

Internal fraud

Who commits it? ... and why



Ryan Mer
managing director
eftsure Africa

International Fraud Awareness Week took place from 14–20 November, highlighting an increasing problem that organisations around the world are facing. According to the Association of Certified Fraud Examiners (ACFE), businesses lose around 5% of their annual revenue globally due to fraudulent behaviour, which experts estimate amounts to a total annual loss around the world of \$3.7 trillion.

Fraud can hit organisations from various angles, and even though cybercrime and external fraud attacks are a huge risk, more often than many companies realise it is perpetrated from within. In fact ...

“The Global Economic Crime and Fraud Survey showed that 41% of economic crimes in South Africa were committed by employees, compared to only 36% by external fraudsters and 21% a collusion between the two.”

Ryan Mer, Managing Director, eftsure Africa, a Know Your Payee (KYP) platform provider says it is crucial to be alert to fraudulent activity within

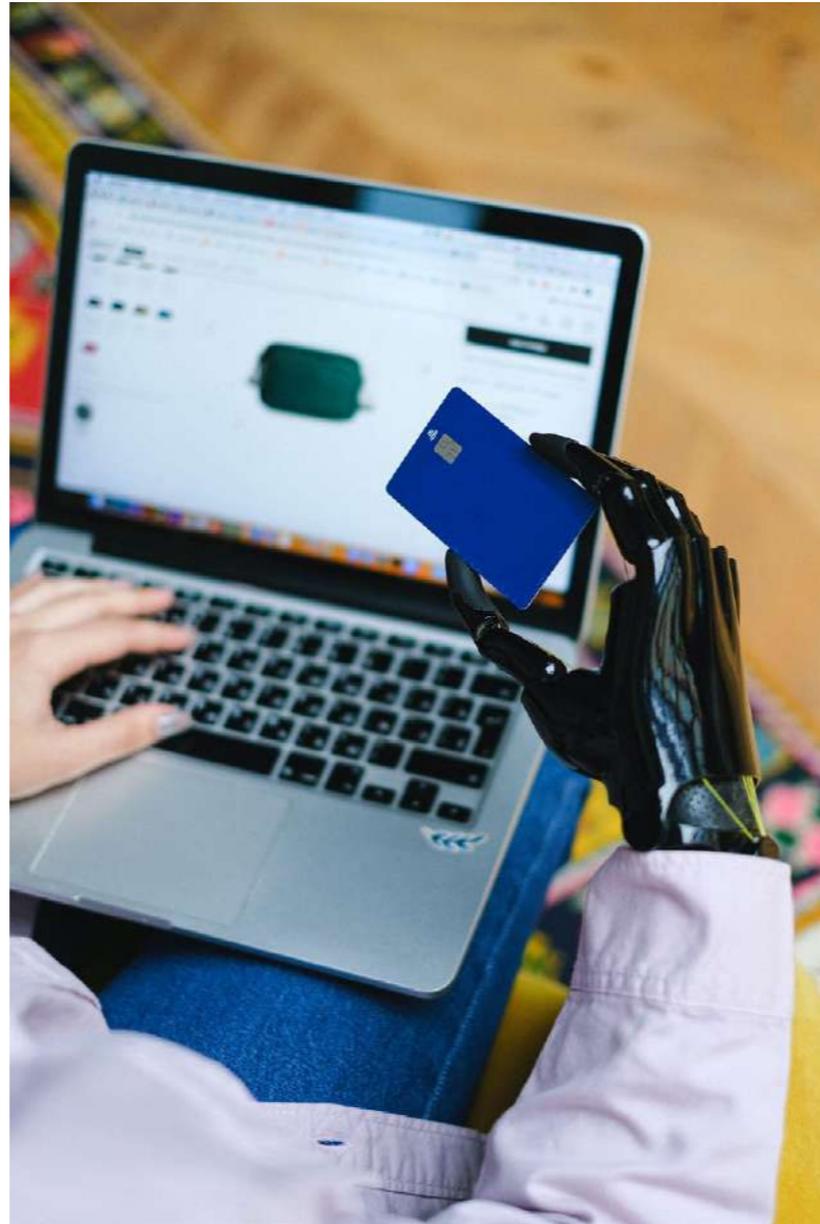


Image: Anna Shvets, Pexels

your organisation and to catch it as early as possible. To do this, you need to understand what drives employees to engage in fraud. “From our experience and conversations with clients

when assisting those who have dealt with fraud internally, employees do not set out to defraud a company and it is usually someone who has been with the company for some time and someone who is seen as unlikely to participate in criminal activity.”

“Criminologist Donald Cressey published a model called the ‘fraud triangle’, which outlines the three factors that can cause employees to commit occupational fraud: motivation, opportunity and rationalisation.”

When an employee has a reason for committing fraud, gets a chance to do so without getting caught, and can come up with a justification for their behaviour, they’re more likely to commit an occupational crime. “The past two years of Covid-19 lockdowns have negatively impacted household finances, providing ample motivation and justification for committing fraud. In the minds of many, desperate times call for desperate measures. Organisations need to be cognisant of this and act accordingly,” advises Mer.

Some of the warning signs exhibited by employees that may indicate fraudulent behaviour include:



- Living beyond their means. Look out for employees who exhibit a drastic change in lifestyle, suddenly arriving at work in an expensive car, flashing designer gear and boasting about new real estate acquisitions with no real reason for the change.
- Guarding their turf. A fraudster won't want to share their duties and may resist taking holidays so nobody can step in for them.
- Have unusually close relationships with a vendor or customer. This allows the fraudster the opportunity create fictitious orders or receive kickbacks. Be on guard if a supplier insists on dealing with one specific employee.
- Working long hours. An employee who comes in early, stays late, works on weekends and does not take sick or annual leave are all red flags. This could indicate that the employee does not want to share their responsibilities with other employees who may detect fraudulent acts.
- Working in a position to commit fraud. Positions that involve administering payments to creditors and suppliers, overseeing and processing invoices and electronic payments, and capturing bank statement transactions present a higher risk for businesses. Fraud can be committed by changing the banking details of suppliers, especially ad hoc suppliers, and adding fictitious suppliers or employees onto the payroll.



Image: Mikhail Nilov, Pexels

How to prevent fraud

By looking at the three factors in the 'fraud triangle' mentioned above, business owners can help to prevent employees from resorting to fraud.

- Relieve the pressure. Remove the motivation to participate in fraudulent behaviour by showing empathy for your employees and offering the support they need in good times and in bad.

- Remove the opportunity. Tighten up your accounting policies and ensure strong internal controls to prevent payments fraud. A common thread in cases of fraud is the human element. A Software as a Service (SaaS) provider can help limit these risks by providing an integrated payments platform that provides organisations with the ability to digitise and automate the verification of payees and eft payment data, on a continuous basis
- Deal with rationalisation. Don't give employees the chance to justify fraudulent behaviour. Develop a transparent and collaborative approach to business that treats employees fairly. This way you're less likely to have disgruntled employees more likely to get involved in fraudulent behaviour.

In the current economic climate, employees may be more tempted to perpetrate fraud, making it vital for organisations to implement best practice anti-fraud strategies. "People combined with technology and sound business processes are at the frontline of fighting fraud and mitigating risk. By building a culture of security within an organisation that ensures cooperation between employees and technology, it is significantly more difficult for employees to commit white-collar crime," says Mer. **SR**

About eftsure: eftsure is a comprehensive, system agnostic solution, designed to give businesses the ability to manage, control and secure the full lifecycle of a payee from onboarding through to the actual point of payment.