Young Fraud Lawyers Association

Dear All,

Welcome to the YFLA Winter Newsletter 2019, sponsored by Colley Intelligence. Details of our upcoming events can be found on our website (**www.yfla.com**) and on our LinkedIn group (search for "**Young Fraud Lawyers Association**"). We hope you enjoy the Newsletter and take this opportunity to wish all YFLA members a happy, healthy and prosperous 2020.

In this issue:

De-banking: what's the appeal?

The announcement that permission to appeal has been granted in the case of *N v Royal Bank of Scotland PLC* [2019] EWHC 1770 (Comm) might offer a ray of hope to companies and individuals whose banking facilities have been frozen or terminated because of suspicions held by the bank that the accounts were being used for fraud and money laundering.

Background

By way of a reminder about the background to the initial decision, the Claimant ("N") provides foreign exchange and payment services to its customers. N held approximately 60 active accounts with the Defendant bank ("RBS"). These comprised four main accounts and separate client sub-accounts in various currencies.

A key clause in the terms governing the contractual relationship provided that RBS give not less than 60 days' written notice to close an account, unless it considers there are "exceptional circumstances".

RBS froze ten of N's sub-accounts which it suspected were being used for fraud or to hold the proceeds of crime. Following this, an attempt was made to make a payment of £500,000 through one of the main accounts "in an apparent effort to circumvent the freeze on the frozen sub-accounts".

RBS's investigations showed that there had been a mixing of funds between the suspect sub-accounts and N's main accounts and consequently RBS took the decision to freeze the main accounts and terminate the customer relationship with immediate effect.
N commenced proceedings challenging the lawfulness of that action on the part of RBS.

The High Court proceedings

In the course of the High Court proceedings, N argued that there were several other avenues RBS could have pursued without having to terminate the contact with immediate effect, for example, ring-fencing the suspect funds or preventing further credits to the account (to avoid further evasion of the freeze).

The Court rejected all of the arguments put forward, largely on the basis that the level of justified concern was at much too high a level for any of the alternatives to be reasonably pursued. The £500,000 attempted payment was evidence of the actions which N and its clients appeared willing to take in order to circumvent the bank's initial freeze and a measure of the seriousness of the situation.

Outcome

The Court found that RBS had been entitled to terminate its relationship with N without notice. It considered that RBS had:

1. Investigated the issue of mixed funds and rightly taken it into account when deciding to terminate the banking facilities;

2. Taken account and properly weighed up the potential risks to N's business; and

3. Considered, rationally and in good faith, that there had been exceptional circumstances for closing the accounts without notice.

The Court concluded that, whilst RBS's decision to terminate the relationship without notice had major consequences for N, it was nevertheless the proper response and one that RBS was entitled to take in the circumstances.

Impact

The initial decision will have been welcomed by banks facing increasing pressures when it comes to anti-fraud and money laundering protection in the financial industry. The judgment empowers financial institutions to take matters into their own hands and not to rely on law enforcement to take action (for example, refusing consent in response to a SAR or in the form of Account Freezing Orders and the like).

However, whilst the Court did find in favour of RBS, the fact is that cases such as this will always need to be considered on their specific facts. It should also be remembered that RBS did take intermediary steps prior to terminating the relationship, such as freezing the sub-accounts, and the decision itself came after careful consideration by RBS's director of financial crime and group money laundering reporting officer in consultation with others.

Most banking contracts will include a clause allowing the bank to immediately terminate the banking relationship in exceptional circumstances. Businesses wanting to avoid such a clause being exercised should take reasonable steps to ensure that they undertake adequate on-boarding, due diligence and KYC checks in order to ensure that they manage money laundering risk their end. In the meantime, watch this space for a Court of Appeal decision which might provide some more general guidance for parties facing frozen accounts and terminated banking facilities.

Katie Allard
Kingsley Napley LLP

Overseas Production Orders and the Future of Electronic Evidence

In complex criminal investigations, there will invariably be electronic material that is held overseas and which law enforcement authorities will wish to access. Until recently, the only way to obtain access to such material was to rely upon Mutual Legal Assistance ("MLA"). The MLA process is infamous, however, for being cumbersome and slow. As a consequence, there have been efforts to circumvent MLA and to enable law enforcement authorities to obtain direct access to information that is held overseas. For example, in *R (on the application of KBR Inc) v Serious Fraud Office* [2018] EWHC 2368 (Admin) the Divisional Court held that section 2(3) of the Criminal Justice Act 1987 has extraterritorial reach. In the case of foreign companies and documents held abroad, this is limited to companies with a sufficient connection to the UK. The consequence of this judgment is to obviate the need, in some cases, for the Serious Fraud Office ("SFO") to rely upon MLA. Leave to appeal to the Supreme Court has been granted and it remains to be seen whether the Divisional Court's construction of the 1987 Act is upheld.

Even if the Supreme Court were ultimately to overturn the Divisional Court's judgment, there is a new tool in the SFO's armoury that will negate the need to rely exclusively upon MLA. The Crime (Overseas) Production Order Act ("the Act") was granted Royal Assent on 12 February 2019. The Act permits an appropriate officer to apply to a Crown Court judge for an overseas production order. Such an order requires a person based overseas to produce or give access to electronic data, regardless of where it is stored. There are safeguards for material that is protected by legal professional privilege, or which constitute confidential personal records.

The following requirements must be satisfied before an overseas production order can be made:

1. the person against whom the order is sought operates or is based in a country outside the UK which is party to, or participates in, a "designated international co-operation arrangement";

2. an investigation has been instituted or proceedings commenced in respect of an indictable offence, or the order is sought for the purposes of a terrorist investigation;

3. the person against whom the order is sought has possession or control of all or part of the electronic data;

4. all or part of the electronic data is likely to be of substantial value to the investigation or proceedings;

5. all or part of the electronic data is likely to be relevant evidence in respect of the offence; and

6. it is in the interests of justice for all or part of the electronic data to be produced.

Once granted, the person upon whom the overseas production order is served must produce or give access to the data specified in the order in a form in which it can be taken away and in which it is visible and legible. The requirement to produce or give access to the data applies regardless of where the data is stored. The consequences of failing to comply with the order are not clear on the face of the Act, but presumably would constitute contempt of court.

Overseas production orders can only be obtained if the information is held in a country with whom the UK has entered into a designated international co-operation agreement. Such an agreement – the US-UK Bilateral Data Access Agreement – was signed by the Home Secretary and the US Attorney General on 4 October 2019. As a result, it will not be long before white collar crime practitioners are receiving enquiries from their clients about how to respond to overseas production orders.

Karl Laird
6KBW College Hill

When is theft not theft? The legal status of stealing information

I admit, this sounds like a bad riddle from an underwhelming Christmas cracker. However, it is also a question an increasing number of firms find they need to ask and many are surprised and disappointed by the answer.

Young Fraud Lawyers Association

Many companies rely on highly confidential information for the success of their businesses. On occasion, a disgruntled (or opportunistic) employee may seek to take improper advantage of access they have to this confidential information and procure it for themselves to leverage for personal gain.

A common response for victims of this behaviour is to consider seeking criminal justice. After all, they have been the victim of a theft, haven't they?

The Law – Theft Act 1968

The basic definition of theft is set out in section 1(1) of the Theft Act 1968 (the "**TA 68**"). As will be familiar to all, a person must dishonestly appropriate *property* in order to commit Theft. The definition of "property" in s4(1) TA 68 includes "*intangible property*".

A simple reading of "intangible property" suggests that it includes confidential information. On its face, therefore, someone who accesses information on a computer and takes it for personal gain could be accused of theft.

Oxford v Moss (1979) 68 Cr App R 183

However, the 1978 case of *Oxford v Moss* makes clear that confidential information does not fall within the definition of "intangible property". In that case, a student dishonestly obtained a copy of an upcoming exam paper, read its contents and returned the paper. He was charged with theft of confidential information but was not convicted, because information is not "property".

Despite being heard over 40 years ago, *Oxford v Moss* remains good authority and creates the curious legal result that an individual can "steal" information without committing theft. In the modern day, with the proliferation of information that is readily accessible, the ruling in *Oxford v Moss* and the relevant legislation can appear increasingly unfit for purpose.

If an individual downloaded copies of documents onto a USB stick, or forwarded themselves copies of documents via email, it could be argued the copies of those documents had been "stolen", because the computer files themselves will have been transferred. However, if an individual simply reads and learns information or takes notes of it, but does not remove the original document itself (whether that document is on a computer or in hard copy) they will not have committed theft. To compound the issue, the response from the police (even when actual documents and client lists have been printed off and taken) is often respond that this is a civil matter.

There are an increasing number of examples of rogue employees taking valuable confidential information from companies. Understandably, this is a practice that firms wish to create a deterrent against and in many cases will seek criminal justice for when they are the victims of it.

Computer Misuse Act 1990

Ironically, one of the best solutions to this outdated legislative position and case law is another piece of arguably outdated and little-known legislation: Section 1(1) of Computer Misuse Act 1990 (the "**CMA**"), which states that:

(1) A person is guilty of an offence if –

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

A person guilty of an offence under s1 CMA can be sentenced to imprisonment for a term not exceeding twelve months on summary conviction, or imprisonment for a term not exceeding two years or to a fine or to both, if convicted on indictment.

There are, of course, a host of civil remedies that might be considered in priority to criminal charges under the CMA. However, if a firm wishes to highlight the potential criminal liability of individuals in order to emphasise the seriousness of their situation and to bring them to the table, the CMA can offer a viable option.

Conclusion

As we approach 2020, it appears increasingly important for the UK to pass legislation to protect companies against abuses that the proliferation of information and documents on computers increasingly allows for. However, this is not immediately in prospect and neither is an overturning of the decision in *Oxford v Moss*.

Until such time as either of those positions change, parties that wish to seek criminal justice for the "theft" of information stored on computers may be better served by considering the CMA, rather than allegations of theft, however counterintuitive that may be.

Max Hobbs
Macfarlanes LLP

Suspicious Activity Reports: The Law Commission's View

Part 7 of the Proceeds of Crime Act 2002 (POCA) came into force on the 24th July 2002; encompassed within it, the suspicious activity report (SAR) regime. This regime operates by way of a 'referral' mechanism where professional firms such as accountants are placed under a legal obligation to disclose suspicious activity on client accounts to the UK Financial Intelligence Unit (UKFIU). The purpose being to prevent, detect and successfully prosecute money laundering activities.

Young
Fraud
Lawyers
Association

Currently, the threshold for reporting is the Da Silva suspicion (a suspicion which is "more than merely fanciful"); a low threshold which resulted in 463,938 SARs being made to the UKFIU between April 2017 and March 2018.
The Law Commission published its report on the SARs regime on 19th June 2019 citing volume and quality of SARs as key issues and outlining four principle pressures for change; "*the low threshold for criminality, individual criminal liability, confusion amongst those in the profession as to their reporting obligations and the application of suspicion*".

In an attempt to reduce the number of SARs, the Law Commission recommend raising the reporting threshold through a test of 'reasonable suspicion' (as opposed to "*more than merely fanciful*"). It is hoped that a higher threshold for suspicion will go some way in reducing SAR numbers. In this vein, the Law Commission have also developed the defence of 'reasonable excuse' for individuals who fail to make a SAR alongside the introduction of a corporate offence for companies who fail to fulfil their obligations under the SAR regime. This would potentially limit the individual criminal liability of those employed by organisations subject to the reporting regime and thus reduce the number of 'defensive' SARs being submitted, subsequently reducing quantity and workload.

In an attempt to tackle the poor quality of SARs being submitted, the Law Commission propose the formation of an advisory board made up of individuals with experience of the SAR system who would be responsible for monitoring the effectiveness of the reporting procedure and feeding advice back to the Secretary of State on how to improve the system.

It is hoped that the recommendations will improve the efficiency of investigation by reducing SAR numbers and improving the quality of SARs being made. There is of course an argument that the proposals increase the weight of the burden that regulated organisations are operating under because the changes to the suspicion threshold will require a more in-depth analysis of each prospective SAR in order to assess whether the test has been met. Generally, the proposals appear to revolve around the construction of further guidance and refinement of practicalities within the current regime as opposed to a complete system overhaul. The Government are expected to provide an interim response to the recommendations made by the Law Commission. Only time will tell how successful the Law Commission proposals will be in improving this vital method of money laundering detection and ultimately, fulfilling the aims of the legislation.

Ellen Wright
15 New Bridge Street

Review of Maryam Hussein's 'Corporate Fraud: the Human Factor and how to engage juries in fraud trials

Maryam Hussain is a partner at EY and leads the government and public sector investigation team within its Fraud Investigation & Dispute Services practice. 'Corporate Fraud: the Human Factor' was published in 2014 by Bloomsbury.

"It was like riding a tiger, not knowing how to get off without being eaten" is how Ramalinga Raju, once-Chairman of Satyam, described his own fraudulent misconduct. Such emotive rhetoric is often missing from paper-heavy fraud trials. It is, however, such rhetoric that engages a jury and goes to the heart of the mechanism of fraud. As the author summarises: 'fraud is all about people: a human perpetrator deceiving human victims'.

Corporate Fraud: the Human Factor is a rigorously practical handbook for businesses, providing an insight into the character profiles of typical fraudsters. Hussain produces a diagram setting out various employee attributes and assesses how they might positively or negatively impact on the success of an organisation. A powerful and credible communicator is, on the one hand, able to disguise any self-doubts which may undermine the organisation; but that person may also be an excellent liar, capable of convincing colleagues, regulators and auditors; ultimately disguising their criminality.

The starting point for this text is that 'at a fundamental level, businesses are all about people'. By extension, Hussain remarks that 'the only limit to the types and mechanisms for fraud is the ingenuity of people'. It is therefore obvious that, in a fraud trial, any number of bank statements can never be as effective as appealing to a jury's collective humanity.

Hussain quotes the financial journalist Diana Henriques when illustrating the principle of trust: 'no fraud deterrence program, however elaborate, will work if it can be switched off for the people we trust most'. It is this uniquely human transaction which underlies most business and makes it vulnerable to fraudulent manipulation. During a seminar at the Saïd Business School in Oxford, the author developed her analysis of the 'human factor' in relation to the HealthSouth scandal. Unlike his co-defendants, the founder of HealthSouth, Richard Scrushy, was not convicted. Hussain suggests this was partly due to Scrushy's lawyer's ability to translate the mundanity of numbers and finances into a relatable scenario for the jury; he put to a co-defendant that, since he was capable of cheating on, and lying to his wife, he was capable of lying to his colleagues and therefore committing fraud.

The advent of Deferred Prosecution Agreements has changed the way complex fraud cases are prosecuted; inter alia, they recognise that corporate frauds are different to 'ordinary' violence or drug-related crime and that paper-heavy cases are not easily

tried by juries. But where DPAs are unavailable, the solution is surely to make the facts of a given case more accessible to jurors.

The concept of fraud sits uncomfortably in the category of general crime, the latter with which most jurors are at least vaguely familiar. It is therefore doubly important to 'set the scene'. Hussain illustrates that, unlike the average criminal, fraudsters are intelligent, successful and often appear to be the least likely person to commit a crime. That sort of characterisation is an effective way of communicating with a jury.

The text is a surprisingly simple one, and therein lies its subtle persuasiveness. Meta in its simple form, the book points to the simplicity of fraudulent enterprise and the fact that its detection should be straightforward. The real complexity is found in our innately human desire to turn a blind eye and ignore any warning sign that 'something clearly isn't right'.

Bramble Badenach-Nicolson
5 Paper Buildings

We would like to extend our heartfelt appreciation to all our contributing authors.