International Fraud & Asset Tracing

This is a timely and important book. Hard-hitting regulatory powers are on the increase and the appetite to use them grows. Multi-national corporations are struggling to grapple with cross-border legal problems arising from fraud, particularly when fast-moving issues need to be addressed in a timely and effective manner in order to avoid extreme financial and reputational consequences.

An in-house lawyer who wants to find out, lawfully, whether or not there has been corrupt conduct by a foreign subsidiary, or whether an internal investigation should be launched, will need help in not tripping up over the differences in foreign legal systems, while trying to gather information. This book provides that help. It is detailed, it is helpful, it is good guidance.

This volume will be a valuable resource to practitioners who may need to find an answer to a question arising in one of the 24 countries covered.

THIRD EDITION 2015

International Fraud & Asset Tracing

General Editor: Simon Bushell, Latham & Watkins

THE EUROPEAN LAWYER REFERENCE

International Fraud & Asset Tracing

Jurisdictional comparisons **Third edition 2015**

General Editor: Simon Bushell, Latham & Watkins

THE EUROPEAN LAWYER REFERENCE

International Fraud & Asset Tracing

Jurisdictional comparisons **Third edition 2015**

General Editor: Simon Bushell, Latham & Watkins

THOMSON REUTERS

General Editor
Simon Bushell, Latham & Watkins

Commercial Director
Katie Burrington

Commissioning Editor
Emily Kyriacou

Publishing Assistant
Nicola Pender

Design and Production
Dawn McGovern

Editing and Typesetting
Forewords

Published in December 2014 by European Lawyer Reference Series,
Friars House, 160 Blackfriars Road, London SE1 8EZ
part of Thomson Reuters (Professional) UK Limited
(Registered in England & Wales, Company No 1679046.
Registered Office and address for service:
Aldgate House, 33 Aldgate High Street, London EC3N 1DL)

A CIP catalogue record for this book is available from the British Library.

ISBN: 9780414035232

Thomson Reuters and the Thomson Reuters logo are trade marks of Thomson Reuters.

Crown copyright material is reproduced with the permission of the Controller of HMSO and the Queen's Printer for Scotland.

Contents

Foreword

Lord Gold, David Gold & Associates

As global trade and interconnectivity continues to intensify, with large commercial groups utilising complex structures across multiple jurisdictions, responding effectively to the discovery of wrongdoing has become ever more difficult. At the same time, an increasingly active international regulatory environment, under which companies have been facing severe civil and criminal penalties (not to mention follow-on civil litigation), only serves to underline the importance of navigating the relevant legal regimes correctly. It is necessary for anyone tasked with advising on such matters to familiarise themselves with the key legal issues relating to corporate fraud and corruption in each of the jurisdictions in which their clients operate. This book will be of great assistance in that regard.

Numerous recent examples highlight the potential consequences where companies fail sufficiently to prevent, investigate, report and/or remedy fraudulent or corrupt activity. The collapse of MF Global in late-2011 took place in the context of allegations of financial misconduct, including dipping into client accounts to make up for its own funding shortfalls, and this has resulted in a number of civil and criminal actions against former officers and the company itself. More recently, the Banco Espirito Santo group in Portugal has collapsed amid accusations of serious financial irregularities, leading to its healthy assets being stripped out into a 'good bank' established by the Portuguese regulators. The huge fines imposed on several banks as a result of the recent Libor scandal, as well as the $490m fine against GlaxoSmithKline in China following serious bribery allegations, serve as further stark reminders of the severity of the potential repercussions that companies can face for unlawful activity. It is clear that this book, which attempts to address corporate fraud and corruption at an international level, has become even more relevant since the publication of the second edition. This has given rise to a need to update and expand the publication. This third edition deals with the major legal developments in the last three years, and there are new chapters covering several important jurisdictions, notably the USA, as well as current and emerging economic powers: Canada, India, and Nigeria and a number of smaller but strategically significant jurisdictions: The Bahamas, Cyprus, Gibraltar, Ireland and Kazakhstan.

Helpfully, and in common with previous editions, the chapters follow a common structure, addressing the following key areas: the management of the internal investigation, obtaining disclosure from third parties, steps that a victim of fraud might take to preserve assets and evidence, causes of action available to a victim of fraud, and anti-bribery/corruption legislation.

The management of an internal investigation in particular is a difficult and sensitive process which requires an appreciation of different legal nuances across the various jurisdictions in which the investigation is to take place. This is no easy task given the number of legal issues that can arise during the course of an investigation. The investigators must ensure that their activities, which will likely include interviews with employees and (if possible) a review of their emails and other communications, are conducted in accordance with applicable data protection, privacy, human rights and employment laws. These can differ widely between jurisdictions, and investigators must not fall into the trap of assuming that the satisfaction of one country's requirements will suffice elsewhere – any failure to navigate the different national rules correctly could result in any evidence obtained being deemed inadmissible, and/or sanctions being imposed on the company itself. Similarly, the rules regarding legal privilege, including the types of communications that can attract privilege and the circumstances in which privilege will be waived, can vary markedly across jurisdictions. Some countries also have strict rules prohibiting 'tipping-off' employees before the authorities have had a chance to seize evidence, with civil and criminal sanctions for non-compliance. A detailed multi-jurisdictional guide such as this will be an invaluable resource for anyone seeking to address these difficult issues.

An issue of increasing prominence in a number of jurisdictions is whether a company (or its employees) should take advantage of leniency regimes by disclosing details of wrongdoing and so seek relief from prosecution and/or other sanctions. Following a number of high-profile corporate scandals and collapses, authorities in various jurisdictions have taken steps to encourage and incentivise whistleblowing and self-reporting. The US has strengthened its whistleblower regime in recent years, and in the UK the new Director of the Serious Fraud Office, David Green CB QC, has reached out to the business community to encourage self-reporting, stressing in a speech in October 2013: *'If a company made a genuine self-report to us … in circumstances where they were willing to cooperate in a full investigation and to take steps to prevent recurrence, then in those circumstances it is difficult to see that the public interest would require a prosecution of the corporate.'* Similar trends can be observed elsewhere.

Another important development has seen competitor businesses sue their rivals for damages where the latter have been found to have engaged in corrupt practice for example in the course of a public procurement process. Such claims have been seen in the US for a number of years (the Compass Group reportedly reached a substantial settlement with two rival companies in 2006 after it was investigated for alleged bribery to secure commercial contracts). 2014 saw the first follow-on damages claim of this sort in the English Courts brought against Innospec which was accused by a Jordanian competitor of having conspired to use unlawful means in allegedly paying bribes to a Middle Eastern Oil Ministry. While such claims will often be difficult (in particular, it will not be straightforward for the claimant to establish that the alleged bribery caused it to incur loss), this

is a development of which practitioners should be keenly aware and the risk of such claims being brought by competitors may factor into their considerations when deciding whether to admit guilt and reach a settlement with national authorities.

Finally, the coming into force of the Bribery Act 2010 in the UK has been a highly significant development with international repercussions, setting a 'gold standard' for anti-corruption regulation. The Bribery Act is extraterritorial in scope (much like the Foreign Corrupt Practices Act of 1977 (FCPA) in the US and goes further in outlawing facilitation payments), and creates offences not just for the giving and receiving of bribes, but also in respect of a failure by commercial organisations to prevent bribery. This requires companies to take a pro-active approach and it is therefore more important than ever for international companies (and particularly those operating in markets known to be high risk for bribery and corruption) to establish robust compliance mechanisms. Although the Bribery Act has given rise to little significant enforcement activity so far, this is likely a result of the complex nature of regulatory investigations and practitioners would be wise not to assume that the UK authorities will be in any way reluctant vigorously to enforce their new powers.

As someone with years of experience advising and working with large corporate entities to investigate and litigate frauds and to strengthen governance and compliance functions and more recently as monitor of BAE Systems plc (appointed by the US Department of Justice), I found this book highly informative and timely. I worked alongside the book's General Editor, Simon Bushell, whilst we were both partners at Herbert Smith. Simon is a leading practitioner in this area, and he has pulled together, in this third edition of *International Fraud and Asset Tracing*, a book which is accessible, detailed and clearly structured, enabling easy comparisons between different jurisdictions. It will be an important resource for both in-house and external counsel advising on international fraud and corruption.

Lord Gold
Solicitor and strategic consultant
US Department of Justice Monitor of BAE Systems plc
Formerly Head of Litigation and Senior Partner of Herbert Smith
info@davidgoldassociates.com

Sweden

Delphi Peter Skoglund*

1. INTRODUCTION

The overall context

Issues over internal fraud and not least corruption have remained important and at the forefront of the legislator's and the general public's attention for many years. The legal and policy fights against corruption have, however, never been more important than they are today.

For instance, the European Commission has calculated that, in the EU alone, each year, an estimated EUR 120 billion is lost to corruption.

As an illustration of the importance of issues concerning internal fraud and graft, and also as an illustration of what may happen when a company's probe into allegations of wrongdoing itself goes wrong and when the probe becomes as equally troublesome as the underlying issues, the recent and still pending case over the Chinese bribery claims made against GlaxoSmithKline deserves mention.

As reported by the media, this case includes all the ingredients to intrigue and capture the interest of the general public, including not only claims of millions of dollars allegedly having been funnelled to Chinese doctors and officials for many years, but also a suspected whistleblower, possibly with a private axe to grind, a corporate detective detained by Chinese authorities for almost a year, a smear campaign, covert camera surveillance, other dirty tricks and a sex video.

Another, very different but more positive, example is when, on 1 July 2014, on the occasion of the first plenary session of the new European Parliament, Transparency International, the global civil society organisation fighting corruption, launched an initiative against corruption, calling for new standards of integrity and transparency and asking members of the Parliament to sign a EU Anti-Corruption Pledge.

According to Transparency International, the aim of the EU Anti-Corruption Pledge is to get the MEPs to commit to greater integrity and transparency in EU law-making, prevention of corruption in EU funding and better protection for whistleblowers. In the words of Carl Dolan, Director of the Transparency International EU Office, 'the stakes are high'.

This initiative as such is positive, but it should be a concern that, in 2014, such an initiative is still deemed necessary.

In 2010, the international consultancy firm EY published a report, based on interviews with 1,400 managers at large international companies in 36

* Jacob Öberg co-authored the original article upon which this article is based, which appeared in the second edition of this book.

countries, where one-third of the Swedish managers interviewed reported that their companies had experienced problems with fraud and corruption. By comparison, the average number of companies in the study that testified about such problems was 21 per cent, up from 10 per cent only one year earlier. In a 2013 follow-up report by EY, based on 3,000 interviews, 12 per cent of the Swedish respondents believed that bribery and corruption were widespread in Sweden.

In Transparency International's 2013 Corruption Perceptions Index, Sweden ranks as the third least corrupt country, meaning that, despite the opinions polled by EY, all is not bad, or that other countries are far worse off.

2. MANAGING THE INTERNAL INVESTIGATION

Any investigation into a case of suspected internal fraud will entail a number of necessary and important considerations. The individual service contract with the employee being the target of the investigation and, when applicable, the collective bargaining agreement with the employee's trade union organisation, as well as the company's internal policies, must be observed and adhered to. Investigations that contravene rules or guidelines so established will rarely survive legal scrutiny. Other important considerations relate to the integrity of the investigation so as to avoid unnecessarily exposing the company to third party claims. Also, the objective of conducting an efficient investigation must not distract the investigator and cause fundamental privacy rights to be trampled on.

A recent example is the already mentioned GSK case, where, based on what has been reported, GSK's probe seems to have focused more on the whistleblower than on the actual problem – the corruption allegations. As a result, GSK faces almost as many questions about the way it conducted its investigation and about general corporate governance issues as about the bribery claims themselves. If there is a fire, one should not use gasoline when trying to extinguish it.

Pipeline legislation

The protection of an employee's right to privacy in the workplace has been widely discussed in Sweden for many years. As earlier reported by this author, in 2009, a governmental committee presented a proposal for an act on the Protection of Personal Privacy in Working Life (SOU 2009:44; the Government Memorandum). The committee's proposals, which have yet to result in an act of parliament, include specific rules on employee surveillance, on the processing of personal data and on the employer's obligation to negotiate with the employees' labour organisations before implementing any such measures. The committee's proposals were welcomed by several employees' labour organisations but opposed by employers' organisations. The incumbent government has declared that it will not propose any such legislation as advocated by the committee. However, 2014 is an election year and, depending on the election results, an Act of Parliament may still happen. Also, although it may be the destiny

of the committee proposals never to be passed into law, the Government Memorandum may still be educational.

On a related subject, camera surveillance, a new and modernised Act (SFS 2013:460) was passed in the last year and the express aim of the new law, which merges rules on camera surveillance with rules on the protection of personal data, is to better balance the legitimate use of camera surveillance, for instance as a crime investigation tool, and the protection of the individual's personal integrity.

The Swedish government has recently decided to initiate a process of making political money more transparent and possibly to forbid parties from accepting anonymous party funding. A report on the subject is to be presented in the spring of 2016 at the latest and, as a result, even though the political system has only reluctantly accepted to be subjected to such public oversight, legislation may follow.

General issues

Who should conduct the investigation?

An important aspect of any investigation into a suspected internal fraud, or another illegal activity or impropriety committed by the company's own employees, such as bribery or a violation of competition laws, price fixing or cartel activities, is to try to preserve and protect information and documents from being disclosed to third parties – for instance, a civil litigant, a competitor or a regulator. Only an investigation conducted by an outside counsel who is subject to the professional rules of conduct established by the Swedish Bar will be adequately protected against such third parties. An outside counsel cannot be compelled to give testimony and all correspondence between the client and the outside counsel would be subject to attorney–client privilege and may not become the subject of discovery. Such correspondence is also protected against disclosure – for instance, during a dawn raid by the Competition Authority. Although there may be other candidates to consider for the role of investigator – such as the company's general counsel, the company's chief compliance officer or an audit firm – legal privilege will only apply to an outside counsel. Also, an in-house counsel or a compliance officer may be perceived as being too close to the persons or matters being investigated to have sufficient objectivity and credibility. Lastly, an outside counsel with trial experience may be better suited than, for instance, an in-house counsel to assess and evaluate evidentiary issues. Depending on the circumstances and the persons or matters being investigated, a truly independent outside counsel may be preferable to the company's regular external counsel. Again, the GSK case may serve as an illustration. Originally, GSK retained a corporate detective to conduct its investigation, but when this person ended up in an orange prison vest and handcuffs, GSK turned to a large US law firm with extensive experience in conducting investigations into corporate fraud and charges of corruption.

Restrictions under labour law

Under Swedish labour law, as a general rule or principle, the employer manages the employee's work and decides what equipment is to be used and the manner in which it is to be used (the Government Memorandum, page 191). On the basis of this general rule or principle, the employer may establish policies with respect to, for instance, employees' email correspondence and use of the internet and the employer may take what steps are reasonably necessary to safeguard and verify that such policies are adhered to by the employees. This general right of the employer, however, is not unrestricted and there are limitations to an employer's right to use supervisory or investigative measures. Among other things, the employer always has to observe what could be described as 'good practices in the labour market'. The highest court for labour law disputes, the Supreme Labour Court, has established the principles of balancing convenience and proportionality. In cases concerning an alleged infringement of an employee's right to privacy, the Supreme Labour Court will assess whether the employer had a legitimate need to employ the supervisory or investigative measures in question, whether those measures were adequate and whether there were other, less intrusive, methods that could equally have been used and whether the employer's interest in being able to use those methods should take priority over the employee's right to privacy. Although the Supreme Labour Court is sensitive to privacy-infringing actions and although the court relies on a particularly 'fine tuned' assessment in such cases, in most cases, the court has actually ruled the employer's measures to be compliant with good practices in the labour market (Öman, Sören, 'Using private email in the working place', *Liber Amoricum Reinhold Fahlbeck* ('Öman'), page 691).

In order for an employer to be able to access an employee's email correspondence or to monitor an employee's use of the internet without the employee's consent, the employer must be able to demonstrate that they are acting with good and acceptable cause, such as a reasonable suspicion relating to a criminal offence, disloyalty, violation of reasonable company guidelines or for IT security reasons. Furthermore, the measure undertaken by the employer must be relevant and suitable in view of the employer's stated reason for undertaking the measure in question. The employer must also take measures to ensure that the email correspondence accessed by the employer is not disclosed to persons other than those who have a need to be able to read the correspondence. Emails indicated by the employee to be private or personal, and which also are private or personal, or that otherwise obviously are of a private or personal nature, should be excluded from the employer's review. A more detailed analysis of when the employer is permitted to access an employee's email correspondence is to be found in Öman, pages 692–698.

When considering employing supervisory or investigative measures, the employer has to observe their obligations to the employee's labour organisation. Under the Swedish act on co-determination in the workplace (SFS 1976:580), section 10, '*[a]n employee's organisation shall have the right*

to consult with an employer on any matter relating to the relationship between the employer and any member of the organisation who is, or has been, employed by that employer'. Further, under sections 11 and 13 of the same act, the employer is under an obligation themselves to initiate, prior to deciding any such work-related issues, negotiations with the employee's organisation. Failure to comply with these rules will make the employer liable to damages. Failing an agreement with the employee's organisation, however, the employer always has the right to decide the contested issue.

Restrictions under human rights legislation

An important consideration of any internal investigation must always be the employee's privacy rights as enshrined in the European Convention on Human Rights (the Convention). The Convention has been enacted as Swedish law by virtue of a 1994 act (SFS 1994:1219). In particular Article 8 of the Convention, which protects a person's private and family life, their home and their correspondence, has to be observed. An Article 8 argument can be advanced not only against investigations, but also against for instance various surveillance measures (the Government Memorandum, page 191). A case decided by the European Court of Human Rights (*Copland v United Kingdom*, 62617/00 ECHR), establishes that an employer's monitoring of an employee's telephone calls and email correspondence from work is liable to infringe Article 8 of the Convention.

The Convention also establishes, in Article 6, the presumption of innocence and the same principle has also been confirmed by the European Court of Human Rights (see for instance *Heaney and McGuiness v Ireland*, 34720/97 ECHR). The presumption of innocence includes the privilege against self-incrimination (the right to be silent and the right not to be compelled to produce inculpating evidence).

Other restrictions

In the absence of specific legislation protecting the employee's right to privacy, some protection is afforded to the employee under rules to be found in the Swedish Personal Data Act (the PDA) (SFS 1998:204), which implements the Data Protection Directive (95/46/EC). In these respects, the PDA confirms and details what is set out in chapter 2, section 6 of the Swedish Constitution (SFS 1974:152), namely that '*everyone shall be protected in their relations with the public institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or monitoring of the individual's personal circumstances*'. Moreover, protection is afforded under rules in the Swedish Penal Code (SFS 1962:700).

One of the fundamental principles of the PDA, is that any processing of personal data must be in compliance with '*good practices in the workplace*'. The test that will be applied under the PDA is very similar to the balancing of convenience test and the test of proportionality as established by the Supreme Labour Court. Further rules and restrictions are set out in sections 10 and 13 of the PDA which, among other things, deal with the processing of particularly sensitive information regarding, eg, race and ethnic

background or origin. The employer also needs to comply with certain pre-notification and information requirements as further set out in sections 23 to 27 of the PDA. However, pre-notification and information need not be specific to a certain instance of monitoring and can be provided in a general manner in the form of a general policy which is communicated to the employees.

The Data Inspection Board provides guidelines on the subject of electronic monitoring and a few years ago, in 2005, the board issued a report titled 'Monitoring in the workplace. Controlling employees' internet use and email' (the 2005 Report). The Data Inspection Board also publishes its findings at *www.datainspektionen.se/personuppgiftsombud/samradsyttranden*.

Under chapter 4, section 8, of the Penal Code, '*[a] person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or in an electronic communication network, shall be sentenced for breach of a postal or telecommunication secret*' and under chapter 4, section 9, of the Penal Code, a person who '*unlawfully opens a letter or a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for intrusion of a safe depository*'. The provision in chapter 4, section 8, will, however, not apply should an employer gain access to an employee's email correspondence from the employer's own local network (the Government Memorandum, page 73). The scope of the provision in chapter 4, section 9, is on the other hand very broad as it, for instance, will apply to documents that are kept in a locked space or in a sealed envelope and to information which is sealed on a disk or a USB memory stick (Government Memorandum, page 74).

The use of certain surveillance measures, such as secretly listening by means of technical equipment ('eavesdropping') to other people's private conversations and the use of surveillance cameras (including the use of CCTV) are restricted and can be penalised.

Pursuant to chapter 4, section 9A, of the Penal Code, a person who '*unlawfully and secretly listens to or records by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access shall be sentenced for eavesdropping*'. The provision does not apply in situations where telephone conversations are intercepted through the regular telephone network. However, the interception of a telephone conversation through internal equipment within a house or a workplace, by way of example, conversations by intercom telephone, is covered by this provision. The provision, however, only applies to a conversation between other people and not to a conversation in which the person making the recording also participates. Also, a digital voice recording is generally considered to constitute personal data within the meaning of the PDA (notice from the Data Inspection Board 1579-2004). Such data processing may therefore, depending on the circumstances, be subject to the provisions of the PDA.

2.1/2 Hard copy and electronic documents

Any internal investigation will require documents (including electronically stored information) to be reviewed. Therefore, the employer must immediately consider whether the employer's normal system of retaining and destroying documents should be suspended. Preservation of documents may be very important, not least if, in a subsequent litigation, it is argued that the employer was complicit in the fraud.

The retention of personal data is governed by section 9 of the PDA, which states that personal data may not be retained for a longer period of time than is necessary for the purpose of the processing. This provision codifies a general principle that employee monitoring data shall only be retained for a limited period of time and only as long as the employer's need for such data exists, eg, as long as an internal investigation is ongoing.

The Data Inspection Board has specifically commented upon the retention of data as a result of the monitoring of email correspondence or use of the internet and the board is of the opinion that such data may not be retained for more than three months (the 2005 Report, page 5). However, should an investigation require more time than three months, the data may be retained for the duration of the investigation (the 2005 Report, page 19). As far as personal data in the form of CCTV or video recordings are concerned the Data Inspection Board has recommended daily or at least weekly reviews and screenings in order to comply with the PDA (the 2005 Report, page 6).

With respect to the retrieval and reviewing of documents, as well as physical materials that have been created by an employee and fall within the scope of the employment, such items will normally be considered the employer's property. (This is in contrast to materials protected by copyright – in their case the intellectual achievement will be proprietary to the employee since, under Swedish law, there is no 'works made for hire' concept.)

In all other respects, the above-detailed restrictions under labour law, human rights legislation, the PDA and the Penal Code will apply.

2.3 Obtaining oral evidence from employees

As mentioned above, the presumption of innocence is enshrined in the Convention. Under Swedish procedural rules, there are also safeguards against self-incrimination. Accordingly, under chapters 36 and 37 of the Swedish Code of Judicial Procedure (SFS1942:740), a person being prosecuted or who is suspected of a crime may not testify under oath and a witness may, also in civil proceedings, decline to testify about such circumstances that would reveal that they have committed a crime. These rules, however, do not restrict an employer wanting to interview their employees as a part of an internal investigation. Neither are there any specific rules that provide that an employee being interviewed should be provided with advance notice, have legal representation or have the right to have a witness (for instance, a colleague) attend during the interview.

Obviously, an employer has no means to physically compel an employee to answer questions during an interview or to otherwise participate or aide

the investigation. Sometimes, however, depending on the circumstances, a court may draw negative inferences from a person's refusal to answer questions. The ultimate sanction against an employee refusing to answer questions or to otherwise participate in the employer's investigation would be summary dismissal or termination with notice. Whether the employer would actually have cause to dismiss an employee or terminate their contract in these circumstances is an open question and the answer would depend on the individual facts of any such case. Such facts, which would have to be considered, would include the nature and the strength of the employer's suspicion, the importance of the matter to the employer, whether the employer's suspicion concerns the employee themselves or a colleague of the employee, whether or not the employee was given advance notice of the interview, whether or not the employee has refused on one or more prior occasions to participate and whether or not the employee has received a warning against the consequences of their non-participation. Generally speaking, however, it would be reasonable to assume that only under exceptional circumstances would the employer have cause to summarily dismiss or terminate with notice the contract of an employee who refuses to participate in an investigation where they themselves are under suspicion. Accordingly, it would be illogical to think that the employer could place the employee in a situation whereby if the employee truthfully answers the employer's questions, the employee will reveal that they have committed a crime, which revelation would result in the employee being dismissed or terminated, or to decline to answer, which refusal would have the same consequences to the employee as if participating and telling the truth. This conclusion would also seem to be consistent with human rights principles and with Article 6 of the Convention.

As a general rule, there are very few restrictions under Swedish procedural rules as to the admissibility of evidence. This principle of admissibility is enshrined in chapter 35, section 1, of the Code of Judicial Procedure, which states that '*[a]fter evaluating everything that has occurred, in accordance with the dictates of its conscience, the court shall determine what has been proven in the case*'. Also under this rule, evidence that may have been obtained in an illicit way, eg, through unlawful surveillance measures, would be admissible. Interview notes resulting from an interview conducted with an employee under suspicion of having committed a crime would readily be admissible, but may, depending on the circumstances, have limited evidentiary value if they lack confirmation by the employee and if they are contested in litigation.

2.4 Legal privilege

In terms of legal privilege an important distinction has to be made between the legal privilege that applies to attorneys as 'attorney–client privilege' and the legal privilege that applies to non-attorneys under the 'litigation privilege'. The Swedish Bar's Code of Conduct (to which an advocate/attorney at law is obliged to respect and adhere) provides that a member

of the bar shall preserve confidentiality with respect to their client's affairs and that they may not without permission, unless there is a statutory duty to disclose such information, reveal anything which has been confided to them in their professional capacity or which they have learned in connection therewith (section 2.2). It is therefore stated in chapter 36, section 5, paragraph 2 of the Code of Judicial Procedure that advocates '*may not testify concerning matters entrusted to, or found out by, them in their professional capacity unless the examination is authorised by law or is consented to by the person for whose benefit the duty of secrecy is imposed*'. A properly conducted internal investigation must be done in such a way that preserves the attorney–client privilege. In this regard, it is clear that the attorney–client privilege under Swedish law and under Swedish rules does not extend to an in-house counsel (see also the ECJ's 14 September, 2010 judgment in case C-550/07, *P Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v the European Commission*, whereby the ECJ denied client-attorney protection for a company's employees' communications with the company's in-house lawyers).

The litigation privilege, which applies to non-attorney trial representatives, is significantly more limited than the attorney–client privilege. It is provided in chapter 36, section 5, paragraph 3, of the Code of Judicial Procedure that: '*Attorneys, counsel or defence counsel may be heard as a witness concerning matters entrusted to them in the performance of their assignment only if the party gives consent.*' The most important difference in relation to the attorney–client privilege is that the litigation privilege is limited strictly to protecting confidential client communications entrusted to a trial representative who is not a member of the Swedish Bar, to facilitate the legal representation in a specific litigation.

The litigation privilege applies only to such legal service providers that have attained the formal status of representing a party in litigation, eg, by means of a power of attorney. It is also required that the communication is germane to and facilitates representation in litigation.

In relation to requests for the production of documents, or discovery, it is further stated in chapter 38, section 2, paragraph 2 of the Code of Judicial Procedure that *' [n]either a public official nor any other person referred to in Chapter 36, Section 5, may produce a written document if it can be assumed that its contents is such that he may not be heard as a witness thereto; when the document is held by the party for whose benefit an obligation of confidentiality is imposed, that party is not obliged to produce the document*'. Documents that are subject to attorney–client privilege or 'litigation privilege' are, therefore, protected against document production both in civil and criminal proceedings. However, protection against disclosure is more limited for the latter category of documents as it would follow the same distinction as is given with respect to the privilege of not to having to testify.

3. DISCLOSURE FROM THIRD PARTIES

In such cases where third parties refuse to volunteer information, Swedish law does not provide private litigants with any general mechanism for pre-

action disclosure and Swedish law provides no right to compel depositions, neither pre-action nor once proceedings have been commenced. The only exception, when evidence, in documentary form or in oral form, can be compelled in advance of the commencement of proceedings is when there is an imminent risk that the evidence will otherwise be permanently lost. One example of such a situation is when a potential witness is very old or terminally ill. Rules granting this limited pre-action right to compel evidence are laid down in chapter 41 of the Code of Judicial Procedure. These rules are explicitly limited to evidence that does not concern facts that imply that a crime has been committed. This limitation applies also in cases where the evidence is intended to be used in civil litigation.

4. STEPS TO PRESERVE ASSETS/DOCUMENTS

Under Swedish law, it is possible to obtain injunctive reliefs to preserve or secure assets of the defendant as well as orders to search an intended defendant's premises for documents and other kinds of evidence, so-called 'Anton Piller' orders. Whereas the possibility to obtain an injunctive relief is open in all cases which concern a claim for the defendant to perform a certain action, eg, payment or a so-called specific performance, or to refrain from a certain activity, search orders are only available in cases concerning an alleged infringement of an intellectual property right and may thus be of little help to a claimant in fraud cases. However, in certain cases, an applicant may attempt to portray, or even disguise, their claim in such a way so as to give it the appearance of an intellectual property claim, eg, concerning database protection (such as relating to a list of customers in a case which in reality concerns the misappropriation of trade secrets by an employee), in order to be granted access to a search order.

Chapter 15 of the Code of Judicial Procedure provides certain measures to help preserve or secure assets before judgment. The general prerequisite that has to be fulfilled in order to obtain an asset protection order is that the applicant has to present a *prima facie* case, both on the merits and the fact that the defendant may attempt to secrete or remove property. An asset preservation order may take the form of an attachment or a sequestration. An order to preserve assets may, under fairly limited circumstances, be granted *ex parte*. The possibility of being granted an order without prior notification to the defendant is explicitly reserved for such cases where a delay could result in the defendant being able to avoid the order, eg by absconding with the money or by disposing of the asset. When a court orders an attachment or a sequestration, the applicant will be liable to compensate the defendant for any loss sustained by reason of the order should it subsequently transpire that the order should not have been given. Therefore, in order to have a court provide such an order, the applicant first has to post an appropriate bond to cover their potential liability. The granting of an attachment or a sequestration will always be subject to the *balance of convenience* test, ie, the granting of such an order must appear to be just and convenient and not be unduly restrictive on the defendant. An asset protection order can be sought both as a pre-action measure and also

when proceedings have been commenced. In the former case, the applicant has to initiate proceedings within one month from the granting of the order.

The granting of a search order is subject to essentially the same restrictions and prerequisites as the granting of an attachment or a sequestration (see for instance sections 56 a to 56 c of the Swedish Copyright Act (SFS 1960:729)).

If Swedish jurisdiction can be exerted and if there is a Swedish venue, the same remedies will apply where principal proceedings have been brought or will be brought in another jurisdiction, but only provided that a judgment or award rendered in such a jurisdiction would be enforceable in Sweden.

An arbitration panel in a Swedish arbitration cannot order any steps to preserve assets or documents. However, where a party wishes to use such measures in connection with a Swedish arbitration, such a request can be made to a Swedish court of law.

A claimant cannot himself apply to have restrictions imposed on a defendant's freedom to travel, such as having the defendant's travel documents confiscated. Travel prohibitions or orders to report to the police can only be obtained by a public prosecutor and only under fairly limited circumstances.

On 14 May 2014, the Council of the EU adopted a regulation establishing a cross-border mechanism, a European account preservation order, to help creditors to secure a debtor's funds and to prevent debtors from dissipating such funds. Applying this new tool, a creditor may be able to obtain from a court in any EU member state an order which will block funds held by the debtor in a bank account in any EU member state. The new regulation came into force on 17 July 2014 (although most of its provisions will not apply before January 2017) and is directly applicable in most EU member states, including Sweden.

5. CIVIL PROCEEDINGS

Available remedies against third parties, either for complicity in a crime, for receiving company property or its traceable proceeds, or for benefitting from the proceeds of a crime by having such proceeds accrue to them, although not having assisted in the crime, may be sought either under general rules on tort or, in the case of misappropriation of company proprietary information, under specific rules protecting trade secret information (Swedish Trade Secrets Act (SFS 1990:409)). Depending on the circumstances, remedies may also be available under other legal theories, such as collusion or conspiracy. Available remedies include the recovery of stolen or misappropriated property or its traceable proceeds, compensatory damages for injuries or losses actually or at least proximately caused by the third party defendant, but not punitive damages, and injunctive relief. These remedies will be available both in criminal and in civil proceedings.

A person aiding or abetting a crime will be liable to damages under chapter 2, section 2 of the Swedish Torts Act (SFS 1972: 207).

A person who receives property knowing that the property is the proceeds of a crime – for example, a theft or a fraud – may be prosecuted for dealing

in stolen goods under chapter 9, sections 6 to 7 a of the Penal Code. The same would apply to a person who benefits from what they know to be the proceeds of a crime, eg a spouse living off the gains of a crime committed by their husband or wife.

Other businesses that have been provided with trade secret information that has been misappropriated by an employee may be liable under the Trade Secrets Act.

6. ANTI-BRIBERY/ANTI-CORRUPTION LEGISLATION

Effective from 1 July 2012, Sweden has enacted a revised and updated anti-corruption legislation. The new rules have been consolidated in chapter 10 of the Swedish Penal Code (section 5a–e).

In addition to bribe giving and bribe taking, the new legislation has introduced the wider concept of influence peddling and it has also established a new offence, negligent financing of corruption. The crime of influence peddling does only apply to the public, and not to the private, sector. Influence peddling involves a third party as the bribe taker, ie another party than the person whose decision making or actions are intended to be influenced by the bribe taker, and who acts as a sort of go-between. Both sides of the transaction – the giving and the taking of the bribe – are subject to the new provision on influence peddling. The crime of negligent financing of corruption covers a form of contributory involvement in the crime of bribe giving, a specific form of aiding and abetting bribe giving: the financing of the bribe.

The new rules are intended to be stricter and more comprehensive, yet simpler and easier to understand, than the old rules, but they represent less than a complete legislative overhaul, like the 2010 UK rules. Whether and to what extent the legislator has succeeded in making it less tempting to peddle, in the widest sense, influence for financial rewards, or to punish such offences when they do occur, is too early to say.

Victims of bribery may bring civil law claims against both the recipient of the bribe, ie the agent who accepted the bribe, and the giver or payer of the bribe. Such actions may include contract rescission and claims for financial compensation.

Contact details

FOREWORD

Lord Gold
David Gold & Associates
3 Fitzhardinge Street
London W1H 6EF
United Kingdom
T: +44 20 3535 8989
E: info@davidgoldassociates.com
W: www.davidgoldassociates.com

AUSTRALIA

Michael Hales & Gordon Williams
Minter Ellison Lawyers
Level 4, Allendale Square
77 St Georges Terrace
Perth 6000
Australia
T: +61 8 6189 7800
F: +61 8 6189 7999
E: mike.hales@minterellison.com
gordon.williams@minterellison.com
W: www.minterellison.com

AUSTRIA

Bettina Knoetzl
WOLF THEISS
Schubertring 6
1010 Vienna
Austria
T: +43 1 515 10 5200
F: +43 1 51510 66 5200
E: bettina.knoetzl@wolftheiss.com
W: www.wolftheiss.com

BAHAMAS

Philip Dunkley QC & Tara Cooper Burnside
Higgs & Johnson
Ocean Centre
East Bay Street
P. O. Box N 3247
Nassau, Bahamas
T: +1 242 502 5200/394 8410 4
F: +1 242 502 5250/394 8430
E: pdunkley@higgsjohnson.com
tcooper@higgsjohnson.com
W: www.higgsjohnson.com

BRITISH VIRGIN ISLANDS

Andrew Thorp & Jonathan Addo
Harneys
Craigmuir Chambers
PO Box 71
Road Town, Tortola
British Virgin Islands
VG1110
T: +1 284 494 2233
F: +1 284 494 3547
E: andrew.thorp@harneys.com
jonathan.addo@harneys.com
W: www.harneys.com

CANADA

Jim Patterson & Kirsten Thoreson
Bennett Jones LLP
3400 One First Canadian Place
P.O. Box 130
Toronto, Ontario
M5X 1A4 Canada
T: +416-777-6250
F: +416-863-1716
E: pattersonj@bennettjones.com
thoresonk@bennettjones.com
W: www.bennettjones.com

CAYMAN ISLANDS

David W Collier
Charles Adams Ritchie & Duckworth
Zephyr House, 122 Mary Street
P.O. Box 709
Grand Cayman
Cayman Islands
KY1-1107
T: +345-949-4544
F: +345-949-7073

E: david.collier@card.com.ky
W: www.card.com.ky

CYPRUS

Nicos Georgiades & Argyris Nicolaou
Georgiades & Pelides LLC
16 Kyriakos Matsis Avenue
Eagle House, 10th Floor
1082 Ayioi Omoloyites
Nicosia
Cyprus
T: +357-22889000
F: +357-22889001
E: ngeorgiades@cypruslaw.com.cy
anicolaou@cypruslaw.com.cy
W: www.cypruslaw.com.cy

ENGLAND & WALES

Simon J Bushell & James M Davies
Latham & Watkins LLP
99 Bishopsgate
London EC2M 3XF
United Kingdom
T: +44 20 7710 1000
F: +44 20 7374 4460
E: simon.bushell@lw.com
james.davies@lw.com
W: www.lw.com

FRANCE

Fabrice Fages, Myria Saarinen &
Hugues Vallette Viallard
Latham & Watkins LLP
45 rue Saint-Dominique
Paris 75007
France
T: +33 1 4062 2000
F: +33 1 4062 2062
E: fabrice.fages@lw.com
myria.saarinen@lw.com
hugues.valletteviallard@lw.com
W: www.lw.com

GIBRALTAR

Michael Nahon & Moshe Levy
Hassans International Law Firm
57/63 Line Wall Road
PO Box 199
Gibraltar
T: +350 200 79000
F: +350 200 71966
E: michael.nahon@hassans.gi
moshe.levy@hassans.gi
W: www.gibraltarlaw.com

HONG KONG

Simon D Powell
Latham & Watkins LLP
18th Floor, One Exchange Square
8 Connaught Place, Central
Hong Kong
T: +852 2912 2500
F: +852 2912 2600
E: simon.powell@lw.com
W: www.lw.com

INDIA

Anand Prasad & Ashish Bhan
Trilegal
A-38, Kailash Colony
New Delhi 110 048
India
T: +91 11 4163 9393
F: +91 11 4163 9292
E: Anand.Prasad@trilegal.com
Ashish.Bhan@trilegal.com
W: www.trilegal.com

IRELAND

Karyn Harty & Audrey Byrne
McCann FitzGerald
Riverside One, Sir John Rogerson's
Quay,
Dublin 2
Ireland
T: +353 1 829 0000
F: +353 1 829 0010
E: karyn.harty@mccannfitzgerald.ie
audrey.byrne@mccannfitzgerald.ie
W: www.mccannfitzgerald.ie

JAPAN

Junya Naito & Hirotoshi Kakumoto
Momo-o, Matsuo & Namba

Kojimachi Diamond Building
4-1 Kojimachi
Chiyoda-ku
Tokyo 102-0083
Japan
T: +81 3 3288 2080
F: +81 3 3288 2081
E: naito@mmn-law.gr.jp
hirotoshi.kakumoto@mmn-law.gr.jp
W: www.mmn-law.gr.jp

KAZAKHSTAN

Bakhyt Tukulov & Bolat Miyatov
GRATA Law Firm
104, M. Ospanov Street
Almaty, 050020
Republic of Kazakhstan
T: +7 727 2445 777
F: +7 727 2445 776
E: btukulov@gratanet.com
bmiyatov@gratanet.com
W: www.gratanet.com

LUXEMBOURG

François Kremer
Arendt & Medernach
14 rue Erasme
L-2082 Luxembourg
Luxembourg
T: +352 40 78 78 276
F: +352 40 78 04 653
E: francois.kremer@arendt.com
W: www.arendt.com

THE NETHERLANDS

Jeroen Fleming & Michiel Coenraads
Stibbe
Stibbetoren
Strawinskylaan 2001
P.O. Box 75640
1070 AP Amsterdam
The Netherlands
T: +31 20 546 06 06
F: +31 20 546 01 23
E: jeroen.fleming@stibbe.com
michiel.coenraads@stibbe.com
W: www.stibbe.com

FEDERAL REPUBLIC OF NIGERIA

Dr Simeon Obidairo, Chisom Nnabuihe & Adeola Fari-Arole
ALUKO AND OYEBODE
1 Murtala Muhammed Drive
(formerly Bank Road)
Ikoyi
Lagos
Nigeria
T: +234 1 462 8360 75
+234 1 792 5484
+234 1 774 3650
F: +234 1 462 8377 79
+234 1 2632249
+234 1 2647505
E: simeon.obidairo@aluko-oyebode.com
chisom.nnabuihe@aluko-oyebode.com
W: www.aluko-oyebode.com

SPAIN

Guillermina Ester Rodríguez, Adriana de Buerba Pando, Sara Martín Mustieles & Luis Paternina Vericat
Pérez-Llorca
Paseo de la Castellana, 50
28046 – Madrid
T: +34 91 436 04 20
F: +34 91 436 04 30
E: gester@perezllorca.com
adebuerba@perezllorca.com
smartin@perezllorca.com
lpaternina@perezllorca.com
W: www.perezllorca.com

SWEDEN

Peter Skoglund
Advokatfirman Delphi
Regeringsgatan 30-32
PO Box 1432
Stockholm
111 84
Sweden

T: +46 8 677 54 00
F: +46 8 20 18 84
E: peter.skoglund@delphi.se
W: www.delphi.se

SWITZERLAND

Paul Gully-Hart
Schellenberg Wittmer Ltd
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1
Switzerland
T: +41 22 707 8000
F: +41 22 707 8001
E: paul.gully-hart@swlegal.ch

Peter Burckhardt, LL.M.
Schellenberg Wittmer Ltd
Löwenstrasse 19
P.O. Box 1876
8021 Zurich
Switzerland
T: +41 44 215 5252
F: +41 44 215 5200
E: peter.burckhardt@swlegal.ch
W: www.swlegal.ch

TURKEY

H Tolga Danışman
Hergüner Bilgen Özeke Attorney Partnership
Suleyman Seba Cad.
Siraevler 55, Akaretler
34357 Besiktas-Istanbul
Turkey
T: +90 212 310 18 00
F: +90 212 310 18 99
E: tdanisman@herguner.av.tr
W: www.herguner.av.tr

UAE & DIFC

Stuart Paterson & Bridget Butler
Herbert Smith Freehills LLP
Dubai International Financial Centre
Gate Village 7, Level 4
PO Box 506631
Dubai
UAE
T: +971 4 428 6300
F: +971 4 365 3171
E: stuart.paterson@hsf.com
bridget.butler@hsf.com
W: www.herbertsmithfreehills.com

USA

Robert E Sims & Ramin Tohidi
Latham & Watkins LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111-6538
USA
T: +1 415 391 0600
F: +1 415 395 8095
E: bob.sims@lw.com
ramin.tohidi@lw.com
W: www.lw.com