

Gathering the Evidence – Following the Money

Dan Morrison and Ben Gallagher

Dan Morrison is a Partner in Litigation and a member of the Corporate Investigations and Asset Recovery Group at Mishcon de Reya. Dan is an expert on the law relating to covert investigations and the recovery of stolen assets, including confidential information, business data and trade secrets.

Ben Gallagher a Solicitor in Litigation at Mishcon de Reya. Ben is a specialist in claimant fraud investigations and also deals with electronic fraud, contentious IP and counterfeiting matters, particularly in relation to computer software.

Abstract

The first few hours of an investigation can secure critical evidence and set the tone for everything that follows. This article examines the investigative and legal options available in the early phases of dealing with fraud, including how to use disclosure orders against banks in order to trace the proceeds of a fraud, and how to make the best use of freezing orders against fraudsters. The authors explain the critical issue of following the money, without which any investigation and legal action will achieve no more than a mere understanding of how the victim was defrauded.

Future articles by Dan Morrison and Ben Gallagher will look further into other legal options for investigation (such as Search Orders – the civil law equivalent of a police search warrant) as well as the legal process involved in actually recovering the money once it has been found.

Imagine the scenario:

You are the Chief Financial Officer of a major company. A senior manager (“Mr X”) from the procurement division is currently on holiday and a colleague who has been covering his work brings disturbing news to you. The stand-in was uncertain of the legal position and has not dug too deeply so far, but believes the company may have seriously overpaid a supplier for raw materials and that Mr X has received kickbacks in return for placing orders with that supplier. The stand-in became suspicious after a phone call with the supplier in which the “usual deal” was mentioned together with vague references to an account in the Isle of Man. The stand-in has checked and the company has no bank accounts in the Isle of Man.

While the particular set of “facts” in the scenario above hints at bribery and corrupt practices, the principles of investigation and recovery will remain essentially the same whether the underlying fraud relates to corruption, embezzlement or even the “mere” theft of confidential corporate information. Likewise, the principles hold true whether the corporate “victim” is a bank, a manufacturer or a supplier of services.

To investigate or not?

The first point to note is that if ever there was a time when such matters could have been swept under the carpet, such practices are no longer viable. The law (in particular the duties imposed on company directors), regulators and general shareholder expectations increasingly call for investigation of fraud and action to remedy losses suffered. In America (always a trend-setter for litigation) there has been significant growth in class action litigation by shareholders against executives who have failed to investigate fraud.

In addition, even if no recovery from the fraudster is contemplated (a very modest position from which to begin), regulators and insurers will demand investigation if only to identify and eliminate weaknesses in systems and policies.

Getting started

The first few hours of an investigation can secure critical evidence and set the tone for everything that follows. Knowing how to proceed from the outset rather than playing catch-up can make the difference between a successful and a disastrous investigation. Having a Fraud Response Plan (together with a designated "point man" with the necessary delegated powers) in place is invaluable. If you don't already have a Fraud Plan, the most important thing you should take from this article is the value of putting one in place so that the "headless chicken" effect can be avoided.

A great deal of information can be waiting to be found internally. Data Protection Act 1998 concerns fall away in this context as the legislation expressly provides for exceptions where data processing takes place in the course of preventing and detecting crime (and almost every imaginable fraud will also amount to a criminal act or acts).

One promising source of information will be the emails passing between Mr X and the customer. You will be able to access and review these emails provided you own the computers in question (usually the case), as this will avoid any liability under the Computer Misuse Act 1990. You must also have taken reasonable steps to make staff aware that their emails and computer use may be monitored. This can be done by way of disseminating an email "policy" direct to staff, through an office manual or in employment contracts themselves and will allow you to avoid liability under the Regulation of Investigatory Powers Act 2000 which governs the interception of communications.

Fraudsters are often careless with what they say in emails, but not surprisingly, you would have to be lucky to find damning information in a saved email. A far more likely source of evidence will be deleted data. These days "deleting" really doesn't mean deleting. Huge amounts of data can be recovered which the fraudster thought to have been safely disposed of. The very fact that a supposed ability to "delete" exists is a significant factor in the carelessness with which people word emails.

You can also check the call logs for Mr X's phone (and for his mobile, if it was provided by the company). If you do not have the capability internally, outside investigators will be able to determine the ownership of dialled numbers. Where suspicious financial dealings are suspected merely knowing that the area code for the Isle of Man is 01624 can be of great assistance. Likewise the codes for other offshore banking centres. In the context of the scenario given above, it would be extremely useful to know that Mr X had called numbers in the Isle of Man as it would take very little effort from that point to identify whether any of those numbers were used by banks.

Where ongoing investigative methods are required such as future monitoring of a suspect's emails or even the direct monitoring of his telephone calls, these methods will also be legal provided you own the telecommunications system in question (i.e. the internal phones and computer equipment) and all reasonable steps have been taken to make employees aware that monitoring may occur.

Just gathering the internal information described above may yield substantial evidence and leads. External investigation firms can be brought in to do further work where necessary, including surveillance in appropriate circumstances. External Investigators are also especially useful for asset investigations. It will obviously be important to know that your suspect has sufficient assets within legal reach to justify the cost of the legal proceedings necessary to make the recovery. In some cases the money will already have been spent but (as will be examined in a separate article) this can actually be advantageous – where the proceeds of fraud are used to acquire an appreciating asset not only is your original loss recoverable, but also the fraudster's profit on his "investment" of the proceeds.

Given that there are a number of legal pitfalls to be avoided during the course of investigations (as can be seen from the legislation referred to above), it is important to involve in-house or external legal advisers from the outset. The use of lawyers also preserves privilege in documents created during the course of the investigation; failing to maintain privilege may result in a loss of control over what documentation must subsequently be disclosed in any legal proceedings resulting from the findings of the investigation. Once the information is in from the internal and/or external investigative efforts, legal options come fully into play. Of principle interest for the purposes of this article are Disclosure Orders against banks which may unwittingly be holding the proceeds of the fraud, and Freezing Orders to secure assets for your eventual recovery.

Disclosure Orders

When you identify a bank to which the proceeds of a fraud may have been channelled you will often not want to jump straight in with a Freezing Order. Service of that Order will alert the target to the investigation and monies may have already moved away from the bank you have identified. The monies will generally remain in the original account in only the least sophisticated frauds. For one thing, money sat offshore will be of little benefit to the fraudster who wants to spend his ill gotten gains at home.

A useful first step is to obtain Disclosure Orders against the banks involved. In order to obtain the Order, you must be able to persuade the Court that wrongdoing has occurred and that the bank is likely to hold information relating to the commission of the fraud and the whereabouts of the proceeds. The bank, of course, is likely to have played an entirely innocent role but this is no bar to obtaining the Disclosure Order. The bank's likely innocence is reflected in the usual costs order, i.e. that you will pay the bank's costs of complying with the order to disclose account information.

Banks have separate and well-defined duties to their customers. In order to avoid the risk that bank employees will give the game away by alerting the customer (even if only accidentally in response to a customer enquiry), the Disclosure Order should be combined with a Gaggling Order. This will prevent the bank from revealing the existence of the Disclosure Order to its customer for a specified period of time, giving you the opportunity to examine the disclosed documents and follow the money through subsequent transfers to other banks. The process can be repeated as necessary in order to gain comfort as to the current whereabouts of the money and make the use of a Freezing Order far more effective.

Freezing Orders

Having established the location of funds you will want to secure them. The Freezing Order serves two main purposes. First, it protects the assets from dissipation while legal proceedings move towards judgment. Secondly, the very fact that you have obtained a Freezing Order demonstrates the strength of your case and allows you to exert a degree of economic pressure on the suspect that dramatically improves the prospects of an early settlement on favourable terms.

To obtain a Freezing Order it will be necessary, in summary, to persuade the court that:

1. Your case is a strong one (i.e. you will present the results of the investigation into the what, the how, and the amount of the fraud).
2. You have suffered serious damage.
3. There is a "risk of dissipation" (i.e. that the suspect is likely to hide the proceeds of the fraud or move them beyond the enforcement jurisdiction of the courts in England and Wales, and other "friendly" jurisdictions).
4. The protection provided for you by the Freezing Order will not be

disproportionately outweighed by the damage it will do to the target (i.e. by preventing him from dealing with "his" assets).

Conclusion

In future articles, we will look further into other legal options for investigation (such as Search Orders – the civil law equivalent of a police search warrant) as well as the legal process involved in actually recovering the money once it has been found (sometimes even recovering more money than has been lost). The methods described above, however, play a critical early role in gathering the initial evidence and following through on it to identify assets and ensure that the subsequent legal proceedings will amount to more than a merely academic post-mortem of what went wrong. Above all, the key to successful investigation is an awareness of the available options as well as the co-ordination that leads to a rapid and efficient investigation. Having a Fraud Response Plan in place and modifying it over time to bring in the improvements suggested by practical experience in investigations will allow you to both make the most of the opportunities considered above and also to satisfy insurers and regulators that effective systems are in place in your organisation.