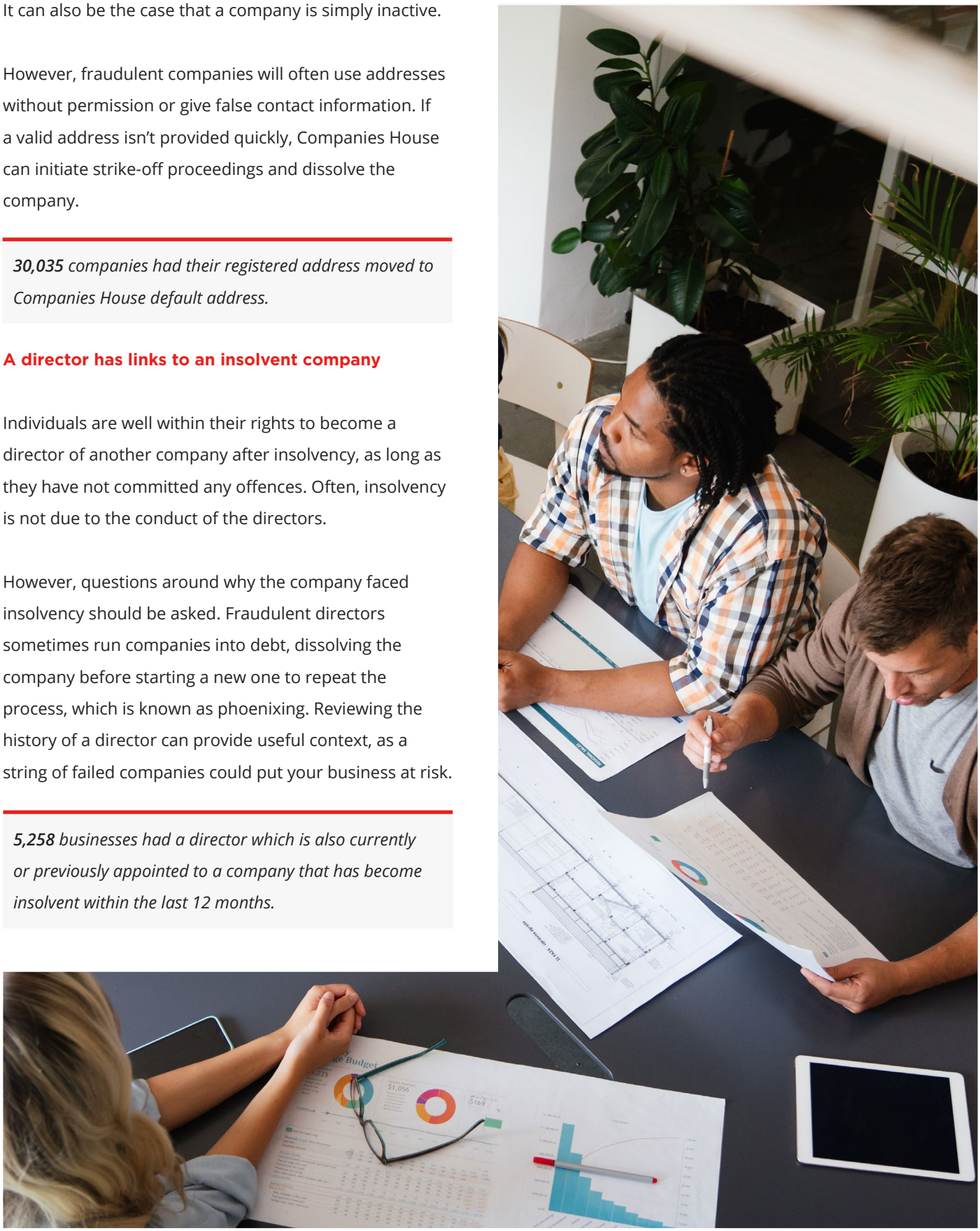
***30,035** companies had their registered address moved to Companies House default address.*

A director has links to an insolvent company

Individuals are well within their rights to become a director of another company after insolvency, as long as they have not committed any offences. Often, insolvency is not due to the conduct of the directors.

However, questions around why the company faced insolvency should be asked. Fraudulent directors sometimes run companies into debt, dissolving the company before starting a new one to repeat the process, which is known as phoenixing. Reviewing the history of a director can provide useful context, as a string of failed companies could put your business at risk.

***5,258** businesses had a director which is also currently or previously appointed to a company that has become insolvent within the last 12 months.*



KEY INSIGHTS

Micro businesses (1-9 employees) have high exposure and low resilience

Businesses of this size experienced some of the largest increases in fraud attempts, and as a result are less confident in their ability to prevent it.

Despite this, they are less likely to spend on fraud prevention, usually due to budget constraints. When fraud does occur, these businesses have the least capacity to absorb losses. Even relatively small incidents can have a devastating impact.

Small businesses (10-49 employees) are more confident, but still constrained

These businesses showed slightly higher confidence in their fraud prevention capabilities but were among the least likely to increase spend.

Resources are still limited and fraud prevention is competing with other priorities. As these businesses scale, the gap between exposure and protection can widen quickly unless they are proactive in risk management.

Mid-sized businesses (50-249 employees) are the most proactive

This group hit the sweet spot of being concerned about future risk and reporting the highest increases in fraud prevention spending. They are relatively confident in their strategy as a result, although not complacent.

At this size, complexity increases. More customers, more suppliers, higher transaction volumes and tighter regulations can all make fraud more difficult to manage. Investment in tools and data that can support risk management is necessary to keep up with growth.

Large businesses (250+ employees) have mixed views

With the lowest increase in fraud attempts overall, large businesses are more likely to have existing systems in place that are working well to prevent fraud.

However, that doesn't mean they are more confident. In fact, confidence levels varied largely from company to company. Fraud prevention isn't uniform across businesses and all of them have their own level of resilience.

While these organisations are generally better positioned to manage fraud, they are also at much higher risk. Manually monitoring thousands of customers is an impossible task, so businesses of this size need to consider tools than can support risk management.

RECOMMENDATIONS

Step 1 – Increase your fraud prevention budget in alignment with risk exposure

Not every business faces the same level of risk. Targeted investment based on exposure means that budget is allocated in areas where it will really make an impact.

Businesses need to identify where their weak spots are, whether that is payments, onboarding or suppliers. In a time of squeezed margins, investing budget wisely matters more than ever.

Step 2 – Formalise your fraud process

Many companies operate without clear strategy on fraud. Responsibilities get shared informally across multiple teams, which result in duplicated efforts and inconsistent responses.

A defined strategy which covers everything from prevention to response creates clarity across your teams, so they understand the part they play and what they're expected to do.

This replaces firefighting with clear action, which leads to better decisions made.

Step 3 – Invest in real-time data monitoring and identity verification

If businesses can only invest in one capability, they should make it visibility. Real-time monitoring of company changes, ownership structures, financial activity and other unusual behaviour provides early warning signals before loss happens.

Instead of relying on periodic manual checks, real-time alerts allow businesses to respond immediately to unusual or high-risk activity.

Credit data with real-time monitoring built in offers one of the most efficient ways to achieve this, delivering continuous oversight without needing additional resources.

Another area to focus on is identity verification. Manual verification is not only time intensive but leaves room for error. Think of the process as a puzzle; if one piece is missed, the picture is incomplete. Missing vital information that could point to past fraudulent activity leaves companies exposed to fraudsters. Advancements in this area mean that tools to support this process are now more powerful at a lower cost.

Build your fraud prevention strategy with Creditsafe

Creditsafe helps businesses move from reactive to proactive fraud prevention by providing the data and visibility needed to identify risk before it's too late.

By combining rich credit data with real-time monitoring and all of your essential KYC checks, you can automate the key processes that help you spot risk early.

About Creditsafe

As the world's most used provider of online business credit reports, we're transforming the way business information is used worldwide. With credit data on over 430 million businesses globally, Creditsafe offers accurate, up-to-date information in an easy-to-use format.

Contact Us

To learn how Creditsafe can support your fraud prevention strategy, get in touch.

For Sales: help@creditsafeuk.com
For Press Enquiries: press@creditsafeuk.com