IT & Fraud: The Golden Hour

David Ingram and Carmel King list the important steps to take at the very beginning of a case where there is a suspicion of fraud and dishonesty of the directors

DAVID INGRAM
Insolvency practitioner,
Grant Thornton UK LLP, London

CARMEL KING
Advisory,
Grant Thornton UK LLP, London

Share your views!

The "golden hour" is that brief period of time following a serious accident in which the outcome for a victim of that accident will depend on what happens in that first hour. Likewise, the first actions taken by a liquidator can dictate the outcome of the case.

This article is written from the viewpoint of a provisional liquidator - a liquidator appointed by the Court on a 'without notice application' - and in the context of English insolvency law. The appointment of a provisional liquidator is reserved for the extreme cases, typically where fraud is suspected and there is a real risk of dissipation of assets or, as examined here, the risk that the company's records may go missing.

Having secured the appropriate Court Orders, it will be necessary to serve the Orders on the company and its directors. It is vital that, from the start, the practitioner takes every possible step to reduce the risk of further dissipation of company property, including its books and records, and sets himself up to conduct a meaningful investigation that will result in the recovery of misappropriated assets.

I would advocate a three-stage approach:

- *information gathering,*
- *developing a strategy based upon information gathered, and*
- *the implementation of that strategy.*

This approach ensures that commercially viable cases are conducted in a controlled manner, progress steadily and produce the best outcome for creditors.

Phase 1: Information gathering

I hope to consider phases 2 (developing a strategy) and 3 (strategy implementation) in future articles, in order to give adequate consideration to each. Phase 1 involves identifying, securing and collecting available evidence in a manner which ensures that it is safely preserved for analysis and future use.

The sheer volume of electronic data in the majority of companies is today significantly higher than the information committed to paper. Information Technology ("**IT**") has a crucial role at the outset of a case: it can be of vital assistance to the practitioner, but without appropriate support from an IT professional, it can also represent a significant risk. IT has the potential to contribute hugely to a long-term case strategy involving investigation, litigation and the recovery of assets for the benefit of creditors.

"The Knock"

A provisional liquidation usually involves visiting a company's trading address without notice, or on very short notice, to the directors and employees. In these circumstances, the practitioner needs to secure the site as quickly as possible, having engaged a suitably qualified digital forensic team to accompany him.

Opportunistic fraudsters can interfere with the process in any number of ways: computers and related technologies are integral tools in the conduct of fraud. Funds can be transferred, correspondence and documents can be deleted, altered or stolen, even when the practitioner is in the room.

The practitioner should immediately remove all suspects, witnesses and bystanders from the proximity of digital evidence. The practitioner needs to ensure that the Court Order provides appropriate powers. He is likely to have the authority to seize certain items these individuals may hold, including company mobile phones, USB memory drives, tablets, credit or debit cards, security swipe cards and SD (secure digital) cards. It can be tempting for disgruntled employees to try to keep small, high-value electronic items, or those which they think will grant them access to the company records at a later time.

It may be necessary to obtain authority to seize or gain access to additional evidence, for example where directors have access to the company's online banking facilities through apps installed on personal phones or tablets. I am reminded of a case where one of my partners attended the company's trading address with a digital forensic team. The director, at one stage, excused himself to use the lavatory. A few moments later, the digital forensic expert raised the alert. The director was remotely deleting company electronic data using a tablet, from the lavatory. Within seconds, the lavatory door had to be forced, and the tablet taken from the director.

Practitioners should obtain information about the systems used from employees, IT staff and the directors. Passwords, usernames, email addresses used and details of the various operating systems are very

> THE 'GOLDEN HOUR' IS THAT BRIEF PERIOD OF TIME FOLLOWING A SERIOUS ACCIDENT IN WHICH THE OUTCOME FOR A VICTIM OF THAT ACCIDENT WILL DEPEND ON WHAT HAPPENS IN THAT FIRST HOUR

valuable. I understand that Apple products, such as iPhones and iPads are notoriously difficult for forensic technicians to "crack" when the password is unknown, and Blackberry devices are not far behind. This article is not sponsored by either brand – I hope readers will take it as a warning not to get locked out of valuable sources of information!

External threats

At the same time as mitigating the on-site security risks posed by employees, directors and third parties, the practitioner should pay attention to the threats that exist off-site. Are the premises remotely monitored by CCTV, and if so, who has access to this system? Usernames and passwords should be changed as soon as possible, as should access codes for online banking. Cloud computing service providers and other third party IT providers should be notified of the practitioner's appointment as soon as possible, to restrict access to the practitioner alone, and ensure the continuity of service where required. Are the computers networked? Steps must be taken to isolate individual stations and any servers, preventing remote access. However, when doing this, special attention must be given to preserving the integrity of these items for later interrogation and use as evidence in recovery proceedings.

The practitioner's own communication needs whilst on-site should be considered. It is not a great idea to use the company's WiFi or network facilities if they might be vulnerable, as this could result in the practitioner's own system being compromised.

> READERS OF THE NSA AND GCHQ SURVEILLANCE STORIES WILL BE UNSURPRISED TO LEARN THAT EVERYTHING WE DO ON A COMPUTER IS RECORDED

Identifying the evidence

The practitioner is required to take all possible steps to preserve the chain of evidence, if the materials he uncovers are to be used as evidence in future litigation. This includes eliminating any potential defence that the evidence has been tampered with or damaged by the practitioner, or erroneously attributed to the fraudster we are pursuing. The practitioner can do this by taking photographs of the equipment to be seized *in situ*, documenting the condition and any pre-existing damage, identifying any connected external components, and noting the relevant serial numbers.

When identifying items to be seized, have a good look around. Back-up tapes are easily overlooked. How many of us keep important passwords written on post-it notes on desks or in drawers? A quick online search for "novelty USB memory drives" shows that they come in every shape imaginable, from model cars to Lego bricks, animals and disturbingly lifelike parts of human anatomy!

Securing the evidence

If the practitioner has instructed a suitably qualified digital forensics team to attend the company premises with him during his initial attendance on site, they can carry out the initial assessment, documentation and labelling of the evidence to be uplifted. In many cases, they can take images of the machines on-site. More complex exercises may require that the equipment be taken back to the lab. A good digital forensics team will have a lab that is temperature controlled and can be locked – the practitioner will not want to pay to have someone supervise an automated imaging process that may take several days and nights in order to preserve the integrity of the evidence!

In situations where costs or other factors prohibit the attendance of a digital forensics team at the company premises at the outset, there are a number of steps that the practitioner can take to collect evidence safely and take it to the lab for imaging. If a computer is turned off, do not turn it on. Similarly, if the computer is turned on, switch it off rather than following the usual shut down procedures, in order to retain the record of the user's most recent shut down.

Disconnect all power sources and remove batteries from laptops. Servers can be more problematic, and it will be worth seeking guidance. They may hold volatile data that should be captured in advance of a shut down. Pulling the plug could severely damage the system – crucial evidence could be lost or corrupted. As well as this, the practitioner's credibility and the reliability of other evidence may be left open to question during litigation.

Collecting the evidence

A digital forensics team will have the expertise to retrieve and present data securely, for use in investigating the conduct of suspected fraudsters and use in subsequent asset recovery litigation. However, the practitioner has knowledge of the case, the players, the circumstances and the end goal. This stage requires both to work closely together. The practitioner must have an understanding of the powerful tools available to the digital forensics team. The forensics side will require guidance to efficiently analyse large amounts of data, targeting the most useful evidence in a cost-effective manner.

A digital forensics team can perform miracles that were not available to practitioners until relatively recently. Keyword searches can be carried out across terabytes of information in different formats including emails, spread-sheets, instant-messaging records, text documents and online activity.

Readers of the NSA and GCHQ surveillance stories will be unsurprised to learn that everything we do on a computer is recorded. It is not difficult to identify when files were created, accessed, printed, altered or deleted, and by whom. Files that have been hidden, password-protected or encrypted are all recoverable. Most emails contain

sufficient data to identify the location of the sender.

Smartphones and some cameras store a user's GPS coordinates, so we can tell whether the dodgy director was where he claimed to be when making that call, or sending that text or email.

Deleted does not mean unrecoverable: an expert team can restore recently deleted files. This extends to a user's internet history, mobile phone call logs, SMS and MMS messages, photos and emails. A suspected fraudster may have been sufficiently cautious to delete incriminating emails from his laptop, but it's possible that he considers his smartphone is a safe location to store his records.

In a very real way, then, the IT records of a company are more likely to reveal evidence of fraud than paper records, when a forensic analysis is employed.

Conclusion

Although this article emphasises heavily the significance of electronic records in all shapes and forms, we should not ignore paper records. On one occasion, having that morning been appointed provisional liquidator of a company, I sat at the director's desk while the digital forensics team went about their work. Shuffling through the documents in the director's in-tray, I came across a draft will which made reference to a Mauritian Trust. Being asset rich, the Trust was most interesting to me, and proved to be a significant element in my investigation and realisation of misappropriated funds.

There are plenty of opportunities for the practitioner to trip up in his efforts to safely identify, secure and collect evidence for use in insolvency cases where fraud is suspected. It's a tough slog, I won't lie. Like many areas of insolvency, it might read like James Bond on paper, but in reality it can involve wading through vast amounts of electronic junk that was deleted for a reason, and emails that frankly constitute an assault on the English language. But it's worth it.

So much more information is stored electronically than on paper, information that is harder to hide, deny or destroy. By taking the correct initial steps during the 'golden hour' to safely secure the company's electronic records, the practitioner gives himself the best possible chance of developing and implementing a decent strategy, enabling him to conduct a successful investigation, pursue fraudsters and recover company property for the benefit of creditors. ■

IN REALITY IT CAN INVOLVE WADING THROUGH VAST AMOUNTS OF ELECTRONIC JUNK THAT WAS DELETED FOR A REASON