England & Wales

Latham & Watkins Simon Bushell & James Davies

1. INTRODUCTION

When a fraud is suspected, increasingly the response is to conduct an investigation to ascertain the facts and take appropriate steps. Investigations may be required for a number of reasons, eg where whistleblowers have alleged that wrongful acts have occurred. A thorough investigation conducted in conjunction with, or exclusively by, external experts such as lawyers or accountants, can usefully pre-empt an intrusive investigation by a regulator or the criminal authorities.

Investigations are also viewed as part of good corporate governance, being managed by audit committees in conjunction with general counsel as part of the steps required before the directors can be satisfied that the company's accounts are a true and fair view.

To an extent, the UK has followed the trend in the US, where, in response to a problem, an investigation is often required. Those responsible for managing the investigation should ensure it is conducted lawfully and in line with its intended use, for example, disciplinary proceedings; providing information and reports to a regulator as part of any cooperation or in substitution of an investigation by that regulator; or for use in legal proceedings. Although rules on admissibility of evidence differ depending upon the intended use, there are common rules regarding the gathering and handling of evidence that need to be followed. Similarly, there are several steps to be considered at the outset of an investigation to ensure that a company's position is not further prejudiced eg by breaching employees' rights or alerting suspected wrongdoers before evidence or assets are seized. As well as incurring civil liability a company could be accused of a criminal offence of prejudicing a criminal investigation. These issues are addressed in section 2 below.

In addition to these considerations, it is also necessary to consider whether legal action is required to be taken in the form of civil proceedings to seek redress against any fraud that might have been discovered. Relevant issues in this regard are addressed in the subsequent sections, including the extent to which it will be possible to seek disclosure of relevant information or documents from third parties (section 3), steps that may be taken to preserve evidence or assets (section 4), and the various types of civil claim that might be brought in respect of different categories of fraudulent wrongdoing (section 5). Civil recovery in respect of alleged acts of bribery is addressed specifically in section 6.

2. MANAGING THE INTERNAL INVESTIGATION

In any investigation, it will be necessary to secure relevant hard copy and electronic material. Where there is no risk of document destruction or withholding, it should be possible to notify employees of the investigation and the need to preserve and later produce relevant documents. Where employees have informally consented to this, it is unlikely that the company will breach any relevant regulatory requirements at this stage.

However, frequently the company cannot advise employees as to do so may be an offence. Where it is not possible or desirable to advise employees, the first step will be to secure all relevant hard copy and electronic documents. In addition to the practicalities in managing a search, securing hard copy and electronic documents, several statutes need to be considered, including the Human Rights Act 1998 (HRA), the Data Protection Act 1998 (DPA) and the Regulation of Investigatory Powers Act 2000 (RIPA).

Practical considerations

Avoiding tipping off/prejudicing an investigation

The Proceeds of Crime Act 2002 (POCA) contains two offences which may be committed if an investigation is not handled properly.

The tipping off offence is contained in section 333A of POCA. This is a relatively narrow offence and only applies: to defined regulated institutions; where a money laundering disclosure has been made internally or to the National Crime Agency (NCA); where what is communicated is the fact of the disclosure; and where the disclosure is likely to prejudice an investigation.

An investigation may be easily prejudiced, eg where individuals or companies are warned and can then destroy documents or move assets to frustrate the investigation.

In most investigations it should not be necessary to advise that a disclosure has been made and in practice the offence will rarely be committed.

The offence of prejudicing an investigation contained in section 342 of POCA, on the other hand, is much broader, applies to all individuals and companies and can apply to any disclosure which could prejudice an investigation. There has been no clear guidance on what it covers, but an offence may be committed if an individual is made aware through an investigation that its wrongdoing has been, or is about to be, discovered such that he can take steps to destroy documents.

Audit trail

It is also advisable for those conducting the search to ensure that a clear audit trail can be established for any document; hard copy or electronic. This will avoid disputes later on in the investigation when, for example, documents are put to a witness and they seek to deny ever having received them. A good evidential record can also help to protect against allegations of falsifying, concealing or destroying relevant documents, for example by the Serious Fraud Office (SFO) under section 2 of the Criminal Justice Act 1987.

To ensure an effective audit trail: draw a plan of any office space to be searched, identifying relevant filing cabinets and numbers of drawers, desks, shelves etc. These should then be labelled on the plan, alpha-numerically. Any documents then located as part of the search should be kept with a log sheet indicating their source using the coding from the plan. A similar approach should be adopted for electronic data, for example, memory sticks, diskettes etc and the identity number of any computer imaged should be recorded.

Conducting the search

When conducting such a search the key issues to have regard to are:

- proportionality of search;
- who should conduct the search. It may need to be a third party if there is a significant risk of private documents being located; and
- if personal documents are identified is it possible to leave them unread.

Employment provisions

There are no provisions of English employment legislation which prohibit an employer from conducting a search of an employee's records. Generally, a company can review its own records. The risk in searching an employee's desk without permission is that the searches may reveal personal effects. Further, if the search is done during office hours and in front of or becomes known to other employees an employee may argue that there has been a breakdown of trust and confidence between employer and employee entitling them to resign and claim constructive dismissal. Employers therefore need to ensure that searches are only conducted without permission where necessary, the nature and extent of the search is proportionate to the harm in question, and personal effects are only reviewed to the extent necessary to determine that they are personal and irrelevant to the subject matter of the investigation.

Frequently the extent to which an employer is entitled to search through an employee's desk (or emails) is set out in an employment handbook. The provisions of that handbook should be checked and satisfied before any search is conducted.

To reduce unnecessary invasion of a person's privacy through the review of personal documents, consideration should be given to arranging for independent persons to conduct that search. Those persons should agree not to report back anything of a personal nature to the company. This should be recorded in writing. Alternatively, the search team should work for a different part of the company so that they do not generally have contact with the employees whose desks are to be searched.

Interviews of staff and third parties

Provided there are no 'tipping off' considerations to prevent interviews taking place, an employer can require employees to be interviewed as part of an internal investigation. A refusal by an employee to attend or to answer questions, even to avoid self-incrimination, could give rise to grounds for

disciplinary action, ultimately leading to dismissal for gross misconduct in serious cases.

Before conducting any interview, a check should be made of any relevant corporate investigation or disciplinary policy. Those policies may give the individual the right to be legally represented or accompanied by a friend, although generally such policies will only apply to the disciplinary stage and not the investigative stage. If there is no policy and an employee wishes to bring a lawyer or friend, the employer is entitled to refuse that request, and if the employee then fails to attend, disciplinary action can then be taken. Similarly, if a custom or practice has developed of allowing employees to be accompanied or concessions have been made in the course of the investigation to other employees, the company would be obliged to follow that custom or offer similar concessions, or otherwise run the risk of the employees complaining that they have been treated inconsistently.

Decisions about what notice the interviewee should receive of the meeting, the issues to be discussed, the opportunity to pre-read documents to be put to them and whether to record the interview are all for the employer to make in their absolute discretion, unless provided for in a handbook or where a custom or practice has developed. Consistency of treatment of all employees to be interviewed is important. If the employer considers that disciplinary action may follow, it may assist to ensure that the employee is given adequate notice of the meeting and the discussion topic to prevent the employee later seeking to change their version of events, subsequently claiming they had by then had an opportunity to properly refresh their memory and gather their thoughts. Similarly, it is advisable for the interviewee to be given regular breaks and for the interview not to be aggressively long, otherwise the results may subsequently be said to be unreliable.

A key consideration when the results of the interview may need to be used in subsequent criminal proceedings is whether a caution under the Police and Criminal Evidence Act 1984 should be given to the effect that: *'You do not have to say anything. But it may harm your defence if you do not mention when questioned something which you later rely on in court. Anything you do say may be given in evidence'* (PACE Code of Practice C, section 10).

The position was considered in *R v Welcher* [2007] EWCA Crim 480, where the court concluded that it was not necessary for a caution to be given for the interview note to be admissible in subsequent criminal proceedings. Tactically, it may not assist the company as part of its fact finding to issue cautions at the start of an interview as it is likely to make an employee nervous and less willing to tell the truth and implicate others for fear of a risk that they will incriminate themselves.

Statutory rules under the HRA, DPA and RIPA

Human rights legislation

Because the search may result in personal items being reviewed, even if only for the purpose of determining relevance to the investigation, the HRA is

engaged, specifically Article 8 which gives individuals the right to respect for private and family life, home and correspondence.

The right can be restricted only in specified circumstances, to the extent that this would be necessary in a democratic society and pursues certain defined aims, including the prevention of disorder or crime.

Such interference must be necessary and proportionate, ie no more than is necessary to achieve the desired aim.

The right has been interpreted broadly and may encompass the right to have personal information kept private and confidential. 'Family life', 'home' and 'correspondence' have also been widely interpreted. Therefore, the key question will be whether the interference is 'proportionate' and no more than necessary to facilitate the investigation.

In determining what is proportionate, a court is likely to have regard to other legislation governing the search, such as the DPA and RIPA (see below). Provided any search or review of documents is conducted in accordance with that legislation, the court would likely consider the interference proportionate.

Finally, the court is likely to have regard to the nature of the suspected wrongdoing. The more serious the concern and the stronger the evidence, the more proportionate the interference is likely to be.

Data protection

The DPA regulates the 'processing' of 'personal data' by a 'data controller':

- Processing includes obtaining, retrieving, consulting, holding, disclosing and deleting.
- Personal data means data which relate to a living individual who can be identified (i) from those data or (ii) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (see the discussion on the scope of this definition in *R (Kelway) v The Upper Tribunal (Administrative Appeals Chamber) and Northumbria Police and R (Kelway) v Independent Police Complaints Commission* [2013] EWHC 2575 (Admin).
- A data controller is defined as the person (natural or legal) who (alone, jointly or in common with others) determines the purposes for which and the manner in which any personal data are to be processed.

The DPA will likely cover the review of employees' documents in the course of an internal investigation and disclosure of information about identifiable individuals to third parties or other group companies. A company processing data as part of an investigation should ensure that it has the necessary registration (called notification under the DPA section 17) permitting that processing, particularly where the investigation is for the purpose of detecting or preventing crime.

The legislation is highly technical, and there are also significant variations in data protection legislation and enforcement within and outside

Europe. It should not be assumed that an English company conducting an investigation which complied with the DPA in England would also be complying with local data protection laws by taking the same approach overseas when accessing overseas office documents, even where the documents in question belonged to the English company.

Whether or not the DPA applies will depend on whether the data controller is searching electronic or hard copy records and whether the data controller is a public authority:

- Any search of electronic documents containing information relating to living, identifiable individuals is likely to engage the DPA.
- Where the company which is the data controller is not a public authority for the purposes of the Freedom of Information Act 2000, hard copy documents are only subject to the DPA where they form or comprise a 'relevant filing system' and in reality, the majority of hard copy documents are unlikely to be included within its interpretation (although, if the company intends to create an electronic copy of the document, then in practical terms this may bring the review of the hard copy document within the scope of the DPA). See Auld LJ's comments in *Durant v FSA* [2003] EWCA Civ 1746. If the organisation is a public authority, then all manual documents and files it controls that include information relating to living, identifiable individuals are likely to fall within the scope of the DPA, whether or not they are relevant filing systems.

The core obligation the DPA imposes on a data controller is to comply with the eight Data Protection Principles, which can be summarised as:

- process fairly and lawfully (the 'first principle');
- process only for purpose(s) specified (the 'second principle');
- personal data must be adequate, relevant and non-excessive;
- personal data shall be accurate;
- do not keep personal data longer than necessary;
- process in accordance with the data subject's rights;
- take appropriate technical and organisational measures to keep data secure (the 'seventh principle'); and
- do not transfer to countries outside the European Economic Area lacking adequate protection (the 'eighth principle').

The first and second principles are significant in the data gathering process. The first principle is addressed in detail below, and the Article 29 Working Party (an EU organisation which provides expert advice on data protection) has published guidance on the second principle's practical application in its Opinion 03/2013 on purpose limitation (WP 203). The eighth principle will be relevant where the investigation is being managed outside the European Economic Area or the results of the investigations are to be shared with a parent company outside the European Economic Area (the EEA).

Where third party contractors are used, eg IT specialists imaging computer hard drives, additional steps are required to satisfy the seventh principle. Specifically, the data controller is required to have a written agreement with

its data processors, imposing prescribed restrictions, such as that the data processor: (i) may only process the relevant personal data in accordance with the data controller's instructions; and (ii) shall implement appropriate technical and organisational measures to secure personal data against loss or any form of unauthorised processing.

Note that the European Commission in January 2012 published a draft Regulation which is designed to eventually replace the existing Directive (on which the DPA is based) and which in its current form would introduce a complex new legal framework to govern data protection and severe fines for companies which breach the new rules (up to the greater of 5 per cent of their annual global turnover or EUR 100 million). The European Parliament voted in support of the proposals on 12 March 2014, which are now being considered by the Council. It is expected that the Regulation will be agreed in 2015 and will come into force in 2017.

DPA – the first principle

Under the first principle, processing will not be regarded as fair and lawful unless at least one of a number of conditions listed in Schedule 2 to the DPA is met. Further, to the extent that any of the data in question is 'sensitive personal data' one of the additional conditions listed in Schedule 3 to the DPA must be satisfied.

The most relevant conditions in Schedule 2 are that the review and any disclosure by the investigating company of the emails or other information containing personal data – in each case is:

- subject to the consent of the individuals affected. Consent must be specific, freely-given and informed. Employment contracts and IT use policies may contain provisions whereby employees are deemed to consent to review of their email accounts for specified purposes, however, it is generally not advisable for an employer to rely on consent from its employees because the validity of such consent is easy to challenge. In any event, emails may contain the personal data of third party individuals who cannot be deemed to have consented in this manner;
- necessary for the purposes of the company's own legitimate interests or those of the recipient (eg a regulator) provided that the reviewing and disclosure would not be unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subjects (ie the employee and any other individual(s) identifiable from the information). This condition requires a balance to be struck between: (i) the legitimate interests in (a) conducting a review and (b) the disclosure of relevant personal data; and (ii) the fundamental rights of the individuals affected, including their (human) right to respect for private and family life and correspondence. This balance needs to take into account issues of proportionality, the consequences for the individual and the seriousness of the issues in question, for example, whether any offences are alleged to have been committed. Would a particular disclosure prejudice the

legitimate interests, rights and freedoms of individual employees, including their right to respect for privacy at work;
- necessary for compliance with any non-contractual legal obligation to which the company is subject. In this respect, the view of the UK data protection regulator, the ICO, is that the legal obligation in question should be an obligation pursuant to English law – a non-UK legal obligation, such as an order from a US court, is unlikely to satisfy this condition (although it may satisfy an alternative condition in Schedule 2); or
- necessary for the administration of justice. It is unclear whether this condition is in fact broad enough to apply to non-English legal proceedings.

The review and disclosure of all the particular information would need to be 'necessary' in each case. Necessary has been interpreted by the English courts as meaning more than merely convenient or desirable but less than essential or unavoidable. The use of keyword searches and limitations in date ranges applied to searches or reviews of material will assist in ensuring that the information subject to the processing is 'necessary' rather than merely being included inadvertently in the material being reviewed.

Where a particular individual was not actually and/or could not reasonably be believed to be implicated in the suspected unlawful activity then it could be argued that a company's processing of that person's information was not 'necessary' and therefore the conditions listed above may not be satisfied (apart from consent). Care should therefore be taken when considering whether to review the emails and documents of those who are not considered to be central to the investigation.

There is a duty under Schedule 1 of the DPA to provide certain information to individuals (or 'data subjects') when processing their personal data. However, this duty is subject to an exception where such processing is necessary for compliance with any (non-contractual) legal obligation. Such legal obligations would include the offences under sections 333A and 342 POCA set out above.

DPA – relevant Schedule 3 conditions

One of the conditions listed in Schedule 3 may have to be complied with if sensitive personal data are likely to be processed in the course of a review. Sensitive personal data is defined to include information about an individual's mental or physical health or condition, their racial or ethnic origin, their sex life and the (alleged) commission by them of a criminal offence. Investigations into fraud, insider trading or corruption, for example, may well involve processing of sensitive personal data. In such situations, a company conducting an investigation is likely to comply with the sixth condition in Schedule 3 which provides that the review and disclosure (if applicable) must be:
- necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); or
- necessary for the purpose of obtaining legal advice; or

- otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Even if the requisite Schedule 2 and/or 3 conditions are satisfied, it is still necessary to ensure that the processing is fair and lawful in general terms, which includes having regard to whether the person from whom the data were obtained was not misled or deceived.

Where the company is seeking to investigate circumstances which suggest a criminal offence may have been committed, which would include fraud then, even if the aim of the company's investigation is to bring civil proceedings to recover the misappropriated assets, one of the Schedule 3 conditions has to be complied with.

Processing will not generally be regarded as fair unless the data subject (ie the individual who is the subject of the personal data) is given, or has made readily available to them, details about the processing of their data (ie the identity of the data controller and the purposes for which the data are to be processed).

Generally, one of these conditions should be capable of being satisfied. However, there may be a variety of reasons (eg tipping off or alerting those involved to the possibility of civil proceedings) which make that impracticable.

There are limited exceptions within the DPA which mean that an individual does not have to be informed. Section 29(1) DPA provides that personal data processed for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of any tax/duty,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and the subject access right (ie the right of an individual to be given access to their personal data by the controller of those data), provided that complying with the first principle and the subject access right would be likely to prejudice any of the purposes listed above. Clearly this is a question of fact in each case, but where there is a risk that someone may destroy documents or hide assets, the conditions above are likely to be satisfied.

RIPA – interception of communications

The RIPA governs the interception of communications made via public telecommunication systems, private telecommunication systems and public postal systems. Of these, only private telecommunications systems are likely to be of relevance to an internal investigation being conducted by a company into its affairs; the arrangement for transmitting emails in most organisations will involve a private telecommunications system.

RIPA makes it a criminal offence to intercept intentionally and without lawful authority any communication in the course of transmission by private telecommunication systems, unless the person intercepting has a right to control the relevant network, eg the company's IT director, has the express or implied permission of such a person to intercept communications on that network.

'Interception' involves the modification or interference with the system, or the monitoring of transmissions, so as to make the contents available, while being transmitted, to a person other than the sender or intended recipient.

Communications are taken to be made available to another where they are recorded, during transmission, such that they are available to a third party at a later time (section 2(8) RIPA). Therefore, the use of keystroke software which allows an independent record to be created in real time of all key strokes by an employee on a computer, or software which allows an email in the course of transmission to be made available to another person, will involve 'interception'.

The Court of Appeal has held that a data controller 'hacking' into saved voicemails that have already been listened to by the recipient will qualify as interception 'in the course of' transmission (*R v Edmondson and others* [2013] EWCA Crim 1026 (28 June 2013)).

It is not clear from the legislation whether an email which has been sent and read is 'intercepted' if it is subsequently copied and reviewed. Views publicly expressed by the ICO, which is responsible for bringing enforcement proceedings under the DPA, are that a review of unread emails would constitute 'interception' but that a review of read emails would not.

Accordingly, where the investigation is likely to involve the review of recent emails, care needs to be taken to ensure that 'unread' emails are not copied. This is frequently impracticable because imaging software takes a complete image of an inbox without distinguishing between read and unread emails. To avoid the risk of committing a criminal offence, the consent of the person with the right to control the system should be obtained.

In addition to criminal liability, civil liability can arise if the review of email is mishandled. Further rules on the interception of communications are contained in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Interceptions are authorised for monitoring or recording communications, *inter alia* to: (i) establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures, or to ascertain or demonstrate standards which are or ought to be achieved; or (ii) prevent or to detect crime.

Unless one of the above criteria is satisfied and the system controller has taken all reasonable efforts to inform users that interceptions may take place, the interception will not be lawful and will give rise to civil liability. An employer conducting a search of its employees' emails for the purposes of an investigation is likely to satisfy one of the above.

Similarly, provided the company has an IT policy which has been made available to employees and which warns employees that their emails may be monitored for any of the above purposes, that will satisfy the requirement to inform users. In practice the Regulations are not considered to require third party individuals who may have sent or received emails to be informed.

Where the conditions cannot be satisfied or there is no relevant monitoring policy, the practical limitation will be a review of unread emails. In those circumstances, to avoid incurring loss to an employee or giving the

employee cause for complaint (or to resign or claim constructive dismissal) care should be taken to ensure that as part of the review unread emails are not reviewed.

Privilege and disclosure

Legal professional privilege

Where an investigation could lead to the discovery of facts which may result in proceedings, civil, criminal or regulatory, being brought by or against the company, it is likely to be important to seek to ensure that the documents produced in and the findings of the investigation are protected from disclosure by legal professional privilege. That remains the case even if a regulator may expect any applicable privilege to be waived.

Under English law, generally a party can avoid disclosing only documents covered by legal professional privilege in legal proceedings or in response to a request for production or a notice requiring production issued by a regulator. It is not clear based on the current authorities whether legal professional privilege applies to all documents produced in the course of an investigation.

There are two branches of legal professional privilege: legal advice privilege and litigation privilege.

Legal advice privilege. Legal advice privilege protects from disclosure communications between a lawyer and their client created for the purpose of giving or receiving legal advice, or documents evidencing the content of such communications.

It is important to note that advice privilege does not cover all communications between a client and their lawyer. It does cover the following types of documents:

- working papers and draft documentation; and
- advice on presentation of evidence to an adversarial inquiry, even if regarded as merely 'presentational' assistance (provided this constitutes advice as to what should prudently and sensibly be done in the relevant legal context).

Legal advice privilege does not extend to communications between the lawyer or client and a third party, or documents produced by a third party even if it was intended that the documents would be put before the lawyer to enable them to give legal advice. Where it is necessary to speak to third parties during an investigation (eg sub-contractors, former employees or professional advisers) those discussions will not be protected by advice privilege and any documentation produced by those third parties will not be protected. This creates problems where forensic accountants work alongside lawyers: the accountants' work product will not be covered by legal advice privilege, particularly in light of the recent decision of the Supreme Court that legal advice provided by non-lawyers (in this case, PricewaterhouseCoopers) cannot be protected by legal professional privilege (*R (Prudential plc and another) v Special Commissioner of Income Tax and another* [2013] UKSC 1).

It is also important to recognise what is meant by 'the client'. The Court of Appeal's decision in *Three Rivers District Council & Others v The Governor and Company of the Bank of England* [2003] QB 1556 interpreted narrowly the meaning of client in a corporate context.

In the context of an investigation, the Board, the Audit Committee, the General Counsel, Company Secretary or certain senior management may all fall within a narrow definition of 'the client'. However, those who are interviewed who may be wrongdoers or simply witnesses may not be part of the client, may never see the lawyers' advice or be interested in it.

Litigation privilege. Litigation privilege is wider than legal advice privilege. It protects from disclosure confidential communications between a lawyer and their client, or between either of them and a third party, which were created for the dominant purpose of gathering evidence for use in legal proceedings or for giving legal advice in relation to such proceedings. The legal proceedings in question must at least be 'reasonably in prospect', if not already pending.

The actual or anticipated litigation can be any first instance or appeal litigation, civil or criminal, whether or not in a court of record, including quasi-judicial proceedings. Litigation privilege can be established in relation to actual or anticipated arbitrations, and includes foreign litigation, but does not apply to inquisitorial rather than adversarial proceedings.

Where an investigation is prompted by a regulatory issue (such as an investigation by the FSA, SFO or Competition and Markets Authority (CMA)) the litigation anticipated may be investigative or inquisitorial, rather than adversarial, and so it would be prudent to assume that only the more restricted legal advice privilege will apply until it is clear that litigation privilege can be asserted (although in some circumstances the courts have been willing to accept that regulatory investigations are sufficiently 'adversarial' relatively early in the investigative process – see *Tesco Stores Limited v OFT* [2012] CAT 6).

Seeking to assert that materials produced in an investigation are covered by litigation privilege can be problematic. By their nature, such investigations are often fact finding. At the outset of an investigation there may simply be an unsubstantiated anonymous allegation. At the other end of the spectrum, a dossier may have been prepared or an audit may show the company has suffered a significant loss. In those circumstances, the purpose of the investigation is not to find out if there is a problem, but who did it and where the assets are. In the latter case litigation privilege would probably apply. In the former, it is much less likely.

Whether litigation privilege does apply will be a question of fact in each case but it may be advisable to document the reasons for any decision that it does apply. Where it does not apply at the outset of an investigation, the position should be kept under review. It is possible that after the document review evidence becomes available which alters the position. The clear advantage in litigation privilege applying is that it will protect

from disclosure the work of third parties as well as the work product of any interviews which are conducted.

Disclosures following the investigation

Depending upon the results of the investigation and the nature of the company, there may be a number of disclosures to be made.

All companies are caught by the POCA which makes it an offence to possess, use, transfer, convert etc property which the company or an individual suspects is criminal property. An offence can be avoided if a disclosure is made to the NCA and consent sought to the prohibited act. Where an investigation finds that employees have committed criminal acts on the company's behalf, consideration should be given to disclosing to NCA.

For regulated companies, guidance and examples of matters which should be reported are given in SUP 15 of the FCA Handbook. An institution may therefore have to report where it has been the victim of a significant fraud that could give rise to loss or reputational harm.

For listed companies, Disclosure and Transparency Rule 2.2 requires a company to announce if it has information which is price sensitive, which could include the financial impact of a significant fraud. Further, pursuant to the FCA Handbook at DEPP 6.2.1(2)(a), 6.4.2(4) and 6.5.A.3(2)(a), the UK Listing Authority (which now sits within the FCA) will take into account whether or not a breach was brought to its attention when determining whether to take disciplinary action, and, if so, what penalty will be imposed.

Companies should also consider self-reporting potential wrongdoings to the Intelligence Unit of the SFO. Self-reporting is no guarantee that the company will avoid prosecution, but paragraph 32 of the SFO's Guidance on Corporate Prosecutions identifies *'[f]ailure to report wrongdoing within reasonable time of the offending coming to light'* and *'[f]ailure to report properly and fully the true extent of the wrongdoing'* as public interest factors in favour of prosecution. The Guidance also states that self-reporting should form part of a broader pro-active approach by the corporate management team when the offending is brought to their notice, and may involve *'making witnesses available and disclosure of the details of any internal investigation'*.

The CMA offers leniency in certain circumstances to businesses and individuals who have participated in cartel activity and come forward with information about the cartel. 'Type A' immunity offers guaranteed immunity from financial penalties, criminal prosecution and Competition Disqualification Orders against cooperating current and former directors, and is available to the first member of a cartel to come forward and will be available provided the CMA has not already begun an investigation and does not already have sufficient information to establish the existence of the alleged cartel activity. 'Type B' immunity is available to a business that is the first to report and provide evidence of a cartel but which does so only after an investigation has started. It offers similar protections as Type A immunity, except that these are discretionary rather than guaranteed. 'Type C' leniency is available to an applicant that reports and provides evidence of

cartel conduct in circumstances where another business has already reported the cartel activity. Type C leniency offers a discretionary reduction in corporate penalties of up to 50 per cent, a discretionary criminal immunity for specific individuals, and protection for its current and former directors from Competition Disqualification Orders.

Disclosure may be required to insurers of circumstances which could give rise to a claim, both to ensure that cover is available in future but also to ensure that insurers are aware of relevant information at the time of renewal.

Subsidiaries may wish to report matters to their parent company. When that company is overseas, particularly outside the EEA, consideration will need to be given to whether that disclosure complies with the Eighth Data Principle. Before a transfer of personal data is made to a non-EEA country, at least one of the following should apply:

The transfer must be:

- necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- necessary for the purpose of obtaining legal advice; or
- necessary for the purposes of establishing, exercising or defending legal rights.
- to a 'white-listed' country such as Guernsey, Argentina, Canada (limited), Switzerland;
- subject to a data transfer agreement incorporating terms approved by the European Commission.

Where the results of the investigation may have ramifications for the parent, for example because it may have to make its own regulatory disclosures, the transfer is likely to be permitted.

3. DISCLOSURE FROM THIRD PARTIES

The victim of a fraud will wish to consider the issue of evidence gathering. Very often, third parties are a valuable source of vita; information relating to both the commission of any fraudulent acts which they may have been innocently involved in; and information as to the whereabouts of any misappropriated assets. The claimant may thus bolster its case by seeking disclosure from such third parties. This can take two forms: (i) third party disclosure pursuant to the Civil Procedure Rules (CPR); and (ii) the Norwich Pharmacal jurisdiction.

Civil Procedure Rules

The CPR makes provision for disclosure against a non-party under CPR 31.17. Specifically, CPR 31.17(3) states that the court may make an order for non-party disclosure where the following jurisdictional tests are met:

(a) the documents of which disclosure is sought are likely to support the case of the claimant or adversely affect the case of one of the other parties to the proceedings; and
(b) disclosure is necessary to dispose fairly of the claim or save costs.

For the purposes of requirement (a), it is important to note that where disclosure is sought of a class of documents, this threshold test must be

applied to each and every document in that class. Unless the court is satisfied that all the documents of the class are 'likely' to be relevant to the proceedings, it will not order disclosure. This is because it is not appropriate to burden the non-party with the duty of determining whether particular documents meet the relevant requirements or not. Equally, the court must be satisfied that the documents do in fact exist, rather than forcing the non-party to search for documents which may not exist.

It is necessary to consider requirement (b) only where requirement (a) has been satisfied. This requirement focuses on the strict necessity of disclosure, since non-party disclosure should not be ordered unless there are no alternatives. In *The Secretary of State for Transport v Pell Frischmann Consultants Ltd* [2006] EWHC 2756, the court rejected the proposition that the law on whether disclosure was desirable under CPR 31.16(3)(d) (which relates to pre-action disclosure) was relevant to the question of whether disclosure was 'necessary' under CPR 31.17(3)(b) (which relates to disclosure against a non-party). Therefore, if the relevant information or documentation can be obtained by another route, disclosure will not be ordered.

Even if both requirements (a) and (b) are satisfied, it does not automatically follow that non-party disclosure will be ordered. In *Constantin Medien Ag v Ecclestone and others* [2013] EWHC 2674 (Ch), Vos J asked the following additional questions: (i) whether the definition of the documents is sufficiently clear and specific, so that no judgments about the issues in the case are required by the respondents; and (ii) whether, as a matter of overall discretion, disclosure of that class of documents should be ordered.

It should also be noted that under the non-party disclosure rules in CPR 31.17, there is a requirement that proceedings must already have been issued. This can be a major problem if the claimant is unaware of the identity of the substantive defendant.

In contrast to the non-party disclosure rules above, CPR 31.16 is designed to assist a claimant seeking information to bring an action. It can be used to seek pre-action disclosure only against someone who is likely to become a party to subsequent proceedings.

Norwich Pharmacal relief

A Norwich Pharmacal order enables a claimant to seek disclosure from a party who is involved or mixed up in a wrongdoing (whether innocently or not), but who is unlikely to be a party to the potential proceedings.

The most common use of the order is to identify the proper defendant to an action, thereby allowing the claimant to bring an action against the wrongdoer where it otherwise could not. However, Norwich Pharmacal orders can also be used for a number of different purposes, including: to identify the full nature of the wrongdoing; trace assets and proprietary claims; obtain the source of information in a publication; and enable a claimant to plead its case. The flexibility of the Norwich Pharmacal order is discussed in greater detail below.

The jurisdiction derives from *Norwich Pharmacal v Commissioners of Customs & Excise* [1974] AC 133. The claimant was the proprietor of patents for a chemical compound. The defendants (HMCE) had published statistics showing the importation of the compound, without disclosing the identity of the importers. The claimant had not consented to these imports; it considered that its patent rights had been infringed, and it wished to bring proceedings against the importers. The claimant requested the names of the importers. HMCE resisted, claiming that they neither had the power to disclose the information, nor were they obliged to disclose it, and in any event the information was confidential. The court ordered HMCE to disclose the identity of the importer.

The relief is fluid and the circumstances in which it may be used are not fixed, allowing it to develop. In fraud cases, the orders are often obtained against banks, for disclosure of bank statements and records to show the whereabouts of monies to which the claimant asserts a tracing claim. In this context, the order is now commonly known as a Bankers Trust order – after the case in which the order was first devised: *Bankers Trust Company v Shapira* [1980] 1 WLR 1274.

Such applications are often made *ex parte*, prior to the commencement of any substantive claim against the defendant, and accompanied by a 'gagging order' relieving the bank of any duty to inform its customer that such an order has been obtained.

To obtain a Norwich Pharmacal order the claimant must establish that:

- There is a good arguable case that a wrong has been committed, making it likely that a claim could be brought against the wrongdoer.
- No other relevant CPR provisions could apply.
- The third party is likely to have relevant documents or information.
- The third party is involved in the wrongdoing (so as to have facilitated the wrongdoing, whether innocently or not).
- The third party is not a 'mere witness'. A mere witness is someone not involved in the wrongdoing but who could potentially be called to give evidence, should proceedings be brought. Exceptions to this rule include where the defendant is the only practicable source of information, or where proceedings cannot be brought without the third party providing information to identify the wrongdoer.
- The order is necessary in the interests of justice (ie to enable an action to be brought against the ultimate wrongdoer).

As well as their obvious pre-action value, Norwich Pharmacal orders are also of great application post-judgment. In *Mercantile Group (Europe) v Aiyela* [1994] QB 366, the Court of Appeal observed that while the Norwich Pharmacal case was concerned with a tortious wrongdoer, there was no relevant distinction between such a person and a judgment debtor deliberately avoiding the consequences of a judgment; the principles applied in both situations. The defendant was ordered to disclose information relating to the whereabouts of the judgment debtor's assets.

For a time, the courts appeared to be tightening the Norwich Pharmacal jurisdiction, emphasising the 'necessity' aspect of the order. In *Yuri Nikitin &*

Others v Richards Butler LLP & Others [2007] EWHC 173 (QB), the claimants sought wide-ranging Norwich Pharmacal relief against a law firm and the private investigators it had allegedly instructed. The purpose of the application was to obtain documentation enabling the claimants to ascertain the extent of an allegedly unlawful investigation and the identity of those involved. The court sought to assess whether the information requested was vital to the claimants' decision whether or not to sue.

The judge held that the claimants had wholly failed to establish the relevant necessity to justify the relief they sought. In particular, it was unlikely the defendant would hold information which was not otherwise accessible to the claimants. Moreover, it appeared from the claimant's serious allegations that they already considered that they held evidence sufficient to bring the claim.

However, in the subsequent case of *R (on the application of Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2008] EWHC 2048 (Admin), the English High Court took a less stringent approach to the test of necessity. The court was of the view that *Yuri Nikitin* had unduly increased the test of what was 'necessary' to enable a claim to be brought, by referring to information or documents 'vital' to a decision to sue or ability to plead, which could not be obtained from other sources. The court held that there was no authority that justified a more stringent requirement than 'necessity'. Accordingly, it should not be considered that Norwich Pharamacal relief is a remedy of last resort.

In *Mohamed*, the claimant sought Norwich Pharmacal relief requiring the Foreign Secretary to provide documents and information which were necessary for his defence of terrorist charges in the United States. In granting the order, the court emphasised the flexible nature of its Norwich Pharmacal jurisdiction. It noted that the remedy was not confined merely to cases where the information/documents were needed to identify a wrongdoer, but could be used for a variety of purposes in all contexts, whether in civil or criminal proceedings. While the necessity requirement remained important, the court held that it was entitled to look at all the circumstances including the size and resources of the claimant, the urgency of its need and any public interest in having those needs satisfied, when determining whether the requirement was met. Similarly, the scope of what could be ordered would also depend on the circumstances of the case and what was in the interests of justice.

In recent years, the courts have shown an increased willingness to 'police' the implementation of Norwich Pharmacal orders with third party experts. For example, in *Media Cat Ltd v Adams* [2011] EWPCC6, the claimant obtained Norwich Pharmacal orders against certain internet service providers compelling them to provide details on thousands of their customers in respect of possible illegal downloads of pornographic material. The claimant subsequently wrote to all the customers demanding compensation, in circumstances where it had not presented evidence that these customers had in fact illegally downloaded any relevant material. In these circumstances, the court suggested that an experienced and neutral solicitor be appointed

to supervise the use of documents obtained pursuant to the order. In *Patel v Unite* [2012] EWHC 92 (QB), a respondent who lacked the necessary technical expertise to comply with an order was compelled to allow an IT expert to access its computers in order to retrieve the relevant data – this was significant, as it was not clear prior to Patel whether or not the court had the power to make such an order.

In summary, the court's Norwich Pharmacal jurisdiction remains a strong and flexible tool to assist the victim of a fraud. However its use as a purely tactical tool is likely to be resisted.

4. STEPS TO PRESERVE ASSETS/DOCUMENTS

A further immediate concern of a claimant faced with a fraud will be to take steps to protect the *status quo*. This pre-emptive step usually has two limbs: identifying and freezing assets pending claims against the defendant; and preserving evidence which might otherwise be destroyed. This section therefore concentrates on:

- freezing (formerly 'Mareva') injunctions; and
- search and seizure (formerly 'Anton Piller') orders.

Both orders are discretionary and therefore may be refused if, in all the circumstances of the case, the court considers it inappropriate to grant relief. In making this assessment, the claimant's own conduct will be scrutinised by the court. It is important to note that both orders are considered draconian and will not be granted lightly.

4.1 Freezing injunctions

A freezing injunction is an interim order which prohibits a party from disposing of or otherwise dealing with its assets. It exists to prevent a defendant from hiding, moving or otherwise unjustifiably dissipating its assets so as to render itself judgment-proof. The order is therefore typically sought by a claimant to preserve the defendant's assets until any judgment can be obtained or satisfied. It can be sought at any stage in proceedings, including after judgment has been given.

The English court has the power to grant a freezing injunction both in respect of assets within England and Wales (domestic freezing injunctions) and also assets situated worldwide (worldwide freezing injunctions, pursuant to section 37 of the Senior Courts Act 1981). Indeed, the effect of that provision is that it is irrelevant where the defendant is physically located, as long as the court has jurisdiction over it. The relevant provision is CPR 25.1(1)(f), which demonstrates that this remedy is discretionary.

A freezing order may only relate to assets against which a judgment could potentially be enforced and so the defendant must have a legal or beneficial interest in the assets frozen. The ambit of the order can include various types of assets (including intangible assets), such as bank accounts, shares, goodwill, physical property and land.

There will, of course, be cases where the claimant is seeking the order not because it wants compensation for a wrong, but rather, because its own assets have been wrongfully taken by the defendant and it seeks to prevent

the defendant from dissipating those assets. English law therefore provides for two types of freezing injunction.

First, there is the definitive 'Mareva' injunction (the name being taken from the case where it was first recognised), prohibiting the defendant from disposing of or dealing with its assets to defeat the claimant's claims. The order will normally be subject to defined exceptions (eg the defendant will not be prevented from spending money on reasonable living expenses or legal fees, carrying out ordinary business transactions, or paying creditors), and a financial limit representing the value of the claim plus interest and costs. The types of freezing order which can be sought are an order freezing a single, identifiable asset, or specific assets; a maximum sum order (an order limited to an amount covering the likely sum that the claimant would recover at trial, which may include interest and costs); and an unlimited order covering all of the defendant's assets.

Alternatively, where the claimant has a proprietary interest in respect of an asset, or its proceeds (ie it asserts that they are, or represent, its own property), it may seek that a proprietary injunction be granted over the specific assets.

The personal order: 'Mareva' injunctions

'Mareva' injunctions may:

- affect assets located within the English jurisdiction (a domestic freezing injunction);
- affect assets worldwide (a worldwide freezing injunction); and
- be used to aid foreign proceedings.

Domestic freezing injunctions

To obtain a domestic freezing injunction, the claimant must demonstrate that:

- it is just and convenient for the court to grant a freezing injunction;
- there is a substantive cause of action;
- it has a good arguable case;
- the defendant has assets within the jurisdiction; and
- there is a real risk that the defendant may dissipate the assets.

Just and convenient. The ultimate requirement is whether the court considers it 'just and convenient' to grant a freezing injunction (section 37(1) of the Senior Courts Act 1981). In this context, it is important to note that the court will examine the claimant's own conduct; the claimant should therefore act reasonably, conscionably and without undue delay. Even if all the further requirements set out below are met, the effect of this provision is that the court retains discretion to refuse relief if freezing the defendant's assets would not be in the interests of justice.

Substantive cause of action. Under English law, a freezing injunction is a remedy, not a cause of action (*Owners of Cargo Lately Laden on Board the Siskina v Distos Compania Naviera SA (The 'Siskina')* [1979] A.C. 210). Accordingly, the remedy can only be granted if it protects the efficacy of underlying court proceedings, domestic or foreign (*Fourie v Le Roux* [2007] UKHL 1). While the

claimant cannot guarantee that it will recover judgment, it must at least point to proceedings already brought or about to be brought so as to show where and on what basis it expects to recover judgment.

A claimant seeking a freezing injunction may find that the defendant has limited assets. In contrast, their spouse, or a company controlled by them, may have more substantial assets. If the claimant, however, has no cause of action against the spouse or company, ordinarily it could not be granted a freezing injunction over them, allowing assets to be dissipated. In practice, therefore, the court will grant a freezing injunction against third parties who are joined to the action as co-defendants, even if the substantive cause of action is not against the third party. The courts have granted freezing orders against: a company of which the defendant was a shareholder (*TSB Private Bank International S.A. v Chabra* [1992] 1 W.L.R. 231); the defendant's spouse (*Mercantile Group (Europe) AG v Aiyela* [1994] Q.B. 366); and special purpose vehicles whose bank accounts were effectively controlled by the defendant (*Yukos Capital SARL v OJSC Rosneft Oil Company & Others* [2010] EWHC 784).

Good arguable case. The claimant must also satisfy the court that it has a 'good arguable case' in respect of the underlying cause of action (*Rasu Maritima S.A. v Perusahaan Pertambangan* [1978] Q.B. 644). This is defined as a case which is more than barely capable of serious argument, and yet not necessarily one which the judge believes to have a better than 50 per cent chance of success (*Ninemia Maritime Corporation v Trave Schiffahrtsgesellschaft M.B.H. und Co. K.G. (The 'Niedersachsen')* [1983] 2 Lloyd's Rep. 600). In evaluating whether there is a good arguable case, the court will consider any suggested defence to the claim, including any limitation defence (*Kazakhstan Kagazy plc and others v Arip* [2014] EWCA Civ 381).

The defendant has assets within the jurisdiction. There must be evidence from which it may be inferred that the defendant has assets within the jurisdiction.

To the extent that assets are known or suspected to exist, these should be identified, even if their value is unknown. If it is known or suspected that assets are in the hands of third parties, for example banks, everything should be done to ascertain their nature and location to the greatest possible extent.

Importantly, where a freezing injunction is obtained, the order applies not only to assets in the defendant's hands at the time it was granted but also to those which it acquires subsequently (*T.D.K. Tape Distributor (UK) Ltd v Videochoice Ltd* [1986] 1 W.L.R. 141).

Real risk of dissipation of assets. This requirement is fundamental to the freezing order. The claimant must prove that there is a 'real risk' that the defendant may remove from the jurisdiction, dispose of, dissipate or hide its assets in any way that will hinder enforcement of any judgment the claimant may obtain. The test is one of real risk, rather than probability of dissipation of assets (*Caring Together Ltd (In Liquidation) v Bauso* [2006] EWHC 2345 (Ch)).

Guidance on what a claimant is required to prove was given by Mustill J in *The Niedersachsen* [1983] 2 Lloyd's Rep. 600, at 606:

'It is not enough for the plaintiff to assert a risk that the assets will be dissipated. He must demonstrate this by solid evidence. This evidence may take a number of different forms. It may consist of direct evidence that the defendant has previously acted in a way which shows that his probity is not to be relied upon. Or the plaintiff may show what type of company the defendant is (where it is incorporated, what are its corporate structure and assets, and so on) so as to raise an inference that the company is not to be relied upon. Or, again, the plaintiff may be able to found his case on the fact that enquiries about the characteristics of the defendant have led to a blank wall. Precisely what form the evidence may take will depend upon the particular circumstances of the case. But the evidence must always be there. Mere proof that the company is incorporated abroad, accompanied by the allegation that there are no reachable assets in the United Kingdom apart from those which it is sought to enjoin, will not be enough'.

It may be easier for an applicant to establish a real risk of dissipation if it has established that there is a 'good arguable case' that the respondent has engaged in fraudulent/dishonest conduct (*VTB Capital plc v Nutritek International Corp and others* [2012] EWCA Civ 808).

Other relevant factors which the court may weigh in the balance include:

- the defendant has begun moving its assets out of the jurisdiction;
- any indication by the defendant to dispose of assets;
- the nature, value and location of the defendant's assets (the more liquid they are, the greater the risk of dissipation);
- the length of time the defendant has been in business (a defendant who has been in business for a long time is less likely to have adverse inferences made against it compared with a less established entity);
- the defendant's financial standing and credit history;
- any evidence of dishonesty by the defendant, particularly in relation to misuse of assets;
- any fraudulent failure to disclose assets;
- the defendant's conduct in relation to the present dispute and any previous disputes (for example, failing to answer reasonable questions or evading service);
- whether the defendant has the skills and experience to move and manage his assets abroad; and
- any delay on the part of the claimant in making the application for the relief (*Cherney v Neuman* [2009] EWHC 1743 (Ch).

Worldwide effect

In appropriate cases, a freezing injunction can be made in respect of assets outside the jurisdiction, to prevent the defendant from dissipating assets located abroad. This is known as a worldwide freezing injunction and may be granted where there are insufficient assets in England and Wales to satisfy any subsequent judgment.

The requirements for a worldwide freezing injunction are essentially the same as the requirements for domestic orders. One notable difference relates to the defendant's assets. Rather than having to demonstrate that the

defendant has assets within the jurisdiction, a claimant is required to show that any assets which are within the jurisdiction are insufficient to satisfy the claim and that the defendant has assets outside the jurisdiction. It may even be possible to obtain a worldwide freezing injunction over the assets of a company which had no significant presence within the jurisdiction (*Mediterranean Shipping Company v OMG International Ltd & others* [2008] EWHC 2150 (Comm)).

Where the court makes a worldwide order, the defendant requires extra protection from the risk of oppression, as it could potentially face proceedings in each jurisdiction where its assets are located. The standard freezing order therefore contains an undertaking that the claimant 'will not without the permission of the court seek to enforce this order in any country outside England and Wales or seek an order of a similar nature including orders conferring a charge or other security against the [Defendant] or the [Defendant]'s assets.'

In *Dadourian Group International Inc. v Simms & Others* [2006] EWCA Civ. 399 the Court of Appeal laid down guidelines (known as the Dadourian guidelines) for the court in considering whether to permit a party to seek to enforce a worldwide freezing order outside the jurisdiction. These guidelines are not intended to be exhaustive, and are not to be applied to the exclusion of any other relevant consideration.

The guidelines include: that the claimant's interests must be balanced against the interests of other parties to the English proceedings, or to third parties who may be joined to the foreign proceedings; that permission should not normally be given where this would enable the claimant to obtain relief in the foreign proceedings which is superior to the relief given by the worldwide freezing order (eg by obtaining priority over other creditors in the event of insolvency); and that the evidence in support of the application should contain all the information necessary to enable the judge to reach an informed decision, including evidence as to the applicable law and practice of the foreign court.

The process of enforcing a worldwide freezing injunction abroad can be problematic, and an applicant should consider seeking relief in the relevant jurisdictions directly. In the EU, while applicants may apply for recognition and enforcement of extra-territorial protective measures in accordance with Article 31 and Chapter III of the Brussels Regulation (44/2001/EC) (or the 2007 Lugano Convention (Lugano Convention)), such relief will not be available if the order was granted *ex parte* (C-125/79 *Bernard Denilauler v SNC Couchet Frères*). In jurisdictions outside the scope of the Brussels Regulation or Lugano Convention, the treatment of English worldwide freezing orders and the procedure for their recognition and enforcement will be a matter of local law, and local counsel should be consulted. The likelihood will be that a local injunction will be required (although such an application may be assisted by the existence of a similar order from the English High Court).

In *JSC BTA Bank v Ablyazov and others* [2009] EWHC 3267 (Comm), the Commercial Court granted a worldwide freezing order in terms that went beyond those in the standard form published in the Commercial Court's

guide and the CPR. In this case the claimant sought a variation of the standard form freezing order, to the effect that the defendant would not be able to deal with any assets outside England and Wales, unless they retained within the jurisdiction assets to at least a specified value. The defendants would therefore only be able to deal with their assets outside England and Wales if they transferred assets to the jurisdiction and left them there for the duration of the freezing order.

The court held that, in this case, there were good reasons to allow the freezing order to be varied beyond the scope initially envisaged, with the effect that greater protection would be afforded to the claimant. The court considered that there was a real risk that the defendant might use the right provided in the standard form freezing order to deal with overseas assets in a manner which put its assets out of the reach of the claimant, the very act which freezing orders are designed to prevent. Although it is not certain how this decision will be applied in future, it will be of tactical interest to parties seeking a freezing injunction.

A new EU regulation (Regulation (EU) 655/2014) creating a European Account Preservation Order (EAPO) came into force on 17 July 2014, and will apply from 18 January 2017 (with the single exception of Article 50, which will apply from 18 July 2016). It is designed to provide a more straightforward procedure to freeze a respondent's EU bank accounts, such that an EAPO raised in one member state would be recognised and enforced automatically in another. Under the regulation, an applicant will be able to freeze funds in the respondent's bank account up to a value equal to its debt plus interest and, if a judgment has been obtained, costs. The applicant will need to establish that there is sufficient evidence to satisfy the court that there is an urgent need for a protective measure and that, without the issue of the order, there is a 'real risk' that subsequent enforcement of an existing or future judgment against the defendant is likely to be impeded or made substantially more difficult. Where the applicant has not yet obtained a judgment, it will need to establish that it is 'likely to succeed' on the substance of the claim. The UK government has not yet opted into the regulation, although it has previously suggested it might consider a post-adoption opt-in.

Jurisdiction of the court: Freezing injunction in support of foreign proceedings

The court has power to grant interim relief, including freezing injunctions, in support of substantive proceedings brought in a foreign jurisdiction pursuant to section 25 of the Civil Jurisdiction and Judgments Act 1982 (as extended by the Civil Jurisdiction and Judgments Act 1982 (Interim Relief) Order 1997 (SI 1997/302)). In addition to satisfying the same basic criteria as is required for a freezing injunction in support of domestic proceedings, the claimant under section 25 must pass a test of 'expediency': the court may refuse to make an order if the fact that it has no jurisdiction over the substantive merits of the case makes it 'inexpedient' for the court to grant relief.

The factors which the court will consider in making this assessment were established by the Court of Appeal in *Motorola Credit Corporation v Uzan (No 2)* [2004] 1 W.L.R. 113. In summary, the court will consider whether:

- granting the order would interfere with the management of the case in the main court;
- it is the policy in the main jurisdiction to refuse to grant the relief sought;
- there is a danger that the order would give rise to confusion or disharmony and/or the risk of conflicting, inconsistent or overlapping orders in other jurisdictions;
- at the time the order is sought there is likely to be a potential conflict as to jurisdiction; and
- the order could be enforced (the courts will not grant an order if there would be no real sanction against the defendant for non-compliance).

These principles were considered in *Banco Nacional de Comercio Exterior SNC v Empresa de Telecommunicaciones de Cuba SA* [2007] EWCA Civ 662. The claimant had obtained an Italian judgment against the defendant. The judgment had been registered in the United Kingdom and the claimant had obtained a domestic freezing order followed by a worldwide freezing order. The defendant appealed against the worldwide order. The Court of Appeal considered the principles in *Motorola Credit Corporation* and gave the following reasons for deciding it would be inexpedient to uphold the worldwide order:

- the defendant was not domiciled in England and Wales;
- any assets in England and Wales were protected by the domestic order;
- the worldwide order was directed only at assets outside the jurisdiction (there was therefore no connecting link between the subject matter of the measure sought and the territorial jurisdiction of the court);
- it was not the policy of the Italian courts to grant worldwide freezing orders; and
- given the multiplicity of enforcement proceedings in other jurisdictions there was a danger that an English worldwide freezing order would give rise to disharmony or confusion or risk conflicting, inconsistent or overlapping orders in other jurisdictions.

Where the substantive action is proceeding in the courts of a state subject to the Brussels Regulation or Lugano Convention, Articles 31 and 24 respectively permit the courts of another member state to grant interim relief in support of those proceedings. The European Court of Justice in *Van Uden BV v KG Deco-Line* (Case c-391/95 [1998] ECR I-7091) has held that in such cases, there must be a 'real connecting link' between the subject matter of the proposed interim relief and the territorial jurisdiction of the court where the relief is sought. Accordingly, it is at least arguable that, in such cases, the English court can make freezing orders only in relation to assets situated in England and Wales, and may not make worldwide freezing orders.

In non-Brussels or Lugano cases, the courts appear to be more liberal. In *Mobil Cerro Negro Ltd v Petroleos De Venezuela SA* [2008] EWHC 532 (Comm), which concerned a worldwide freezing order made in support of foreign

(New York) arbitral proceedings, pursuant to the Arbitration Act 1996, the court refused to grant the application in the absence of any exceptional feature such as fraud or any link with England and Wales. Although the claimant was unsuccessful, the judgment suggests that where there are allegations of international fraud, the court may be more willing to assist a claimant whose claim lacks a territorial connection to England and Wales (*Mobil Cerro Negro* at paragraph 155; see also the comments of Field J in *USA v Abacha* [2014] EWHC 993).

The courts have been reluctant to grant worldwide freezing orders in aid of foreign proceedings where the defendant has no assets in England and Wales (see *Barwa Real Estate Company v Dean Rees* [2009] EWHC 2134 (QB) (Comm)), but in *Royal Bank Of Scotland plc v FAL Oil Company Ltd and others* [2012] EWHC 3628 (Comm) the court was willing to make such an order in circumstances where there was a 'real link or connection' with the jurisdiction (which in this case included bank accounts in the jurisdiction – albeit overdrawn).

Jurisdiction of the court: freezing injunction in support of arbitral proceedings

Unless otherwise agreed by the parties in writing, interim (including freezing) relief is also available in support of arbitral proceedings, under section 44 of the Arbitration Act 1996. That regime is based on similar considerations to those under section 25 of the Civil Jurisdiction and Judgments Act 1982. Specifically, in arbitral cases, the court may refuse to exercise its powers to grant relief if, in its opinion, the fact that the seat of the arbitration is/will be outside England and Wales, makes it 'inappropriate' to do so (section 2(3) Arbitration Act 1996).

Generally, unless the case is urgent, the claimant must first seek the leave of the arbitral tribunal to apply to court for an order. But if there is a real risk that the defendant will dissipate assets, the application process to the tribunal will be useless. In those circumstances, the claimant can apply to court directly. The court can then grant such orders as it thinks necessary for the purpose of preserving evidence or assets, including freezing relief. However, once it becomes practicable to obtain the leave of the tribunal, it should be sought promptly and, indeed, the claimant must seek that permission if the relief is to remain in force. Accordingly, where orders are made ex parte, the court may provide in the draft order that the order shall cease to have effect if the tribunal so orders.

The without notice application

To avoid the risk of the defendant frustrating the purpose of the freezing order, by disposing of its assets before the order is granted, applications for freezing orders are usually made without notice to the defendant. The defendant will have a later opportunity (at the 'return date') to seek to vary or discharge the order.

As part of the 'bargain' which the court strikes with the claimant for granting such far-reaching orders in this initially one-sided process, the

claimant must give what is termed 'full and frank' disclosure of all material facts and matters which might influence the court in deciding whether or not to grant the orders sought. This includes identifying any disputed facts, any arguments which might be advanced by the defendant, and any factors which might affect the court's discretion, including matters relating to the claimant's own conduct. Failure to comply with this duty can lead to the discharge of any order granted and an order that the claimant pay the defendant's costs on an indemnity basis. It is also likely to impair the claimant's credibility, which could damage an otherwise strong case.

The position of the defendant

The defendant is further protected by a cross-undertaking in damages, which the claimant must provide to obtain the injunction. This is an undertaking by the claimant that it will comply with any order compensating the defendant for any loss suffered, if it is later shown that the injunction should not have been granted. The court may require the claimant to give security in support of the undertaking, eg by bank guarantee (known as 'fortification' of the undertaking). The duty to provide full and frank disclosure extends to the cross-undertaking, such that the claimant has a continuing duty to draw any material change in its financial position to the defendant's attention, which relates directly to the claimant's ability to satisfy his cross-undertaking in damages (*Staines v Walsh* [2003] EWHC 1486 (Ch)).

A freezing injunction granted by the court is binding on any party who is subject to the court's jurisdiction, who is validly served with the order. Consequently, the order may not only affect the defendant but also any third parties who breach its terms. Indeed, it is a contempt of court for a third party knowingly to assist in a breach of the order or intentionally to frustrate the purpose of the order. The claimant should therefore serve the order on any banks or other third parties holding assets on the defendant's behalf, to prevent them assisting in their disposal.

The standard freezing injunction includes a disclosure provision obliging the defendant to swear an affidavit giving the value, location and details of its assets, either within the jurisdiction or, for a worldwide order, elsewhere. Such disclosure enables the claimant to identify the whereabouts of the defendant's assets and notify relevant third parties (especially banks). Where there are concerns about the veracity of the defendant's affidavit, the court may order it to submit to cross-examination in relation to its assets.

The proprietary order

In addition to a personal order preventing the defendant dealing with its own assets, a proprietary injunction may be granted where the claimant asserts that the defendant is holding property belonging to the claimant, ie cases where the claimant has a proprietary claim, such as, where the defendant has stolen its assets and remains in possession of them (or their traceable proceeds). In contrast to a personal order, a proprietary injunction will be granted over the specific assets to which the claim relates.

Due to the proprietary nature of this injunction, the claimant need not establish a risk of dissipation. Rather (see *Polly Peck International plc v Nadir* (No2) [1992] 2 Lloyd's Rep. 238):

- the claimant must establish an arguable case;
- once this has been established, the court should consider the balance of convenience; and
- when the balance of convenience is evenly balanced, the court should then take into account the merits of the claimant's case.

It can be good practice in appropriate cases to apply concurrently for both a proprietary injunction and a freezing injunction in order to take advantage of the benefits of both types of order. For example, both proprietary and freezing injunctions were granted in *Madoff Securities International Ltd v Raven and others* ([2011] EWHC 3102), due to uncertainty over whether the claimant would be able to identify and trace the specific assets that would be subject to the proprietary order.

4.2 The search and seizure order

The order

The second nuclear weapon in the claimant's arsenal is the search and seizure order. This is a form of mandatory interim injunction, which acts as a means of preserving evidence where there is a real risk that without the order such evidence would be destroyed. It requires the defendant to give the claimant's solicitors access to its premises to search for and seize specified evidence, eg documents, electronic data, etc. The purpose of the order, therefore, is to preserve evidence; search orders cannot be used as a means of obtaining evidence.

Although obtaining and executing a search order is likely to be an expensive process, it can give the victim of fraud an exceptional early advantage in any proceedings against the fraudster. Given its intrusive and even draconian nature, it is only available in very limited circumstances.

Applications for orders are made under CPR 23 and the additional procedural requirements under CPR 25 must be followed. Most applications are made before the issue of a claim, but a claimant may make an application for a search order at any stage during the proceedings. However, like the freezing order, a search and seizure order is an equitable remedy, so the claimant should apply for the order as soon as possible, as delay may jeopardise the claimant's application.

The defendant against whom a search order may be granted could be a company, an individual or a representative of a group of defendants, provided that the claimant has a cause of action against the whole group. The premises to be searched must be specifically identified in the search and seizure order and be under the defendant's control and in the UK. Where the court has jurisdiction over the defendant, however, the court may be able to grant a search and seizure order in respect of overseas premises, although this is still an evolving area and is very rare. No materials can be removed from the defendant's premises unless they are specifically identified in the order itself (CPR PD 25A.7.5(1)). This means that the order cannot include

a catch-all provision which would allow the claimant to remove material discovered during the search, but not specifically mentioned in the order. The types of materials that can be seized include documents, computer records and files and chattels or classes of chattels. As it is unlikely that all relevant information at the defendant's premises will be in hard copy form, the claimant should engage appropriate experts to assist with the execution of the order to ensure that all relevant evidence, including electronic evidence, is preserved. Importantly, legally privileged material cannot be removed (see section on privilege against self-incrimination below).

The test

The test the claimant must satisfy when applying for a search order was established in *Anton Piller KG v Manufacturing Processes Ltd and Others* [1976] Ch. 55, and extended by The Staughton Committee. There are four conditions:

- an extremely strong *prima facie* case;
- evidence of very serious damage (potential or actual) to its interests;
- clear evidence that the defendant has in its possession incriminating documents/materials and that there is a real possibility of the defendant destroying such material before any application *inter partes* can be made; and
- the harm likely to be caused to the defendant and its business affairs by the execution of the search order must not be excessive or disproportionate to the legitimate object of the order.

Further, the court must be satisfied that the order is just and convenient in all the circumstances.

Strong prima facie case. The courts are not inflexible when applying this rule, recognising that the evidence may be limited, or the full extent of the claim not known, at the time of applying for the search order. However, the courts will not grant an order where the claimant is on a 'fishing expedition' to determine whether there is a cause of action against the defendant; the claimant must hold more than a suspicion that there is a claim.

Very serious damage. The claimant must provide the court with evidence of what damage has happened, or what it believes will happen, because of the defendant's actions.

Real possibility of the defendant destroying the material. The courts accept that there may be no evidence that the defendant will destroy the material, but the claimant must show more than it is in the defendant's interests to do so. Where there is evidence of a serious fraud, the courts may be more willing to infer that the defendant would destroy the material to prevent the fraud being discovered. If the defendant has destroyed material in the past or has made comments that it will destroy the documents, then this will usually suffice.

Not excessive or disproportionate. If the court considers that the likely harm to the defendant is excessive or disproportionate to the legitimate object of the order, it will not grant the order. However, it may grant an alternative order to protect the claimant's position, eg a 'doorstep order', which requires

the defendant to disclose documents to the claimant's solicitors on service of the order at its premises, but which does not allow the claimant's solicitors access to the premises.

Procedural requirements

When applying for the search order, the claimant must follow the procedural requirements in CPR 23 and 25, as failure to follow these requirements may lead to the court discharging the search order. Essentially, a claimant has to file an application notice, supporting evidence and a draft order, together with the relevant court fee, at least two hours before the hearing, if there is sufficient time (CPR PD 25A.4.3(1)). Applications for search orders are invariably made without notice to the defendant, as giving notice would alert the defendant and defeat the purpose of the search. This means that the claimant will have an initial hearing in private with the judge, who will decide whether to grant the order. If the search order is granted, the court will fix a return date for an 'on notice' hearing, at which the defendant will be present. This is usually one week after the initial hearing, by which time the order will have been served on the defendant and the search already carried out. A report on the execution of the search will be presented to the court at the second hearing, and the court will consider whether the search order should be continued or varied. The costs of the application may also be dealt with at this stage.

Defendant's safeguards

There are safeguards in place to protect the defendant's position during this process. These include:

- the claimant's duty to make full and frank disclosure;
- the claimant's cross-undertaking in damages;
- an independent solicitor (known as the 'supervising solicitor') being appointed to supervise and report on the execution of the search; and
- the privilege against self-incrimination.

Claimant's duty to provide full and frank disclosure. As the application for a search order, like a freezing injunction, is typically made without notice, the claimant must disclose all matters that are material to the court's decision as to whether to grant the order, even if they are adverse to its own case. This duty includes drawing the court's attention to any matters about which the claimant knew or ought to have been aware with reasonable inquiry, any unusual provisions of the draft order and the defendant's likely defence to the allegations. Failure to satisfy these requirements may lead to the order being discharged and the defendant being awarded costs on an indemnity basis.

Claimant's cross-undertaking in damages. As with freezing orders, unless the court orders otherwise, the claimant must provide (CPR PD25A.5.1(1)) an undertaking to compensate the defendant for any damage it sustains for which the court considers the claimant should pay, for example, if the court subsequently determines that the search order should not have been granted, or that the execution of the order was in breach of the terms of the order. As with freezing orders, the cross-undertaking in damages may need to be

supported by security, where there is doubt over the claimant's ability to meet the undertaking. The undertaking is given to the court, not the defendant, and it is therefore at the court's discretion as to whether or not to enforce it.

The supervising solicitor. The supervising solicitor is an officer of the court, who must be independent of both the claimant and defendant and their respective solicitors. That solicitor must also be experienced in the operation of search orders (CPR PD25A.7.2). These requirements are intended to protect the defendant's rights, as the defendant is likely to have instructed its solicitor on very short notice, and the solicitor may have little or no experience of search orders. The supervising solicitor ensures that the search order is executed correctly. Typically they will serve the search order on the defendant and inform the defendant of their legal rights before the claimant enters the defendant's premises. The supervising solicitor must ensure that only material recorded in the order is removed. They must therefore list all material removed and give a copy of the list to the defendant (CPR PD25A.7.5(6)). The supervising solicitor must then provide a report to the claimant's solicitor on the carrying out of the search order. This report will be presented to the court. The court can then assess whether the claimant's search complied with the specific terms of the search order.

Privilege against self-incrimination. The defendant may seek to resist handing over material by relying on the privilege against self-incrimination. This allows a defendant to refuse to produce material/information which might incriminate it in criminal proceedings, or expose it to a penalty in England and Wales. The right is based on common law privilege and section 14(1) of the Civil Evidence Act 1968. The supervising solicitor must inform the defendant that it has this right before the claimant enters the defendant's premises, providing a powerful safeguard for the defendant.

There are, however, two recent developments which have limited the circumstances in which the defendant can claim the privilege against self-incrimination. First, there are statutory exceptions, notably section 13 of the Fraud Act 2006, which disapplies the privilege in relation to that Act and related offences (including bribery). Secondly, the Court of Appeal has recently cast doubt on the extent to which a defendant can rely on the privilege to avoid handing over potentially incriminating material that came into existence separately from any compulsory powers under the search order (*C Plc v P* [2007] EWCA Civ 493). The application of the privilege against self-incrimination to free-standing evidence has previously received considerable judicial attention (see, for example, *Saunders v United Kingdom* [1996] ECHR 19187/91 and *AG's Reference (No 7 of 2000)* [2001] EWCA Crim 888). Commentators and the courts have generally tended to take the view that independent, non-testamentary evidence already in existence should not benefit from the privilege, because such evidence will 'speak for itself', and there is no risk of the defendant being coaxed into making a false confession. This is more clearly the case in the context of a search order rather than ordinary disclosure under the CPR, pursuant to which the defendant would have to testify that the incriminating documents exist or have existed. In *C Plc v P*, a search order was granted in a claim for breach

of confidence and copyright infringement. When the order was executed, the supervising solicitor passed computers to an independent expert for the purpose of imaging the contents. The expert uncovered highly objectionable images of children. He applied to court for directions as to what it should do with the offending material.

At first instance it was held that the domestic law of privilege against self-incrimination should be amended to enable this material to be transferred to the police. The material was 'free standing evidence'; the defendant had not created it under compulsion of the court order.

The Court of Appeal upheld the first instance decision with the effect that the offending material which existed independently of the search order was not protected by the privilege. However, the court emphasised that its decision related specifically to the context, ie an application by a third party computer expert. The court did not consider it necessary to find, as a general rule, that there was no privilege in respect of pre-existing or independent material. Nevertheless, it is likely that defendants may encounter difficulties in successfully asserting privilege in the context of self-incriminating 'independent' material that comes to light during the course of a search order.

Moreover, in a plain-speaking and direct judgment, the Court of Appeal in *JSC BTA Bank v Ablyazov & Others* [2009] EWCA Civ 1125 refused an appeal against an order of the English High Court that certain defendants subject to a freezing order must disclose their assets to the court. The defendants sought to rely on the privilege against self-incrimination, asserting that the information provided would be used against them in Kazakhstan. Their argument found no favour with the Court of Appeal, which made interesting observations on the privilege. The case is noteworthy because of the court's apparent irritation at the attempt to use a long-standing shield as a sword. Had the defendants succeeded with their argument, the privilege would not only have protected the defendants from their alleged concerns about Kazakh justice, but also acted as a virtual knock-out blow to the claimant's case, thereby preventing the bank from vindicating its rights. Even if the claim were likely to be successful, it would most probably not have been worth pursuing in the absence of disclosure of the assets, or its value would at least have been severely diminished.

There are other limitations for a claimant when seeking and executing a search order. For example, the grant of a search order does not allow forced entry to the defendant's premises. If the defendant chooses to disobey the order, the claimant's only remedy is through contempt proceedings (the search order must contain a penal notice stating that the defendant will be in contempt of court if he breaches the order). Where the defendant disobeys the order, it is possible that documents may have been destroyed or hidden. Even if access to the premises is granted, there is no guarantee that probative documents will be found.

Gagging orders

Search and seizure orders usually contain a provision preventing the defendant from discussing the order with anyone but its solicitor. This is

designed to aid the preservation of evidence and ensures that the defendant cannot inform anyone that the proceedings exist, or that an order has been made. The provision is of greatest importance where proceedings against multiple defendants could be weakened by the first defendant forewarning other defendants of impending searches. Due to the draconian nature of the gagging order, it is unlikely to be granted for any more than a few days.

Delivery-up of passport

An order for delivery-up of passport can be made with a freezing or search and seizure order. It provides that the defendant should deliver its passport to the supervising solicitor until the court orders otherwise. This ensures that the defendant cannot leave the jurisdiction, and applies pressure to comply with the principal order. The effectiveness of this order has increased in the era of the multi-national company where even relatively junior figures cannot work effectively without the ability to travel.

5. CIVIL PROCEEDINGS

English law has developed over centuries to strive to assist victims of fraud. In doing so it has taken a flexible and creative approach to the application of legal principles, highlighted for example by the development of constructive trusts, and the evolution of interim remedies such as the freezing injunction and search order. This section outlines the principal claims and remedies available to a victim of fraud seeking redress against the wrongdoer(s).

Breach of trust/fiduciary duty

The notion of a 'trustee' or 'fiduciary' in English law is very broad and is pivotal to many fraud remedies. The concept is best summarised in the following passage of *Bristol and West BS v Mothew* [1998] Ch. 1 at 18:

'A fiduciary is someone who has undertaken to act for or on behalf of another in a particular matter or circumstance which gives rise to a relationship of trust and confidence. The distinguishing obligation of a fiduciary is the obligation of loyalty. The principal is entitled to the single-minded loyalty of his fiduciary.'

There are a number of established categories of fiduciary in English law, including an agent acting on behalf of its principal and a lawyer acting on behalf of its client. All fiduciaries are subject to certain implied duties arising from their position:

'A fiduciary must act in good faith; he must not make a profit out of his trust; he must not place himself in a position where his duty and his interest may conflict; he may not act for his own benefit or the benefit of a third person without the informed consent of his principal. This is not intended to be an exhaustive list, but it is sufficient to indicate the nature of fiduciary obligations. They are the defining characteristics of the fiduciary.'

There are a number of personal and proprietary remedies available where there has been a breach of trust or fiduciary duty. Thus, where there has been a breach of trust, the trustee/fiduciary can (among other things) be liable to compensate its principal for the losses suffered, to remedy the

breach by being made to account for the losses and, possibly, to account for any profits made by the trustee as a result of the breach. In addition, the injured beneficiary may attempt to follow or trace the trust property or its proceeds in order to assert an equitable proprietary interest over the same. The concepts of following and tracing are discussed in greater detail below.

Assisting in the breach: knowing receipt/dishonest assistance

There are two distinct causes of action entitling a claimant to sue a 'stranger' (ie a third party who does not owe pre-existing fiduciary duties to the claimant) in respect of another's breach of trust or fiduciary duty: knowing receipt and dishonest assistance. In each case, the third party wrongdoer is liable to account as if it were a trustee or fiduciary.

Knowing receipt is concerned with the liability of a third party who receives trust property or its proceeds, knowing that it was transferred in breach of trust, or who receives misdirected assets which were controlled by a person who owed fiduciary duties in respect of its handling of those assets. The recipient's state of knowledge must be such as to make it unconscionable for it to retain the benefit of those transferred proceeds. In these circumstances both a proprietary and a personal claim will lie against the knowing recipient, even if it is no longer in possession of the trust property or misdirected assets. It should be noted that dishonesty on the part of the third party is not required to establish liability for knowing receipt.

In contrast, dishonest assistance does not depend on establishing that the third party actually received any trust property. The test has three elements:

(i) a breach of trust or fiduciary duty, causing or resulting in loss;
(ii) assistance in that breach of trust or fiduciary obligation by the defendant; and
(iii) dishonesty on the part of the defendant.

One of the leading cases on dishonest assistance is *Royal Brunei Airlines Sdn Bhd v Tan* [1995] 2 A.C. 378. The case established that 'dishonest' in this context means 'not acting as an honest person would in the circumstances'. Assessing dishonesty is largely objective. The relevant question therefore is whether the defendant fell below the standard of ordinary honest people. It does not matter whether the defendant was conscious of that standard or that its conduct fell below it. However, there is also a subjective element in that the court must have regard to what the defendant actually knew and understood at the time, rather than what a reasonable person would have known. It should be noted that liability for dishonest assistance does not require that the trustee itself should have been dishonest. For a more recent discussion on the meaning of 'dishonest' in this context, see the judgment of the Court of Appeal in *Starglade Properties Ltd v Roland Nash* [2010] EWCA Civ 1314.

The remedies available against strangers are identical to the remedies available against a trustee or fiduciary. As a result, dishonest assistants and knowing recipients can be ordered to account for the value of misapplied property, account for profits (where these exist), pay a measure of

compensation equivalent to what a trustee or fiduciary would be required to pay and so on.

Conspiracy

A victim of fraud may also have a claim in the tort of conspiracy where it can establish that the defendants conspired to injure it. This allows the claimant to cast its net more widely against a number of defendants, even though it might not otherwise have a direct cause of action against all of them.

The tort has two forms: conspiracy by lawful means, in which case the claimant must also establish the defendant's predominant intention to injure it; or conspiracy by unlawful means, where the claimant must establish the defendant's intention to injure, though not necessarily a predominant intention. The first tort is rarely seen in practice. In the second, 'unlawful means' will be established where the claimant has an actionable claim against one or more of the conspirators in respect of the unlawful means used (this will generally be so in cases of fraud), but also where one or more of the conspirators has been guilty of criminal conduct which is intended to and does in fact cause loss to the claimant.

Deceit/fraudulent misrepresentation

Where a party makes a false representation, knowing it to be untrue or being reckless as to whether it is true, intending that the claimant rely on that representation, it will be liable if the claimant so relies and suffers loss. This is the tort of deceit, or fraudulent misrepresentation.

In order for the claimant to establish a common law claim in deceit, the following must be established (as recently confirmed by the Court of Appeal in *Eco 3 Capital Ltd and others v Ludsin Overseas Ltd* [2013] EWCA Civ 413):

- There must be a representation of fact made by words or conduct.
- The representation must be made with knowledge that it is or may be false. It must be wilfully false, or at least made in the absence of any genuine belief that it is true.
- The representation must be made with the intention that it should be acted upon by the claimant, or by a class of persons which includes the claimant, in the manner which resulted in damage to it.
- It must be proved that the claimant has acted upon the false statement.
- It must be proved that the claimant suffered damage by so doing.

Where fraud cannot be established, there may in appropriate circumstances be a claim for negligent misrepresentation, but the measure of damages tends to be more generous in fraud cases; in such a case, 'the plaintiff is entitled to recover all his loss directly flowing from the fraudulently induced transaction. In the case of a negligent misrepresentation the rule is narrower: the recoverable loss does not extend beyond the consequences flowing from the negligent misrepresentation.' *Smith New Court Securities Ltd v Citibank* [1997] A.C. 254 at 283. For a more recent case which emphasised the extent of the damages possible in cases of fraudulent misrepresentation, see *Parabola Investments Ltd v Browallia Cal Ltd* [2009] EWHC 901 (Comm); [2009] 2 All E.R. (Comm) 589.

There is also a statutory base in English law for suing in misrepresentation, under the Misrepresentation Act 1967. This allows the innocent party to rescind the contract and, where the defendant cannot demonstrate a belief in the representation at the time it was made, claim a measure of damages commensurate with the level of damages available in fraud cases. This route is often preferable to suing in fraud because of the high hurdle (discussed above) required to prove fraud and because of the reversed burden of proof.

Proprietary remedies: following and tracing

A victim of fraud has a proprietary remedy against a third party who has received property transferred in breach of trust and who still retains either the trust property or its proceeds, unless the third party is a *bona fide* purchaser for value without notice of the breach of trust. This means that the claimant can recover the actual trust property, or its proceeds from the third party. The main advantage of bringing a proprietary claim is that, in contrast with personal claims, it gives the claimant priority over other creditors in the event of the defendant's insolvency.

Proprietary remedies are assisted by the English law rules of 'following' and 'tracing', most simply defined as 'a process whereby assets are identified' (*Foskett v McKeown & Others* [2001] 1 A.C. 102 at 109). Following and tracing are not claims or remedies in themselves, but rather a series of complicated evidential rules allowing a claimant to identify its property or its proceeds for use in the claim. Where a fraudster has transferred the claimant's asset to a third party, the claimant generally has a choice: it may recover the asset from the third party (assuming it was not a *bona fide* purchaser for value without notice) by 'following' it into their hands; or, if the fraudster obtained value for the transfer of the asset, the claimant may be able to 'trace' into the proceeds of sale or the new asset which the fraudster obtained from the third party.

Where there has been a mixing of funds, complicated rules apply to ascertain the claimant's share of the fund or any asset purchased with it. Although it is difficult to navigate through these rules, they generally favour the victim of a fraud.

6. ANTI-BRIBERY/ANTI-CORRUPTION LEGISLATION

Bribery

The Bribery Act 2010 repealed all existing legislation and reshaped the laws on bribery in England. The Bribery Act 2010 received Royal Assent on 8 April 2010, and the offences created by it have been in force from 1 July 2011. The four new offences created by the Bribery Act 2010 are set out in the paragraphs that follow.

First offence: bribing another person. A person is guilty of this offence where that person promises, offers or gives another person a financial or other advantage either:

(i) intending the advantage to induce a person to perform improperly a relevant function or activity; or

(ii) intending the advantage to reward the performance of such a function or activity; or
(iii) knowing that the acceptance of the advantage would itself constitute the improper performance of a function or activity.

Second offence: receiving bribes. A person ('R') is guilty of this offence where:

- R requests, agrees to receive, or accepts a financial or other advantage intending that a relevant function or activity should be improperly performed by R or any other person; or
- R requests, agrees to receive or accepts a financial or other advantage where the request, agreement or acceptance itself constitutes the improper performance by R of a relevant function or activity; or
- R requests, agrees to receive or accepts a financial or other advantage as a reward for the improper performance of a relevant function or activity by R or any other person; or
- R or any other person (at R's request or with their assent or acquiescence), in anticipation of, or in consequence of R requesting, agreeing to receive or accepting a financial or other advantage, improperly performs a relevant function or activity.

In respect of the first two offences, 'relevant function or activity' refers to functions of a public nature, or activities connected with a business, trade or profession, or activities performed in the course of a person's employment or on behalf of a body of persons (including unincorporated bodies).

For the purposes of the first two offences, 'improper performance' is judged first by whether the person performing the function or activity was expected to perform it in good faith, or impartially, or was in a position of trust. It is then necessary to consider whether the performance is in breach of the relevant expectation, or whether there is a failure to perform the function or activity and that failure is itself a breach of the relevant expectation.

Third offence: bribery of foreign public officials. There are four parts to this offence:

- the briber (P) must intend to influence the foreign public official (F) in their capacity as a foreign public official;
- P must intend to obtain or retain business or an advantage in the conduct of business;
- P must directly or through a third party, offer, promise or give an advantage to F or to another person at F's request or with F's assent or acquiescence; and
- an offence is not committed if F is permitted or required under applicable written local law to be influenced in their capacity as a foreign public official by the offer, promise or gift.

Fourth offence: corporate offence – failure of commercial organisations to prevent bribery. A corporate body or partnership is liable where:

- A person (A) is performing services for or on behalf of the commercial organisation (C);

- C is either a corporate body or a partnership which is incorporated or formed in the UK, or which carries on a business or part of a business in the UK;
- A bribes another, intending to obtain or retain business or an advantage in the conduct of business for C; and
- C is unable to make out the defence of having in place adequate procedures designed to prevent persons associated with it from engaging in bribery.

All of the new offences have extra-territorial application. As a result, the offences may be prosecuted, if committed by a British national or corporate, or by a person ordinarily resident in the UK, regardless of where the act or omission which forms part of the offence took place. The Bribery Act 2010 also raised the maximum jail term for bribery by an individual from seven years to 10 years and a company convicted of bribery or failing to prevent bribery could receive an unlimited fine.

Financial recovery from the agent/employee

In addition to the new Bribery Act (which governs criminal sanctions for bribery), English civil law has an established regime to deal with bribery. A principal who discovers that his agent or employee has been bribed has several remedies against that bribed agent and party paying the bribe.

It is well-established under English case law (*Industries & General Mortgage Co. Ltd* v *Lewis* [1949] 2 All ER 573) that a bribe/payment of a secret commission arises when a person:

(i) makes a payment to the agent of a counterparty/principal;
(ii) knowing that that person is the agent of the counterparty; and
(iii) fails to disclose the payment to the counterparty.

If the principal can establish the first three points, the law makes an irrebuttable presumption that the party paying the bribe did so to cause the agent to act favourably to him, and also that the agent was actually influenced by the bribe. The essence of the bribe is the agent's conflict of interests.

The agent cannot avoid liability by arguing that the payment is governed by a foreign law with no civil law consequences. The English courts will not apply a foreign law if to do so would conflict with principles of domestic public policy.

There are two routes of recovery along which the wronged principal can proceed against the agent: common law damages and equitable remedies.

In each case, the principal cannot recover twice; he can seek damages or recovery of the bribe, but not both. However, the principal does not have to make this election until he is at a stage when he can enter judgment on one of the remedies.

Damages

The law presumes that 'the price is loaded as against the principal at least by the amount of the bribe' in any contract entered into as a result of the bribery (*Industries & General Mortgage*, above). In other words, there is a presumption that the principal has suffered financially at least to the value

of the bribe. In addition to recovery of that sum, the law also allows a right to extensive damages for a principal whose agent has been bribed, similar to those found in deceit cases, in respect of other damage suffered by the principal as a consequence of the bribe. This includes damages for the principal having been induced to enter into a less advantageous contract than he otherwise would as a result of the agreement negotiated by his bribed agent (*Fyffes Group Ltd v Templeman* [2000] 2 Lloyd's Rep. 643). As is the case with deceit cases, the defence of contributory negligence will not be open to the defendant (*Corporacion National del Cobre de Chile v Sogemin Metals Ltd* [1997] 1 WLR 1396). However, when it comes to assessing the measure of damages, the law will take account of whether the principal would have entered into the contract in any event (*Fyffes Group*, above).

Other remedies

Where there is a contract in place between them, such as an employment or service contract, the principal will also be entitled to recover damages for breach of contract from the bribed agent. This claim is premised on the agent breaching either the expressed or implied terms of the contract in accepting the bribe, or acting in breach of his duty of good faith and loyalty to his employer.

The principal is also entitled to recover the value of the bribe from the agent, on the basis that the bribe is money had and received to the principal's use. In these circumstances, the principal is not required to prove loss caused by the bribe; nor is he required to show that the bribed agent owes to him a fiduciary duty. It is sufficient that the bribes are paid to the agent (*Mahesan v Malaysian Government Officers' Co-operative Housing Society* [1979] AC 374). The principal will also be able to recoup the value of the bribe from the briber on the same basis (*Salford Corporation v Lever (No.2)* [1891] 1 QB 168). This will assist the principal where he cannot recover from an insolvent agent.

If the bribed agent is in a fiduciary position at the time when the bribe is received, he is obliged to disgorge the amount of the bribe to the principal. As before, the claimant does not need to prove any loss. The recent Supreme Court case of *FHR European Ventures LLP and others v Cedar Capital Partners LLC* [2014] UKSC 45 has clarified that a bribe or secret commission is held on constructive trust by the agent for the principal, and that the principal therefore has a proprietary claim to the bribe or secret commission. The practical effect of this decision is extremely important because, in the event of the agent's insolvency, the principal's claim will rank above that of other creditors, and the principal will be able to trace the funds into the hands of knowing recipients. The decision overrules the recent Court of Appeal decision in *Sinclair Investments (UK) Ltd v Versailles Trade Finance Limited (In Administration)* [2011] EWCA Civ 347.

Where the agent is a fiduciary, the principal may also pursue the bribing party in a personal claim for dishonest assistance in a breach of trust. This arises because the briber is inducing the agent to breach his fiduciary duty to the principal. The basis of such a claim is discussed earlier in this chapter.

The principal whose agent has been bribed may rescind all transactions between the principal and the briber, or company associated with him, where the bribe is given in respect of the contract between the claimant and the briber. Any money legitimately paid under the contract by the principal will be recoverable up to the date where the bribe has been disclosed to the principal. Of course if the principal is 'locked in' to a fraudulent transaction into which he would not otherwise have entered, it is likely that the briber will be liable for extensive damages (see *Parabola* below). This is because the basis of the rescission is essentially that the briber has fraudulently induced the principal to enter into the contract, albeit without an express representation (ie deceit).

Competitor claims

In some circumstances, it may be possible for a company to bring a 'follow-on' claim for damages against a competitor which it suspects of bribery. For example, a case has recently been brought against Innospec by Jalal Bezee Mejel Al-Gaood & Partners, a Jordanian firm, for US$42 million in respect of bribes allegedly paid by the defendant to a Middle Eastern Oil Ministry. The claim is for a conspiracy to injure by unlawful means (see above). In order for such a claim to succeed, it will be necessary to establish an intention to injure the competitor. This may be difficult for a claimant to prove, as it will not be sufficient to establish that the bribe was merely likely to injure the claimant.

Although, in *Innospec* [2014] All ER (D) 230 (Oct), the claim is being brought by only one competitor, it is possible that multiple competitors could potentially bring multiple claims in respect of one act of bribery (even though only one of them would have secured the contract) – so it is possible that a number parties had a 'lost opportunity' in respect of the relevant contract.

While cases of this type are still unusual, follow-on claims for damages in competition cases have become increasingly common in recent years, and this may indicate that similar claims in respect of alleged bribery might also become a more regular occurrence.