

Managing fraud risks

How to keep fraud out of your business

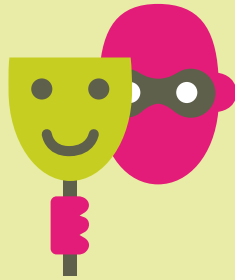


Fraud is much more common than most people imagine. It can happen to any business, including yours. That makes managing potential fraud risks an essential part of good business practice.

This guide explains how to make a solid start managing your own fraud risks, with practical steps to help keep your business safe.

What is fraud?

Put simply, fraud is stealing by deception. If somebody lies to steal money, property or data, then they have probably committed fraud.



Fraudsters aren't always who you would imagine. They could be a trusted colleague, a relative, a supplier, or a customer. But they could also be someone you don't know – perhaps pretending to be someone you do.

Fraud takes many forms.

- Submitting a false invoice.
- Buying something using fake or stolen card details.
- Making an inflated claim for business expenses.

All these are common examples of fraud.

Why is it important to manage your risks?

If you haven't been targeted yet, you are in a fortunate minority.¹

Actively managing your fraud risk, and not leaving it to chance, is good for business and good for your bottom line. Preventing fraud – or at least spotting it early and putting a stop to it – can head-off financial losses and reputational damage and might even save your business from collapse.



What does it mean to manage fraud risks?

It means implementing procedures that are proportionate and proactive, but which don't have to be expensive or complicated.

Ideally, aim to progressively build fraud resilience into every part of your business.

- Use hard controls (such as secure passwords and system access restrictions) as well as soft ones (policies and procedures that are clear and well communicated).
- Get every member of staff and management, at every level, actively involved.
- Look beyond your organisation. Reach down through your supply chain to work with your suppliers, then out to the very front line of the business to your customers.

The fraud management lifecycle



Watch out for these common risks

Cybercrime

Crime committed online. It might be a hacking; phishing; ransomware or DDoS (distributed denial of service) attack on computers, networks and mobile devices; or using the internet to commit a traditional crime like harassment, bullying or fraud.



Staff fraud

An employee using their job to commit fraud. This can happen at any point, from hiring to leaving. Common examples include lying on a job application, forging documents to inflate expenses, and stealing stock or data to misuse or resell.



Financial statement fraud

The deliberate altering of financial statements to conceal the true business position or performance. Common examples include creating bogus sales, inflating the value of assets or concealing debts.



Procurement fraud

Fraud in the buying of goods, works and services. This can happen at any stage, from initial decision-making to final delivery. Frequently two or more people will cooperate (or conspire). Often they will work for the victim and/or one of its suppliers. Sometimes several suppliers will work together to defraud a customer, which could be you.



Payment fraud

Using stolen or cloned card details to make purchases, often via online transactions, over the phone or by email (so-called 'card-not-present fraud').



Fraudsters also impersonate genuine suppliers (or other trusted third parties such as banks, the police or HMRC) so that legitimate payments are diverted into bank accounts that they control.

To find out more about these frauds check out our toolkit at lovebusiness-hatefraud.org.uk.

Responding to risks

Once you understand the risks you can respond in one of four ways. Which one you use will depend on how much risk your business is ready and able to accept (this is your so-called 'risk appetite').

- **Accept it:** Perhaps the risk seems tiny or the cost of reducing it is too great. (Risks that seem acceptable now should still be monitored and reviewed regularly in case they become unacceptable.)
- **Transfer it:** Typically to a third party, like an insurance company.
- **Tackle it:** Perhaps by implementing controls to reduce the likelihood or lessen the potential impact.
- **End it:** By halting whatever activity is creating the risk in the first place.



StoneTurn

Thanks to Lucy Cryan from StoneTurn for kindly writing this guide. Published March 2023. © Fraud Advisory Panel and Barclays 2023. Fraud Advisory Panel and Barclays will not be liable for any reliance you place on the information in this material. You should seek independent advice.

This work is licenced under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Licence.



Love business. Hate fraud.

This practical guide highlights some of the things you can do to manage the risk of fraud to your business. But it always makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on [Twitter](#) and [LinkedIn](#).



¹ PWC (2022). [Global Economic Crime Survey 2022: UK Findings](#)

Managing fraud risks

How to keep fraud out of your business



A checklist

Ask yourself...

- What fraud risks are we exposed to?
- How bad could things get if each risk became a reality?
- How often might that happen?
- What can I now do about the risks and consequences I've identified?

Do...



- Be crystal clear with all staff and suppliers that your business takes every fraud seriously.
- Make regular, well-informed assessments of the risks you face. And involve your staff!
- Include fraud on your risk register and review it regularly.
- Make sure someone with sufficient authority is responsible for overseeing all fraud matters.
- Clearly set out the standards of behaviour expected of staff, suppliers and other third parties. Formal policies covering fraud and conflicts of interest can help you do this.
- Using communications and training, embed fraud prevention culture and thinking throughout the business.
- Exercise appropriate due diligence when selecting staff, contractors, suppliers and others, both as a form of risk assessment and a means of mitigating risk.
- Have a simple, hassle-free way to raise concerns about fraud. Make sure it is available to staff and anyone you do business with.

- Monitor and review the effectiveness of, and compliance with, anti-fraud policies, procedures and controls, then make improvements as necessary.
- Create a fraud response plan and practise it regularly to make sure it works.
- Include lessons learnt in employee training about previous frauds.
- Consider the need for crime insurance.
- Trust your instincts. If something feels wrong, it probably is.



Don't...

- Expect staff to understand the term 'fraud' if you haven't defined it for them.
- Underestimate the importance of a strong 'tone from the top'. When owners and managers are seen to follow the fraud prevention standards set by the business, employees are much more inclined to do the same.
- Adopt generic control policies and procedures across the business – risks often vary across operations, so responses should too.
- Assume that 'once is enough' when communicating anti-fraud policies and procedures to staff. Training needs to be refreshed and re-delivered regularly.
- Encourage staff to confront suspected fraudsters and/or investigate their own suspicions. It could be dangerous or cause evidence to be destroyed.
- Ignore red flags. Make sure risks are addressed.

Protecting your business

A few simple steps can make your business safer.

Set the tone from the top

Good fraud risk management starts at the top. It is not enough for senior people to simply talk the talk, they must walk the walk as well. Owners, directors and managers must lead by example, setting the standards of behaviour expected of everyone else – staff, suppliers, contractors and other third parties.



Assess your risks

Be aware of all possible risks so that you can identify, assess and manage them across the whole operation. Seek out areas most at risk. Focus your attention where it is most needed by thinking about all the ways money, assets and data flow into, through and out of your business.

Whenever a risk is identified add it to your risk register. Include details of its nature, likelihood, potential impact and the controls that will help to prevent it.

Take steps to prevent fraud

Think about how you will reduce the likelihood of each risk becoming a reality. Which policies and controls are needed? Should you segregate finance duties, implement authorisation thresholds, limit access to certain IT systems or office areas, conduct checks on new recruits, consider propriety checks on new business partners, suppliers and service providers?

And don't forget to consider insurance. Do you need cover for crime protection (fidelity, cyber) and/or a directors' and officers' liability?

Have ways to detect fraud

Even the best controls won't stop every fraud. Create manual and automated systems and processes that help you detect fraud by providing early warnings.

At the very least educate staff to identify common frauds, encourage staff to raise their concerns or suspicions, conduct spot audits (stock, sales, purchase ledgers and the like), and review profit and loss statements regularly.

Have a response plan

Be prepared to act quickly and decisively. Have a response plan ready and make sure it is well understood so that everyone knows what they should do and when. Include:

- details of the investigation process (who, what, when and how);
- any duties to report fraud (to shareholders, customers, banks, insurance companies and regulators); and
- the action (disciplinary, regulatory, civil, criminal) to be taken against the culprits. (Remember, different responses require different standards of proof.)



Monitor and review

In the event of a fraud, review what happened and take remedial action urgently to stop anything similar happening again.

Business practices and activities often change over time, so review policies, procedures and controls regularly. Make sure they are still fit for purpose and appropriate to the needs of your business. A good way to do this is with an annual fraud risk assessment.



StoneTurn

Thanks to Lucy Cryan from StoneTurn for kindly writing this guide. Published March 2023. © Fraud Advisory Panel and Barclays 2023. Fraud Advisory Panel and Barclays will not be liable for any reliance you place on the information in this material. You should seek independent advice.

This work is licenced under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Licence.



Love business. Hate fraud.

This practical guide highlights some of the things you can do to manage the risk of fraud to your business. But it always makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on [Twitter](#) and [LinkedIn](#).

