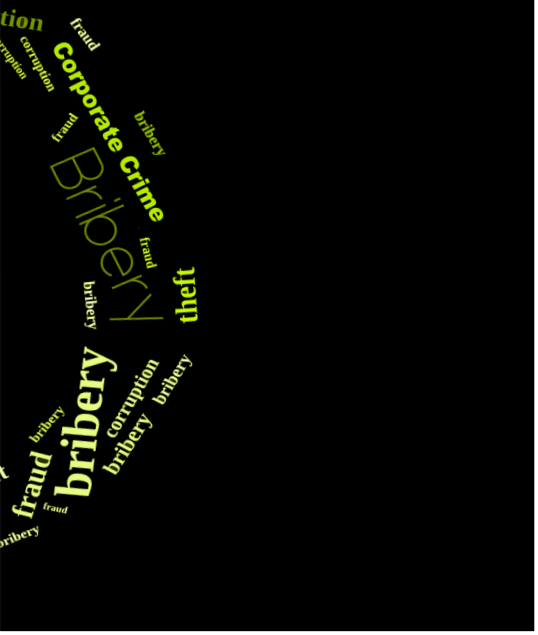

# CORPORATE CRIME

## HOW TO IDENTIFY IT AND WHAT TO DO WHEN YOU DO

In recent years, it has not been unusual to see, on a daily basis, a news report where a business has been either the victim, or the perpetrator, of crime. The financial services, engineering, mining and pharmaceutical sectors have all been the subject of high profile investigations which, in some cases, have resulted in multi-million pound fines. So what are the danger areas, and what should a company do if they suspect criminal activity within their business? We find out from an exclusive article by Christopher David, Counsel at WilmerHale.

Before looking at these potential areas to be aware of, it is important to understand how a company can be guilty of a criminal offence. In general terms, a company is a legal person capable of being prosecuted for most criminal offences. At present, (although reform is currently being considered), corporate criminal liability is based on the identification principle, often called "directing mind" liability. This essentially means that the offence must be attributable to someone who, at the material time, was the 'directing mind and will' of the company. In reality, this means that it will normally only be senior officers of a company at, or close to, board level whose acts can be identified with the company in this way (as opposed to those acting merely as the company's agent). That said, irrespective of the legal position of the company itself, other concerns arise if criminal conduct is confined to junior employees – these concerns include potential linked civil liability and reputational harm and mean that a company should be vigilant for any instances of criminality.

The most common corporate criminal offences which arise are fraud and corruption. Fraud is a broad term which covers any act of deception intended for personal gain or to cause a loss to another party. Common examples include false accounting, insurance fraud, mortgage fraud, Ponzi




schemes, procurement fraud and pyramid schemes. Corruption is an agreement to directly or indirectly give, offer or promise, anything of value to influence someone so as to obtain or retain a business advantage. The UK Bribery Act prohibits the giving and receiving of bribes to both private individuals and public officials and, in addition, the law specifically criminalises a company who fails to prevent a person associated with it bribing someone with the intention of benefiting the company. This means that a company can be liable for the conduct of any third party who acts on their behalf. Third parties include agents, distributors, consultants, resellers and vendors. There is though a complete defence, if the company can show it had in place 'adequate procedures'.

This concept of 'adequate procedures', in addition to providing a legal defence under the Bribery Act, is also the tool by which a company can try and identify criminal conduct. For reasons of space, it is not possible to go into detail with regards to what systems and controls a company should have, but if only one thing is kept in mind it is that there is no point in having in place a complex set of policies and procedures if the end result is that no one from within the business reads or follows them.

Each business will require its own clear and concise set of systems and controls that suit its particular industry and structure but there are two areas on which particular focus should be made – employee expenses and third parties. The reasons for a robust expenses policy are self-evident; this is an area where it is not unusual for employees to attempt to defraud the company, sometimes on a large scale. In addition to sensible oversight over expense claims, a good expenses policy (and associated controls) should ensure that there are suitable checks to identify unusual expense claim patterns which could identify fraud or corruption.

The use of third parties to conduct business or act on behalf of a company is another notorious danger area, not least as a company can be liable under the Bribery Act for the acts of its third parties. It is, therefore, essential that appropriate due diligence is done on all new third parties so as to ensure that the company know who they are dealing with and can rely on them, as far as possible, to act in a legal and ethical manner.

Unfortunately, no matter how robust a company's systems and controls are, it is almost inevitable that at some point, something will go wrong. Once an issue has been discovered, it is vital that a company moves fast to investigate the allegations. It is a common response to want to establish as quickly as possible what has happened, but it is almost always advisable, however, to take a step back and consider carefully the scope of the investigation before beginning the substantive work. This is critical both in relation to deciding the ultimate objectives of the investigation and, in practical terms, how these objectives are going to be achieved.

It is not possible to set out in detail everything that a company should do but on realising that there is an issue requiring an internal investigation, a company should establish internally who is going to be responsible for conducting and/or managing the investigation. This is important for the efficient running of an investigation as well as for creating a legally privileged environment. Whoever is conducting the investigation, whether they are internal or external to the company, should establish the investigations precise scope carefully and clearly at an early stage. An internal investigation is not intended to be a fishing expedition to identify any and all potential problems a company may have, but rather a response to a particular and specific problem that has been identified. This is not to say that unanticipated issues coming to light in the course of the investigation should be ignored, but rather that a precise and focused investigation will undoubtedly be more effective at resolving issues in a time and cost-effective way.

Once an investigation plan has been agreed it is important that a company takes immediate steps to secure all relevant evidence. This should include all relevant electronic data, hard copy documents, and electronic devices. Care should be taken that routine document destruction and electronic deletion programs are stopped. Additionally, all potentially relevant electronic devices such as laptops, phones and hard drives should be secured. Relevant employees should be informed by way of a document hold notice what material should be preserved without giving away details of what the investigation relates to. If necessary a specialist forensic IT team should be brought in to ensure reliable evidential collection, as well as to assist with recovery of deleted data. Once the data has been secured, a careful review of the available evidence should be conducted so as to build up a clear as possible set of facts.

A further issue that should be considered at the outset is the status of any employees that, on the face of it, may be implicated in the conduct under investigation. Normally, the most prudent approach will be to suspend any employees concerned with immediate effect, pending the outcome of the investigation. Once the internal investigation is complete, the decision will have to be made whether to dismiss the employee, reinstate them or extend the period of suspension.

Finally, care should be given as to how any findings are recorded. There is no requirement in English law to report a criminal offence, whether that be an employee or the company itself. A company's decision to self-report should only be done following advice from experienced external counsel as a misstep at this stage could result in serious implications for the company for many years to come. **LM**