

## IS YOUR COMPANY A VICTIM OF FRAUD?

It is never an enjoyable day for a company director or in house counsel, when they discover that the company has been the victim of fraud, especially when the perpetrator is a colleague or close supplier. The first question following this discovery is usually "how big is it", followed quickly with "how did we miss this?" The truth is, incidents of internal and close supplier nature are extremely common and can be very difficult to detect. Global trading, global company structures, electronic payment systems and the sheer volume of electronic data and communication are all major contributing factors that make the problem ever more difficult to detect.

There is a lot of commentary that businesses are becoming victim to these practices more often and that they should continue to keep their guard up. Often these are reports by those organisations with an interest in selling the latest fraud prevention software or audits. However, that view is not entirely correct. Although it is obviously important for businesses to remain vigilant, there is a view that the problem is as much of an issue now as it has been for a number of years. In a recent poll by Deloitte published in New York in April 2016, it was noted that supply chain fraud levels have remained unchanged for the last three years. Some sectors have even reported a decrease in fraud levels, with the technology, media and telecommunications sector reporting a 6% drop over the year 2015-2016.

Whether companies are becoming victims of fraud more than previously is up for debate, however fraud prevention should always be a key consideration of the business.

There are a number of systems and processes available for implementation to offer protection to businesses and reduce the chance of them falling foul to fraudsters. These include:

- ▶ avoid major relationships being owned or controlled by one or two individuals – this is a red flag that is commonly over looked;
- ▶ change key account managers and/or introduce peer review and assessment on key accounts;
- ▶ a culture of challenge – are people in the business able to and do they challenge things that "don't look right";
- ▶ unrealistic targets – some of the largest instances of fraud arise not for personal gain, but in order to achieve targets or objectives that were not realistic and put individuals under personal pressure to deliver the impossible;
- ▶ if you do allow corporate hospitality (and for many organisations it is entirely right to do so) monitor both type and frequency of hospitality closely and have a system to raise red flags;
- ▶ don't ignore the obvious – "we did wonder why he had such a nice car" – is a very obvious but all too common post incident response;
- ▶ have systems to monitor international payments and new supplier companies, especially in emerging or higher risk jurisdictions;
- ▶ do your financial DD on your suppliers; and
- ▶ have a public zero tolerance approach – if the senior management set the tone the business will respond.

If you would like further information on this topic, please contact Mark Molyneux or Nichola Peters.

### Who to contact

**MARK MOLYNEUX**  
Partner, Litigation

0161 934 6872

mark.molyneux@addleshawgoddard.com



**NICHOLA PETERS**  
Partner, Litigation

0207 160 3371

nichola.peters@addleshawgoddard.com

