Commercial fraud litigation – London pow-wow, June 2019

Gerald Byrne
Brown Rudnick, London
GByrne@brownrudnick.com

Jessica Lee
Brown Rudnick, London
jslee@brownrudnick.com

Joanna Curtis
Brown Rudnick, London
jcurtis@brownrudnick.com

Jane Colston
Brown Rudnick, London
jcolston@brownrudnick.com

Commercial fraud is a continuing global menace costing hundreds of billions every year. Crimes such as money laundering, asset misappropriation and insider trading are ever present in financial institutions and across other sectors.

Inadequate anti-fraud systems compound the problem, meaning clear red flags are often missed due to a lack of robust policies and procedures leaving fraudsters often ahead of the game.

To discuss current trends, the Commercial Fraud Lawyers Association met for a breakfast roundtable on 13 June 2019 at the offices of Brown Rudnick, London. The discussion was organised and hosted by partner Jane Colston who was helped in chairing the discussion by Ravinder Thukral, Gerald Byrne, Jessica Lee and Joanna Curtis.

The meeting focused on three topical issues and provided for a very open and thought-provoking discussion on some of the matters facing practitioners at present. Below is a summary of the matters addressed.

Topic 1: What frauds are members seeing and what should corporates and banks do to respond effectively?

Members cited a number of issues that they had come across in recent months such as consumer fraud, asset misappropriation, tax evasion, cybercrime and business misconduct. It was noted that internal actors, such as senior management and rogue employees, seemed to pose the most common threat of the most disruptive frauds. It was also noted that while cybercrime – mostly malware and phishing – has increased recently, asset misappropriation, in the form of embezzlement or false accounting, continues to be prevalent. Business misconduct, such as money laundering and bribery, also continue to make headlines.

Another development noted was the ever-increasing international nature of the many investigations in areas such as money laundering and data breaches. The rise of cross-border misconduct means more complex investigations are being conducted by more regulators in more jurisdictions.

In terms of cultural shifts in companies, many senior executives and board members are thought to be becoming more sensitive to fraud risk and are more likely to ask questions or require additional reporting about fraud risk within the organisation. It was noted that often the hierarchy and culture of a company means a dishonest senior executive or director is not, however, questioned, which permits the dishonest actor to carry out the fraud assisted by other directors who turn a blind eye or are bullied or rewarded into silence.

It was noted that systems are needed so that honest directors play a vital role in detecting and preventing fraud. Those directors who fall below the standard of care required of them should expect to be held to account for any fraud the company suffers while they were 'sleeping at the wheel' or blindly following the dishonest actor.

Topic 2: How is artificial intelligence (AI) being used and what would be a good protocol to agree with opponents?

The use of AI was of particular interest to members both in terms of fraud prevention and as part of disclosure processes in proceedings or investigations.

Fraud prevention

Most members agreed with the proposition that companies needed to embrace AI in addressing fraud-prevention issues, but must ensure that it fits into a holistic approach in which proper systems and controls are in place, which include elements of AI together with human interaction.

It was remarked upon that AI is now capable of detecting fraud in real time and of being anticipatory rather than just reactive. It is also used to speed up internal investigations, with computer-assisted reviews now processing vast amounts of information, recognising patterns, removing duplicate information and determining relevancy unaided.

In this regard, civil disclosure orders against banks often reveal that the banks' anti-money laundering systems are inadequate as banks are allowing accounts to be opened which are then used to receive and launder stolen monies. The risk for banks here is that they may become a more attractive target for both fraud claimants and regulators.

Members also raised matters relating to the limitations to the application of AI in fraud prevention. It was suggested that it is common in fraud cases that emails are written using code words (eg, jumbled numbers or particular codes), or that the necessary communications facilitating the fraud involve lots or oral conversations which would not be picked up by a document review using AI.

Disclosure exercises

In terms of disclosure exercises in proceedings or investigations involving instances of fraud, members recognised that the use of AI was here to stay and will be useful, but raised concerns that the sample set used by the AI may not capture some of the communications required for the system to be properly trained. To combat that issue, senior lawyers should review sample sets and conduct sampling on documents that the AI had discarded as being not relevant.

It was added that AI was also very useful for thematically categorising documents for human review and mapping communications between certain people to show how often they might be communicating, helping to identify areas of interest (eg, where two people should not really be communicating at all).

Finally, the discussion turned to the possible knowledge gap between the technical experts who facilitate AI platforms and the legal counsel tasked with making submissions on the scope of disclosure. To bridge that gap and to facilitate cooperation between practitioners when addressing disclosure matters and the new disclosure pilot scheme in the High Courts of England and Wales (see the IBA Litigation Newsletter, May 2019, for an article on such scheme), it was suggested that a very early discussion between the parties on the use of AI in the disclosure process was very important. In addition, it was suggested that at any hearing dealing with disclosure issues, a person with technical expertise should be present to assist the court with matters of AI.

Going forward, we will likely see more corporates using AI and smart technology to review disparate data quickly in order to recognise irregularities and raise red flags for humans to investigate. This increase of use follows in the footsteps of regulators (such as the Serious Fraud Office) and the courts recognising the usefulness of AI in investigating fraud.

Topic 3: Discuss a sensible common practice regarding post-service dealing with freezing injunctions

A key area for discussion was the usefulness of first return date following service of a freezing order given the short timeframe and various asset disclosures/tracing a defendant is required to do in advance of any meaningful hearing. Rare was the experience of the first return date being used to seek a discharge of a freezing order, albeit there are now several cases where the courts have discharged injunctions, for example, on the basis of material non-disclosure by a claimant.

Often the first return date is used to get directions while reserving the position regarding any discharge of the freezing injunction until further return dates.

Difficulties are caused where a proprietary freezing injunction has been granted over assets held by a defendant, as well as a personal freezing injunction. If the defendant's cash assets are all subject to a proprietary injunction, then the defendant may have difficulty in funding its legal representation because to do so would breach the injunction and also risk that the claimant could ultimately enforce a proprietary claim over any money paid out in legal fees to the lawyers. This could mean that the lawyers would have to pay their fees over to the claimant. Possible solutions discussed included: (1) if there are other fixed assets available, apply to vary the injunctions such that money can be paid out from under the proprietary injunction, but that such monies are replenished from other assets, for example, fixed assets when they are sold; and (2) asking the claimant to undertake not to enforce a proprietary claim against the defendant's legal counsel.

Generally, it was acknowledged that the evidential and costs burden on an applicant to bring an injunction was high, and that claimants with smaller claims or limited funds may struggle to bring full injunction proceedings directly against the party who had committed a fraud. However, the courts of England and Wales have a myriad of remedies pre and post judgment which are available to claimants and can be adapted depending on the legal budget the claimant has.