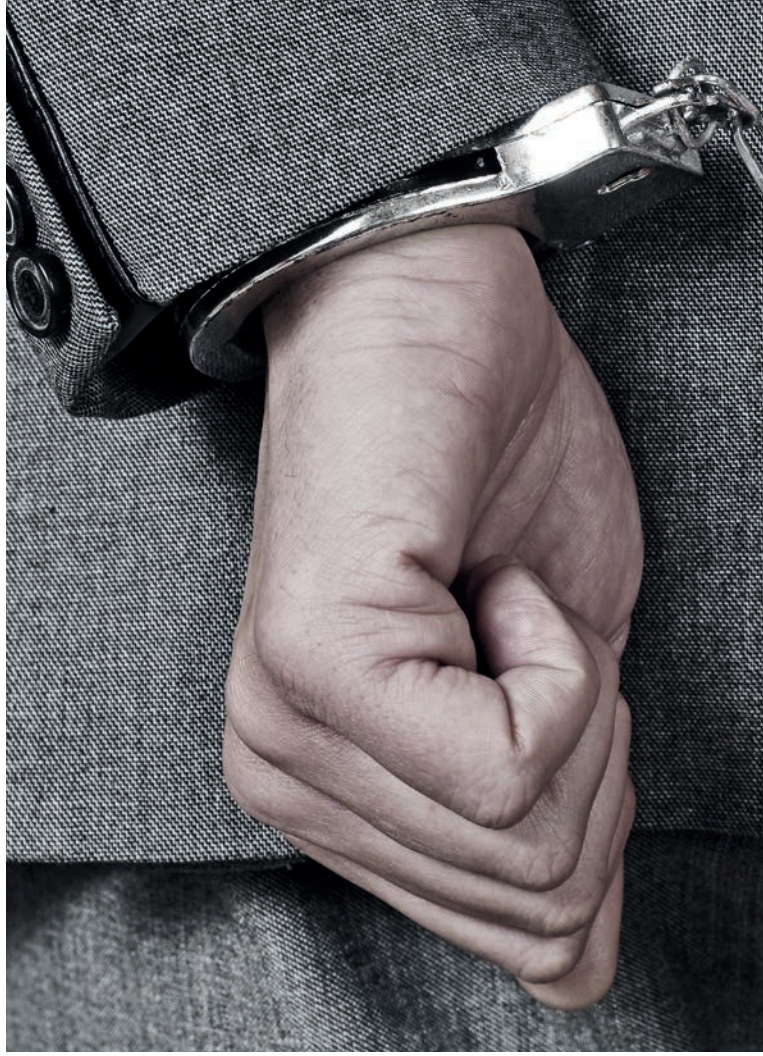
Criminal exposure

Managing and responding to corporate crime risk is no easy task, but a legal and ethical responsibility nonetheless. Christopher David sets out the obligations for treasurers and the parameters for internal investigations



Corporate crime is a current hot topic: financial services, sport, defence, mining, engineering and the pharmaceutical sectors have all been the subject of high-profile and very public investigations, which, in some cases, have resulted in multimillion-pound fines. In a number of these cases, the conduct could potentially have been identified and stopped by a company's treasury function. This is not to say it is easy to identify and stop conduct of this nature – businesses are complicated and it is impossible to second-guess decisions by senior executives or rogue employees, but being alert to potential red flags in relation to fraud and corruption can go some way to protecting a company. Additionally, if illegal or suspected illegal conduct is discovered, then it is vital that a company takes considered and appropriate steps to investigate it.

Fraud and corruption convictions carry significant fines for the companies – and prison sentences for the relevant individuals – and would be a breach of the ACT's Ethical Code.

Looking for warning signs

Each business will require its own clear and, preferably, concise set of systems and controls that suits its particular industry and structure, but, from a treasury point of view, two key areas to focus on are M&As and capital expenditure. On a relatively simplistic level, these areas are where there are significant outflows of company funds and therefore carry the risk of misuse or misappropriation, but also are occasions where a treasurer may have an opportunity to spot potential red flags.

Obviously, a large part of this responsibility falls to the legal and/or compliance function, but it is worth being aware of the more common potential red flags. On a simple level, extra care should be taken if the transaction or the third party is in a country known for widespread corruption, as measured by the Transparency International Corruption Perceptions Index. Reputational checks should be carried out on all third parties and any suggestion of a poor business reputation should be investigated thoroughly. Any link that a third party, to whom a payment is being made, has with a government official should be treated with extreme caution. This includes taking steps to identify beneficial owners of shell companies. Finally, care should be taken if any party, internal or external, requests approval of a significantly excessive budget or unusual expenditures.

From a treasury point of view, extra care should be taken in relation to payment instructions that fall just below delegated approval limits or are brought within this limit shortly before completion of a transaction. Unusually large requests for funds for capital expenditure from overseas subsidiaries should also be carefully reviewed and considered before any funds are made available.

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 a possible issue has been discovered, it is vital that a company moves quickly 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 any 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.

Taking action

An internal investigation can be complex and long, and it is not possible, for reasons of space, to set out in detail everything that a company should do. However, the first thing a company should do

SHUTTERSTOCK

on realising that there is an issue requiring an internal investigation is to establish internally who is going to be responsible for conducting and/or managing the investigation. This person or group should have sufficient authority to issue instructions on behalf of the company, as well as obtain relevant documents and material. This is important for the efficient running of an investigation as well as for creating a legally privileged environment.

The **ACT** Ethical Code can be found at: www.treasurers.org/ACTmedia/ethical_code1.pdf

Whoever is conducting the investigation, whether they are internal or external to the company, should establish the investigation's 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.

Securing the evidence

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 set of facts that's as clear as possible.

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.

POTENTIAL FOR EXPOSURE

The most common corporate criminal offences that arise are fraud, money laundering 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.
- **MONEY LAUNDERING** is essentially the processing and handling of criminal property, including money derived from criminal conduct, and disguising it so it looks like it has come from legitimate sources.
- **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 that 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 that acts on its behalf. Third parties include agents, distributors, consultants, resellers and vendors. There is, however, 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.

Christopher David is counsel at WilmerHale