Understanding staff fraud

How to keep fraud (and fraudsters) out of your business

Businesses like yours are losing as much as 5% of their revenue to fraud committed by their own staff.[1] Understanding how (and why) is the first step in stopping it happening to you.

This guide will help you understand the risks and think about the practical things you can do to keep safe.

What is staff fraud?

Staff fraud has many names – insider, internal, workplace, employee or occupational fraud – but it is always the same thing: an employee is using their job to commit fraud.

They may act alone or in collusion with someone else. Sometimes they will have been recruited by a criminal gang to be 'on the inside'. Sometimes they might even be a trusted colleague, friend or relative.

Who commits fraud?

Some staff pose higher fraud risks than others.

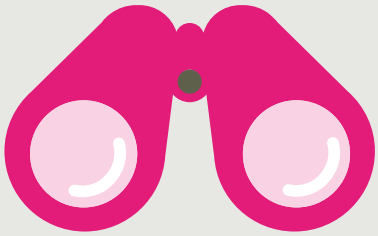
If your business has high staff turnover for whatever reason, it could be particularly at risk.

High-risk employees typically include anyone:

- in a senior position or with lots of autonomy;
- with a current or historic grievance;
- working-out their notice because they are about to leave; or
- in a position to influence the company's financial systems.

Know the signs

Certain kinds of staff behaviour should set alarm bells ringing [2] – and prompt you to take a closer look – even though they may not be clear-cut evidence of fraud.



Does anyone appear to be:

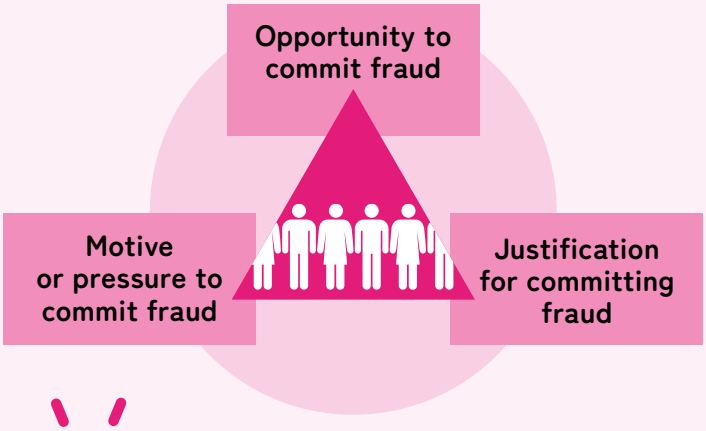
- living beyond their means;
- having family or financial problems;
- struggling with drugs, alcohol, gambling or some other addiction?

Or are they:

- unwilling to share their duties or hand over tasks to others;
- sensitive about what they do and how they do it;
- aggressive or bullying so that others are reluctant to challenge them;
- unusually close to one customer or supplier in particular;
- reluctant to take holidays;
- working excessive hours or staying late after everyone else has gone home;
- behaving out of character, perhaps by being more secretive or controlling?

Why do they do it?

Understanding what can lead staff to commit fraud is the first step in preventing it.



Opportunity: If your financial controls are weak, non-existent or inconsistently applied, security systems are poor, or your employment policies and procedures are unclear, you are almost certainly making it easier for a staff member to commit fraud.

Clear rules and strong controls – which are understood by all and apply to everyone – are very important in preventing staff fraud.

Motive: People sometimes believe they have been driven to commit fraud. Common motives include money problems (including greed!) and personal problems, like addiction or a relationship breakdown. They may have a grievance of some kind against you, their employer. Perhaps they are being blackmailed. Or they may simply be looking for thrills.

Justification: Fraudsters often need an excuse for the things they have done wrong. They tell themselves things like: 'I'm only borrowing the money – I'll pay it back when I get straight'; 'They owe me for all the unpaid overtime'; 'The money's mine – I haven't had a pay rise in years'; 'They are getting what they deserve – they make it easy'.

The cost-of-living crisis should remind us that economic hardship makes people desperate and unfairness breeds resentment, increasing the risk that someone will act dishonestly.

A key part of good insider-fraud prevention is to watch out for your staff, treat them well, and do what you can to support them through hard times, financial difficulties or problems with drugs, alcohol or gambling.

Beware of risks at every stage of employment

Are you confident your recruitment and employment procedures are up to scratch? If not, fraud can easily creep in undetected.

Hiring staff

Applicants may lie about their qualifications, previous experience or right to work in the UK. They may hide unspent criminal convictions and provide fake or altered documents and references. Even genuine documents may have been obtained using false information.

During employment

Staff may hide unethical relationships, or even criminal associations, inside and outside work. They may abuse their position in any number of ways: taking kickbacks from suppliers; selling confidential information to competitors; forging documents to inflate expense claims; falsifying sales to boost bonuses; reporting sick while working a second job.

Leaving the business

Departing staff may see this as their chance to steal without consequences, taking stock, data or confidential information to misuse or sell-on later.

FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

Thanks to Andrew Herring from Pinsent Masons LLP for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights some of the potential staff fraud risks to your business. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.

[1] Association of Certified Fraud Examiners (2022). 'Occupational Fraud 2022: A Report to the Nations'.

[2] Ibid.

Understanding staff fraud

How to keep fraud (and fraudsters) out of your business

Love business Hate fraud

A checklist

Ask yourself...

- How confident am I that this applicant is who they say they are?
- Have I done enough to really get to know my staff?
- Have I spoken to my staff recently about our fraud risks and how to reduce them?

Do...

- Be crystal clear with all staff that your business always takes fraud seriously.
- Have a written anti-fraud policy and code of conduct covering all staff at all levels.
- Make everyone aware of the fraud risks to the business and to themselves.
- Have a simple, hassle-free way for staff to raise their concerns about fraud.
- Keep a record of all conflicts of interest, gifts and hospitality (given and received).
- Make sure staff teams are properly supervised and have clear reporting lines.
- Test operating procedures regularly to make sure they work properly and are being followed by everyone.
- Use pre-employment screening of new recruits and in-service checks for established employees. Make sure everyone knows about them.
- Make sure any digital monitoring and surveillance complies with UK privacy laws and other legislation. You might need specialist advice.
- Recover all business assets from departing staff and make sure they no longer have access to systems and buildings.
- Be alert to what is going on in your employees' lives, especially anything that might put them under increased pressure.

Don't...

- Tolerate workplace fraud.
- Rely on trust – it is not a fraud control.
- Take shortcuts when recruiting.
- Simply assume that policies and procedures are being followed.
- Ignore staff fraud risks.

Protecting your business

Some simple steps can make your business safer.

Screen everyone

Do pre-employment checks for all new recruits, permanent and temporary. Insist on original proof of ID. Check qualifications with the issuing body or the Higher Education Degree Datacheck service. Check work history and take up references before they start work. For senior and finance positions consider enhanced checks.

Perform periodic checks and ongoing monitoring

Let existing staff know you will be screening them periodically too, including when they are promoted or given a new role. Think about ways to watch out for unusual and out-of-character behaviour. Consider the need for digital monitoring of staff email, internet and phone use, as well as traditional CCTV and video surveillance (where appropriate).

Separate sensitive staff duties

Try to segregate financial responsibilities like authorising/making payments (including expenses) and changing bank account details. Do bank reconciliations routinely to help you spot anything unusual.

Encourage staff to raise concerns

Make it easy for staff to raise their concerns or suspicions. Have clear policies and promote them with your employees. Posters, videos, quizzes and blogs can all be good ways to do this.

Manage leavers

Have a formal process for managing all leavers (staff and contractors). You might need to vary it according to their reason for leaving, who the new employer is (are they a competitor?), the current role and the access they had to sensitive information. Always include things like:

- returning business equipment and other physical assets (security passes, keys, company phones, laptops, credit cards, files, etc);
- removing access rights to business premises and electronic systems;
- deactivating email accounts;
- cancelling credit cards and bank mandates; and
- removing the person from the payroll.

FRAUD ADVISORY PANEL

Sponsored by BARCLAYS

Thanks to Andrew Herring from Pinsent Masons LLP for kindly writing this guide.

Love business. Hate fraud.

This practical guide highlights some of the potential staff fraud risks to your business. But business fraud comes in many other guises. It makes good business sense to find out more.

Go to lovebusiness-hatefraud.org.uk or follow the campaign on Twitter and LinkedIn.