Allianz

Allianz Trade

Protection in the age of deception

A practical guide to staying ahead of modern business fraud

ALLIANZ-TRADE.CO.UK/FRAUD

A new era of business risk

New legal and regulatory guidance looms over UK businesses. The Economic Crime and Corporate Transparency Act's (ECCTA) new failure to prevent fraud offense piles pressure on firms to deal with fraud by associated persons intending to benefit their organisation.[1] But it's clear - fraud is much more likely to target your business, not benefit it.

Fraud doesn't discriminate. No matter the industry, sector, or business size, fraud attempts are omnipresent. Fraud is the most common type of crime that takes place in the UK, amounting to 41% of all crime in England and Wales as of September 2024.[2]

With advances in modern technology from the likes of artificial intelligence, the ways in which fraud is perpetrated are becoming smarter, faster, and more personalised. Year on year, fraud cases continue to grow, with Cifas reporting over 420,000 cases filed to the National Fraud Database in 2024. This is a 13% increase, the highest number recorded so far.[3]

This isn't just a UK problem - fraud is a global concern. The Association of Certified Fraud Examiners found that occupational fraud itself caused losses of over $3.1 billion across the 138 countries and territories covered in its 2024 report.[4]

This calls for businesses to improve their fraud resilience by being more aware of the common types of fraud taking place, trends and developments shaping future attempts, and the options available to businesses hoping to fight back.

> Quite simply, fraud is and always has been a prevalent issue affecting all types of businesses. The challenge now is that fraudsters are using advanced technology to find smarter ways of perpetrating crimes.
>
> Vikshay Vijai, Fraud & Crime Lead Underwriter – UK & Ireland

CONTENTS

[1] *Economic Crime and Corporate Transparency Act 2023 – Legislation.gov.uk: https://www.legislation.gov.uk/ukpga/2023/56/contents*
[2] *Fraud – National Crime Agency: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime*
[3] *Fraudscape 2025: Reported fraud hits record levels – Cifas: https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels*
[4] *Occupational Fraud 2024: A Report to the Nations – ACFE: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf*

The rising cost of deception

~60%

Of fraud cases come from within the business, rather than external criminals[7]

81%

Of large UK businesses (more than 1,500 employees) have experienced fraud, compared to 27% of small businesses (200-499 employees)[5]

55%

Of UK and Irish businesses have experienced fraud attempts in the past 24 months[6]

> Preventative fraud risk mitigation is no longer optional, it has become an imperative.
>
> Vikshay Vijai, Fraud & Crime Lead Underwriter – UK & Ireland

Every two minutes

A new case of fraud is reported to the National Fraud Database, which prevents £2.1bn in losses[8]

[5] *Fraud Survey 2024 – BDO: https://www.bdo.co.uk/getmedia/25626540-aa71-459e-8fa2-9e41fd03a313/Fraud-Survey-2024-Nov-2024.pdf*
[6] *Global Economic Crime Survey 2024 – PwC Ireland: https://www.pwc.ie/services/deals-advisory/insights/global-economic-crime-survey-2024.html*
[7] *Allianz Trade Loss Statistics - Artificially intelligent fraudsters: How white-collar criminals are leveraging modern technology*
[8] *Fraudscape 2025: Reported fraud hits record levels – Cifas: https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels*

Fraud's impact by sector

Construction

With its high pressure, high-stakes environment, the construction sector creates the perfect setting for fraud attempts to take place. In fact, PwC reports that the engineering and construction sectors had the highest rates of bribery and corruption of any industry.[9]

[9] *Fighting corruption and bribery in the construction industry – PwC: https://www.pwc.com/gx/en/economic-crime-survey/assets/economic-crime-survey-2014-construction.pdf*

[10] *Legal advice on fraud in the construction industry – Taylor Rose: https://www.taylor-rose.co.uk/posts/construction-industry-fraud*

Technology

Fast growth and high-value transactions make the tech sector a top target for fraud. With complex systems and sensitive data in play, attacks are frequent and costly.

66%

Two-thirds of companies in this sector have experienced fraud, making it the most affected industry.[11]

38%

Of companies with revenue less than $100m have suffered an individual fraud incident that has cost more than $1m.[11]

>$50M

One in five organisations with revenues over $10 billion faced individual fraud incidents exceeding $50 million[11]

Food

As a highly regulated sector, the food industry faces a multitude of fraud risks. This applies to most aspects of food production, from the marketing claims made by suppliers, to outright cargo theft.

£2bn annually

The amount that food fraud costs the UK economy[12]

£268m

The burden of food fraud on businesses per year as of 2022[13]

1,041%

The increase in food fraud incidents between 2020 and 2023[14]

[11] *Fraudsters target tech - two-thirds experienced fraud in past 2 years, PwC report states: https://www.pwc.com/gx/en/news-room/press-releases/2022/global-economic-crime-and-fraud-survey-2022.html*

[12] *FSA and FSS publish strategic assessment to support businesses and protect consumers against food fraud – Food Standards Agency: https://www.food.gov.uk/news-alerts/news/fsa-and-fss-publish-strategic-assessment-to-support-businesses-and-protect-consumers-against-food-fraud*

[13] *The Cost of Food Crime Phase 2 – Results – Food Standards Agency: https://www.food.gov.uk/research/the-cost-of-food-crime-phase-2-results*

[14] *Food Fraud Explosion: A Tenfold Increase from 2020 to 2024 — Predictions and Prevention Strategies – SGS Digicomply: https://www.digicomply.com/blog/food-fraud-explosion*

Retail

The retail industry experiences fraud from multiple angles. Not only do incidents carry financial damages, but they can also affect a brand's reputation in a very public manner. Repeated instances lead to substantial losses, with aspects like returns policies being frequently abused.

16.7m
Incidents of customer theft reported by retailers in 2022/2023[15]

38%
Of UK consumers claim to have engaged in return policy abuse[16]

£4.2bn
The total cost of retail crime, including crime prevention - £2.2bn of which resulting from customer theft[17]

Healthcare

With high transaction volumes, complex service models and pressure on public funding, the healthcare sector is especially vulnerable to fraud. From billing scams to false patient data, the financial and operational toll is mounting.

$100,000
Is the median fraud loss per case, with average losses reaching $721,000 according to ACFE[18]

5.6%
Is the average healthcare expenditure on fraud each year[19]

1.27bn
Lost to NHS fraud annually,[20] with over 6,300 cases reported in 2023/24 alone[21]

[15] *Retail crime: Impact on workers, the community and local economies - House of Lords Library: https://lordslibrary.parliament.uk/retail-crime-impact-on-workers-the-community-and-local-economies*
[16] *2024 Consumer Fraud Report – Loop: https://info.loopreturns.com/hubfs/2024%20UK%20Consumer%20Fraud%20Report.pdf*
[17] *BRC Retail Crime Survey 2025 – BRC: https://brc.org.uk/news-and-events/news/operations/2025/ungated/brc-retail-crime-survey-2025*
[18] *Occupational fraud 2024: A report to the nations https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf*
[19] *NHS at greater risk of fraud with new private providers in system, finds CHPI: https://www.chpi.org.uk/blog/nhs-greater-risk-fraud-new-private-providers-system-finds-chpi*
[20] *Fraud in the NHS: https://www.cnwl.nhs.uk/patients-and-carers/fraud-nhs*
[21] *NHS Counter Fraud Authority – Reporting trends: https://cfa.nhs.uk/about-nhscfa/corporate-publications/SIA-2024/SIA-2024-reporting-trends*

Five forms of fraud you need to know about

There are five types of fraud that all businesses should be familiar with.

1.

Financial statement fraud

Financial statement fraud covers the misuse of company funds, including financial records. By inflating invoice values, for example, an employee may pocket the balance for their own personal gain.

According to a 2024 survey, financial statement fraud was one of the most common incident types faced by UK corporate entities, with 23% of them reporting an instance of it.[22]

2.

Social engineering

Social engineering is an act of duplicity, where attackers infiltrate the internal systems of a business by directly manipulating people. Technology can be used to assist social engineering, through voice masking or deepfaking images and videos. However, social engineering ultimately comes down to exploiting vulnerabilities in human behaviour, making it a highly deceptive (and hard to prevent) attack.

These tactics can take many forms. Phishing emails may trick employees into revealing sensitive information. Business email compromise (BEC) attacks go further, using impersonation to manipulate senior staff and authorise fraudulent actions.

Social engineering is most prevalent in cybercrime - it makes up 98% of all cyber attacks.[23]

3.

Identity fraud

While closely associated with social engineering, identity fraud is commonly dealt with as its own attack. Using stolen credentials obtained through social engineering or otherwise, attackers assume the identity of an influential figure within an organisation, abusing their power for their own gain.

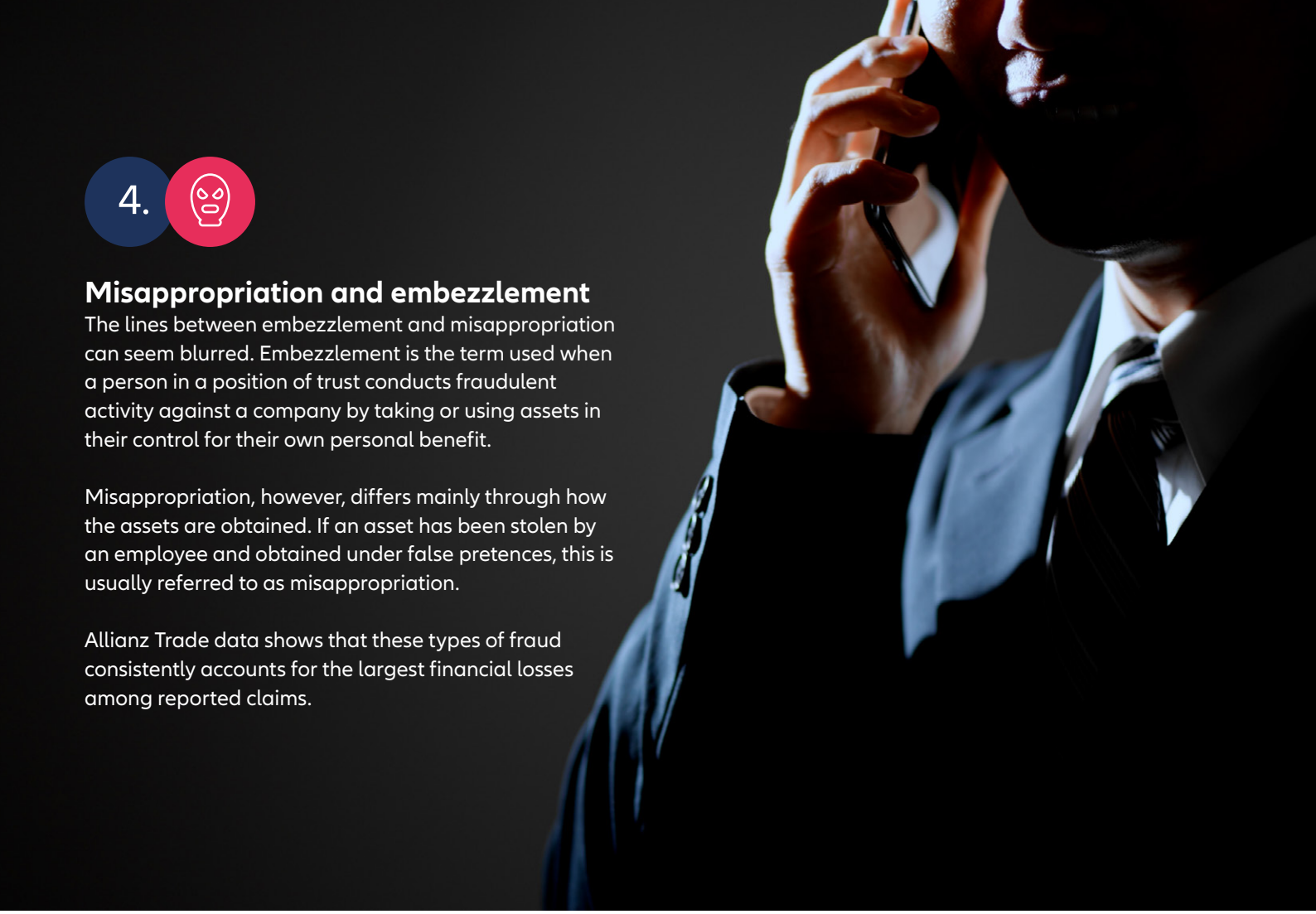
As recorded in 2024, identity fraud costs the UK an estimated £1.8 billion each year and is one of the most common types of fraud reported to Cifas.[24] Globally, identity fraud costs organisations $7 million annually.[25]

[22] *UK businesses report significant increase in fraud awareness after introduction of the Economic Crime and Corporate Transparency Act – BDO: https://www.bdo.co.uk/en-gb/insights/advisory/forensic-services/uk-businesses-report-significant-increase-in-fraud-awareness-after-introduction-of-the-eccta*

[23] *What Is Social Engineering? – Proofpoint: https://www.proofpoint.com/uk/threat-reference/social-engineering*

[24] *Cifas and RUSI highlight growing threat to UK security from identity fraud – Cifas: https://www.cifas.org.uk/newsroom/cifas-rusi-growing-id-fraud-threat*

[25] *Identity fraud costs organizations an average of $7 million annually, says new research from Docusign and Entrust – Entrust: https://www.entrust.com/company/newsroom/identity-fraud-costs-organizations-an-average-of-7-million-annually-says-new-research-from-docusign-and-entrust*



4.

Misappropriation and embezzlement

The lines between embezzlement and misappropriation can seem blurred. Embezzlement is the term used when a person in a position of trust conducts fraudulent activity against a company by taking or using assets in their control for their own personal benefit.

Misappropriation, however, differs mainly through how the assets are obtained. If an asset has been stolen by an employee and obtained under false pretences, this is usually referred to as misappropriation.

Allianz Trade data shows that these types of fraud consistently accounts for the largest financial losses among reported claims.

5.

Supplier and buyer fraud

Supplier fraud is when attackers impersonate vendors or suppliers, submitting false invoices or changing payment details to divert funds for goods or services that are never delivered.

Buyer fraud, on the other hand, targets your business as the seller. Fraudsters may place orders using fake identities, request goods to be delivered to unverified addresses, or abuse 'buy now, pay later' schemes with no intention of settling the invoice.

Supplier fraud is one of the more common business fraud types, with 93% of UK companies falling victim to it in 2024.[26]

Fraud is sector-agnostic: manufacturing, logistics, finance, and professional services are just a few of the targets.

[26] *Ninety-three percent of UK Companies Experienced Vendor Fraud in 2024, According to New Trustpair Research – Business Wire: https://www.businesswire.com/news/home/20250211180324/en/Ninety-three-percent-of-UK-Companies-Experienced-Vendor-Fraud-in-2024-According-to-New-Trustpair-Research*

Business fraud is evolving

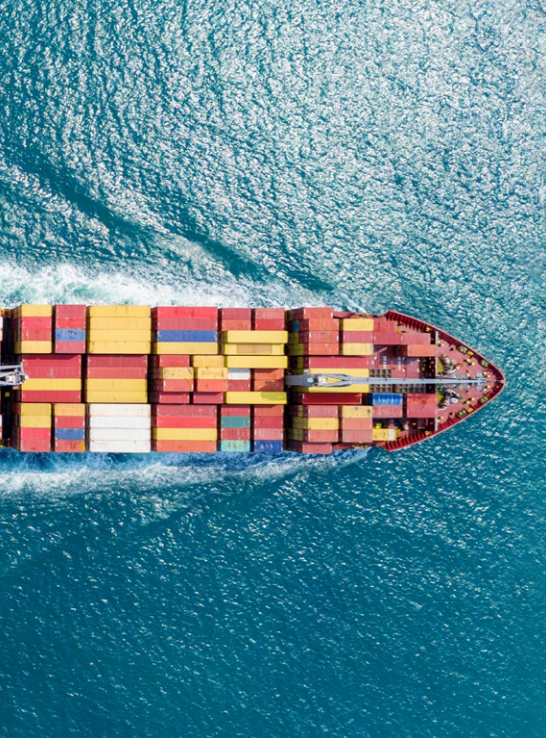
Like many other forms of crime, fraud is constantly evolving. Perpetrators are continually seeking to exploit new developments and trends to enhance their fraudulent activities. Therefore, in addition to the six types of fraud previously discussed, it's crucial to remain vigilant about:

AI-driven fraud

Artificial intelligence (AI) has boomed in the past few years. While the concept of AI isn't anything new, its proliferation among the public, businesses, and fraudsters has allowed the technology to be used for advanced forms of social engineering.

AI tools can scrape social media, emails, or leaked data to craft highly tailored phishing messages that are grammatically perfect, context-aware, and incredibly convincing. Deepfake technology has also enabled the creation of highly detailed spoof images and videos of various individuals,[27] fuelling a rise in deepfake scams being attempted every five minutes in 2024.

[27] *Deepfake Scams Are Stealing Millions—How To Spot One – Forbes: https://www.forbes.com/sites/alexvakulov/2025/03/09/deepfake-scams-are-stealing-millions-how-to-spot-one/*



Supply chain vulnerabilities

Supply chain fraud is a growing concern among businesses worldwide. Despite advancements in recent years, supply chains are still prone to attacks at numerous stages. Reports show that procurement fraud had increased by 13% year-on-year among over 170 UK companies[28], such as incidents where staff awarded contracts to companies they held undisclosed financial interests in.

Supply chain analysts from BSI Consulting report a year-on-year increase of thefts in-transit, from 27% in 2023 to 41% in 2024. Additionally, BSI reports that strategic thefts involving fraudulent activity most often take place in Brazil, India, Germany, and the UK.[29]

Without proper checks on buyers and suppliers, like regular monitoring, payment verification, and vetting, businesses become far more exposed to financial and operational damage.

[28] *173 companies report procurement fraud up by 13% – International Accounting Bulletin: https://www.internationalaccountingbulletin.com/news/173-companies-report-procurement-fraud-up-by-13/*

[29] *One lens of risk: Elevating resilience with supply chain risk management – BSI: https://page.bsigroup.com/l/73472/2025-02-26/2ccb3j5/73472/17405904141QLLGfGS/BSI_Consulting_2025_Supply_chain_risksand_opportunities_report.pdf*

Highlighting real-world fraud cases

The Cloned Call

An energy company received a call from a "CEO" with an urgent demand for a total of $243k to be transferred to an account held in "their" name. The attack involved a fraudster utilising voice imitation software powered by artificial intelligence, allowing them to connect one-on-one with the company's director.[30]

While the request initially raised alarm bells, the director proceeded with the transfer due to the urgency of the situation.

Shortly after the first phone call, the director received another, with a near-identical request for even more funds to be sent. Thankfully, this second call was enough to trigger the director's suspicions, prompting them to hang up and reach out to the CEO via their personal number.

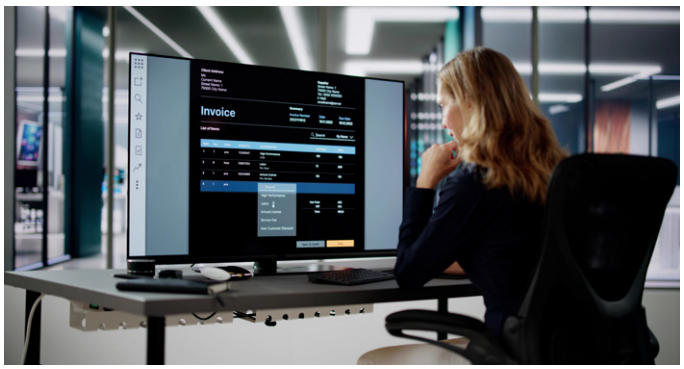
While speaking to the CEO, who was understandably confused, the director saw another phone call come through from the fraudster. At this point, the realisation settled in.

The Swindling Supplier

Working for a family company, an employee abused their position of trust by misrepresenting the value of invoices and delivery notes.[31]

The scam saw one individual working inside the company issuing invoices with exaggerated values, far exceeding the needs of the family business. Together with a supplier, the two falsified financial records, leading to the family business overpaying for stock that wasn't delivered. In exchange, the employee received cash handouts from the supplier as a cut of the profits.

After five years, an internal audit revealed that stock worth a total of £1.1m was completely missing, which eventually led to the arrest of the employee.



[30] *Bandits steal $243,000 with deepfake audio mimicking CEO voice – Perallis Security: https://www.perallis.com/blog/bandits-steal-243-000-with-deepfake-audio-mimicking-ceo-voice*

[31] *Two jailed for tricking family business in £1m invoice fraud scam – BBC News: https://www.bbc.co.uk/news/uk-england-stoke-staffordshire-65167757*

The Trusted One

After climbing through the ranks over many years, a fraudster manipulated their position of trust by gradually embezzling £600k worth of funds from their employer over the course of three years.

Working in a senior position, the employee was well regarded among their peers and often received acknowledgements for their contributions toward company goals. This glowing performance had granted them access to many company assets such as cars, facilities, and bank details.

After striking up a friendship with a newer employee, the two began to spend time with each other outside of work, often going out to lunches and dinners together. It was only when the fraudster boasted about said activity being funded "by the company" that they revealed the extent of their embezzlement.

The newer employee brought this information to human resources. After this, a deeper investigation was conducted into the fraudster's activities, revealing the £600k deficit. Numerous undocumented transactions were revealed to the employer, in addition to a pattern of frequent, small withdrawals over a sustained period.

The Disappearing Buyer

A UK-based food producer received a large order for premium goods from what appeared to be a reputable overseas supermarket. The buyer provided official documentation, used familiar contact details, and maintained convincing communication throughout the process.

After dispatching the goods, worth over £300k, the supplier discovered the delivery address was untraceable and payment never arrived. Closer investigation revealed the buyer's identity had been fabricated using cloned details of a genuine business. The goods were never recovered.[32]

[32] Neal's Yard Dairy Victim of Theft, Reaffirms Ethical Commitment to Pro – Neal's Yard Dairy: *https://www.nealsyarddairy.co.uk/blogs/news/press-neal-s-yard-dairy-victim-of-fraud-reaffirms-ethical-commitment-to-producers?utm_source=chatgpt.com*

How fraud penetrates a business

As evidenced in the real-world examples, fraud can happen in many ways:

Weak internal processes

Fraud thrives in businesses that fail to instil suitable procedures for dealing with attacks. Whether it's too much or too little responsibility, or a lack of an incident reporting process, fraud attempts can go unrecognised, undocumented, and unchecked. This allows for the spread of confusion, adding even more difficulty.

Exploitation

Exploitation is ultimately what underpins most fraud attempts. Whether it's people, technology, or processes, attackers find or poke holes in your business until something comes undone.

- **Trust:** Strong business is built on trust and authority. Executives in high-paying positions are trusted to steer companies in the right direction, and suppliers are trusted to deliver their goods and services on time. However, this trust can be manipulated, offering attackers advanced access to sensitive company details and tools for their own gain.

- **Urgency:** Many businesses work to tight deadlines. This creates a fast-paced environment, which often lowers inhibitions and alertness in pursuit of meeting demand, allowing attackers to slip under the radar.

Over-reliance on digital communication

Although instant messaging, email, and video calls have paved the way for more efficient communication between employees, an over-reliance on these can make a business more vulnerable.

While many providers of digital communication tools offer reassurance, particularly through security procedures, they can still be penetrated. Without face-to-face meetings, for example, it's not always possible to verify someone's identity.

How to COMBAT fraud

Fraud attempts can't be prevented. However, there are various processes that businesses can implement to mitigate the risk.

1. Communication

Transparency is key to unlocking better fraud risk mitigation, and it ultimately begins with open communication. Encouraging people to talk about fraud within your business can provide employees with a safe space to report questionable activity, free from judgment.

However, it's not just internal communication. Openness and honesty are two virtues that define how a business recovers from fraud. If an attempt may have compromised your customers' personal or sensitive data, you should let them know as soon as you can.

2. Observation

Without adequate measurement and reporting procedures, it's impossible to track fraud attempts across your business. But this is only half of the story. To truly ensure your procedures are in an optimal state, you'll also need to regularly test your mitigation measures to see if they meet expectations.

3. Management

High-level, senior figures carry a lot of influence throughout an organisation. As such, there's a need to "lead by example" from the top down and instil an ongoing commitment towards anti-fraud procedures wherever possible.

4. Background check

Knowing and trusting your suppliers and B2B buyers is essential for successful business dealings. It's in every business' best interest to vet their suppliers prior to any substantial work taking place. While doing this, be sure to verify:

- The name of the supplier
- Their business address
- Any associated individuals
- Testimonials from other customers
- Creditworthiness

With our graded system Grade Check, you can assess the risk profile of your clients. Grade Check grants insight into client creditworthiness, backed by our global intelligence as an experienced leader in trade credit insurance.

5. Assessment

All businesses are at risk of fraud. But some are at more risk than others. An essential step in reducing this is to identify the parts of the company where it is most prevalent by conducting regular, ongoing risk assessments.

Risks can come from many avenues, be that a gap in commercial insurance protection, lack of training in a particular department, or poor security protocols.

Find out where your business may be vulnerable

Allianz Trade's Business Fraud Insurance team offers a fraud risk gap analysis. This analysis helps highlight prominent gaps in a business' current risk mitigation procedures in the initial stages of an enquiry, while also supporting a reduction in policy premium at the start of a new term. To arrange your own risk gap analysis, **get in touch**.

6. Training

They say a chain is only as strong as its weakest link. Well, the same applies to fraud risk mitigation.

Employee training is the cornerstone of safeguarding against fraud in your business. Without adequate knowledge of how fraud occurs, employees are poorly equipped to deal with breaches and attempts. Therefore, an up-to-date, ongoing anti-fraud training regime is highly recommended.

Access our insights

All Allianz Trade Business Fraud Insurance policy holders are granted access to our Fraud Resilience Library. This curated collection of e-books and guides covers many high-impact fraud subjects, such as social engineering, AI-enabled fraud, and online payment fraud.

Where do you stand on fraud resilience?

Mitigating fraud risks is a complex process that involves many moving parts. It doesn't stem from just one function of a business – it requires a combination of people, processes, systems, and policies working in tandem.

People

The hard-working people within a business are ultimately the first line of defence against fraud attempts. Most fraud begins with social engineering, which preys on ill-informed, potentially vulnerable members of staff. We recommend starting your mitigative measures here.

- Are your staff trained to spot fake authority?
- Do you have efficient fraud reporting procedures?

Processes

The internal mechanisms a business has in place to prevent fraud can greatly dictate how it responds to incidents. With well-distributed documentation on procedures like issuing payments to suppliers, verifying contact details, and logging into company resources, employees can carry out their jobs in a safe, secure way.

- Are dual approvals required for high-risk payments?
- Do you independently verify new contacts?

Technology

Building on processes, the technology that your employees have access to can also be used against them. However, through proper regulation and investigation, you can allow your employees to do their best work, away from prying, fraudulent eyes.

- Have you ensured controlled access to financial systems?
- Do you use AI or fraud detection tools?

Policy

Clear guidance is helpful across a wide variety of businesses. With set parameters around responsibilities, and fair expectations given to employees of all levels, blurred lines become a thing of the past.

- Are there clear roles and responsibilities?
- Do you have a documented fraud response plan?

Business Fraud Insurance as part of your risk strategy

It's impossible for businesses to eliminate all fraudulent attempts against their organisation, but it doesn't have to be detrimental to operations.

What is business fraud insurance?

Business Fraud (also called Crime or Fidelity) Insurance is a specialised policy designed to protect companies from financial losses due to fraudulent activities, ensuring stability and continuity. It supports your fraud resilience in three ways:

- **Proactive measures:** Access tools and guidance to strengthen your fraud defences and reduce risk before issues arise
- **Crisis support:** Get immediate help from fraud specialists to manage the response
- **Indemnification:** Gain financial scover for direct losses from insured fraud events

Allianz Trade: your trusted partner in Business Fraud Insurance

At Allianz Trade, we understand the critical importance of safeguarding your business against fraud. Our solution offers robust protection against both internal and external threats. From employee theft and embezzlement to external scams like payment diversion and impersonation, our policy covers it all.

But we go further than financial cover. Our policy includes:

- **Tailored protection** that adapts to your business profile
- **Unlimited retroactive cover** for past events, offering peace of mind
- **Business continuity support** for up to six months after a fraud event
- **Access to expert support** when you need to respond quickly and effectively

With over 60 years of experience and deep expertise across European markets, we help your business stay resilient — not just reactive.

Our service and expertise

- Our business fraud team handles several hundred claims per year
- Claims can be paid out as quickly as 48 hours
- German market leaders in fraud insurance for decades
- 50+ dedicated fraud experts across Europe supporting several thousand clients
- High overall client satisfaction leading to exceptional retention rates
- Average client tenure of 10+ years

Take the next step

Business fraud remains a complex issue that can't be solved with quick fixes. Technology has enabled fraudsters to keep pace with many preventative measures, which puts greater pressure on businesses to stay not just one, but many steps ahead. That's where we can help. Our Business Fraud Insurance offers not just cover after the fact, but practical support to help reduce exposure and tackle fraud early.

Want to know where your risks lie?

Book your free, no-obligation consultation with one of our fraud specialists.

You'll receive:

- A tailored fraud risk gap analysis
- Expert guidance to strengthen your internal and external defences
- A clearer view of how business fraud insurance can support your business

Contact us

Call +44 (0)20 7860 2063
Email businessfraudinsurance@allianz-trade.com

Or request your consultation at allianz-trade.co.uk/fraud

AUGUST 2025