

# Data fraud in hedge funds

Paul Jacobs/Andy Harbison  
Originally published in HFM week

It is an unfortunate fact of life that when economic times are tough, fraud investigators become busy. At Grant Thornton we have noticed that while the general tempo of economic activity has slowed, our Forensics functions have been receiving more and more request for help. This includes my area, IT Forensics.

I spend a lot of time helping companies develop their incident response plans for dealing with internal frauds and teaching business people how to react effectively to fraud events. I have long since stopped talking about “Computer fraud”, however. This is not because computer fraud is uncommon, but conversely because it is all-pervasive. Nowadays if fraudsters are not using computers to carry out their schemes they should really consider another occupation.

Before I continue I should quickly define what I mean by “fraud” – it is a rather inexact term covering a lot of different offences. To us, to carry out a fraud is “To obtain money, property or information, to gain an advantage of value, or to cause a financial loss without the consent or authorisation of the rightful owner.”

This is a fairly general definition, and covers a large number of computer based activities that one would not necessarily consider immediately to be fraudulent. You might expect, for example, that most frauds would involve the theft of money. However, at Grant Thornton we expect to see as many information theft cases as we do financial frauds. Just about anything that you can store on a computer we have seen stolen at some time or other. Customer databases, marketing plans, software source code, pricing models, research material, price lists, personnel records, and many other types of data.

Information, you see, is potentially even more valuable than cash, and is a great deal easier to steal and transport. Just as importantly to data thieves, is that it is much more difficult to detect an information theft than a financial one, and once detected it is much more complicated to value the stolen material (the value of information quickly diminishes over time), making prosecution less likely.

Hedge funds seem to be particularly prone to this kind of problem – after all it is an industry where considerable reliance is placed on up-to-date information. It is also an industry where there is a lot of movement of personnel between companies, and most information thefts seem to occur when individuals are leaving one company and joining another. During the last period of stock market chaos, the deflation of the Dot-Com bubble, we saw a lot of IP theft from hedge funds and related institutions.

Another form of data fraud of which we saw much during the last downturn involved the forgery of contract and other documents. For example, as shares began to fall, three of our clients were approached by investors brandishing side letters to their contracts, typically allowing participants in hedge funds to remove their funds without loss. Of course any such document is highly suspicious, but it is not unknown for some hedge fund managers to set up side agreements in order to entice major investors into their funds at start-up. This means that all had to be investigated.

Fortunately, in the modern world almost all documents are prepared on computer. It is the nature of computers that, because they are designed to store data quickly and reliably, they are conversely very inefficient at deleting it once it is no longer required. Just because a document is deleted doesn't mean that it is gone for good. Additionally, any document prepared on a computer will leave a substantial trail of data from which it is possible to deduce much about its creation, storage and use.

In the side letter cases we were able to quickly determine when, where and by whom each document was created. Microsoft Word documents contain large amounts of hidden data which can tell us all this information, as well as the names and locations of all previous edits, and often material that has been deleted from the document prior to release. This allowed us to develop full "histories" for each of the questionable documents.

Just as importantly, analysis of the computers on which the documents were first written also gave us the context in which the documents had been written. In one case we found that the manager of the hedge fund was intending to defect to another company and had fabricated the side letter in an (unsuccessful) attempt to bring one of his major clients with him. We were able to do this by recovering the individual's web-mail messages. Most people do not realise that just about anything you look at using your web-browser is stored for a time on the computer's hard drive – including web-mails. We can use information like this (preserved Google searches are particularly useful) to work out what a suspect was planning long after events have come to light.

In another case, however, the side letter appeared to be genuine. It was prepared by the manager at the inception of the fund, completely without authorisation by his company, to attract two major banks to participate. In this case we at least were able to demonstrate from recovered e-mails and other communications that the letter was prepared without authorisation, which at least gave our client some legal standing in the dispute.

The same principles apply to all other fraud investigations. You might be surprised just how many fraudsters use "Google" to help them plan their crimes. In many cases we can map out the entire path of a fraud, from inception, to planning, to implementation, to dispersal of funds, all through computer analysis.

So how do you deal with this problem? I am afraid that I would need a lot more space to answer that question than I have here, but there are a few general principles that can help:

- first, operate a policy of “least privilege” – Don’t let people have access to data they don’t need. What they don’t have they can’t steal.
- don’t let any computer or other storage device on your computer network you do not own. If people steal information onto their own equipment (computers, USB pens or anything else) it is a lot more difficult to get it back than if it is copied onto your own hardware.
- if anyone leaves your employment suddenly, or for a competitor, or under a cloud, or if they had access to critical information, it is worthwhile checking for information theft.
- if you suspect something, follow it up. Most IT Forensics investigators will act discreetly, and (just as important) inexpensively. If necessary they can take a copy of a computer at night, without anyone else knowing it has been done. This will allow you to determine the truth, or otherwise, of your suspicions without causing any undue fuss.
- don’t try to analyse computer evidence yourself. Computer evidence is ephemeral, and there are complex legal rules governing how it must be handled. It is very easy through mishandling to turn crucial evidence into interesting but legally worthless data. Phone a specialist.

### Contact

#### **Paul Jacobs**

Partner, Forensic & Investigation Services  
D +353 (0)1 6805 835  
E paul.jacobs@grantthornton.ie

#### **Andrew Harbison**

Director, IT Forensics & Investigation Services  
D +353 (0)1 6805 766  
M +353 (0)86 040 7211  
E andrew.harbison@grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should always be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

