BUSINESSFIRST
THE MAGAZINE FOR BUSINESS LEADERS MAGAZINE

Dealing with payroll fraud

Tracy Angwin 0

What could have been done to stop a lone employee stealing almost $20 million from her employer asks Tracy Angwin.

Although it's impossible to accurately quantify, payroll fraud is more common than you might think. Unfortunately when there are large amounts of money exchanging hands on a regular basis, you will find people who want to take advantage of it and siphon some for their own benefit.

However, there are things that you can do to help ensure the fraud risk in your payroll is minimised.

The reality is that the best friends of the fraudster are mediocre processes, untrained people and loose systems. The more work you do in tightening your processes, paying particular attention to accountability, the less likely your money will be stolen.

With the realisation that most payroll fraud cases go unprosecuted, due to the minimal chance of recovering the funds, the fraud is often not reported in the press and it is simply managed by internal HR processes and written off.

A major clue in payroll fraud is someone living way beyond his or her means. This was particularly evident in the largest payroll fraud in Australian history.

Sonya Causer was the Payroll Manager at Clive Peeters, the large electrical retailer, reportedly being paid $125,000 in her role. Over a two-year period Causer stole $19,365,768 from her employer.

Surprisingly, her colleagues failed to notice behaviour that was odd for a 38-year-old payroll manager on such a salary. It may be human nature to downplay or even dismiss warnings that we don't want to see, but there would have been plenty of clues to suggest something was seriously wrong.

No one took notice of the fact Causer was running a significant property portfolio, which consisted of 44 properties in Melbourne's eastern suburbs, purchased over 18 months. She also bought several cars and motorbikes and thousands of dollars worth of jewellery. She was also at one point, one of the largest private shareholders in Clive Peeters, having spent some of the stolen money on Clive Peeters shares.

Causer was deemed so trustworthy, that she initially assisted the company's auditors in the investigation of her own fraud.

But after her initial denials, Causer admitted to the fraud. The properties, including her family home, were sold as part of the restitution. There remains a shortfall of $3 million.

So, what are the seven most common areas that give rise to suspected fraudulent payroll activity?

1. **Payroll audit trail**
   If your payroll system doesn't have a robust audit trail or if it does and you aren't using it to audit critical fields, you need to address this today. The payroll audit trail will often point directly to fraudulent activity and show up the areas that need to be investigated.The activity that you might be looking for is varied, but if there is fraudulent activity in your payroll it is often quite obvious to someone who understands the process. I can't stress enough how important it is to ensure the auditing feature of your payroll system is working so it's available if and when you need it.
2. **Regular masterfile changes**
   If there are regular changes in employee bank details or entitlement balances, this should be investigated. There could be simple explanations for these changes, but it is a common red flag in payroll fraud.
3. **Duplications of data and ghost employees**
   Although I have come across cases of twins that share a bank account and live at home with their parents being on the same payroll, this is rare indeed! If you identify duplicate names, addresses, dates of birth, tax file numbers or other masterfile details, you should investigate further to eliminate the risk of ghost employees.
4. **Out of hours access**
   Much fraudulent activity occurs out of normal office hours and often by remote access to the payroll system. If people in your organisation are regularly accessing the payroll outside business hours, the need for this access may need to be questioned. Alternatively, after hours activity should be audited.
5. **Loose security**
   I'm a firm believer that the only people that should have write access to a payroll system are those that are in the business of paying people. Anyone else, including senior management, should have restricted or read only access. Not only does this reduce the possibility of payroll fraud, it protects those who only need read only access from suspicion.
6. **Sharing logins or using obsolete logins**
   Sharing logins is an absolute no-no and concerns should be raised about anyone who does this. If you have a genuine reason to access a payroll system you need to have your own login and password. Likewise, with turnover of payroll staff you should ensure that old logins are deleted so no third party can use them.
7. **High percentage of casual employees**

Although not cause for suspicion in itself, much payroll fraud is committed using a casual workforce. If you have a high percentage of casual employees, more attention needs to be given to processes that minimise or eliminate the opportunity for payroll fraud.

So what checks and balances did Clive Peeters have in place? Not so many it seems.

Perhaps they should have paid more attention to instinct and gut-feel. If you have a niggling feeling that something is wrong, no matter how big or small, investigate it. It seems quite unfathomable that someone was able to steal so much money, for so long, without being noticed.

There are many morals to this story, but the most poignant of all is this: if you are not on the ball, you may have no one to blame for payroll fraud but yourself.