Contents

Fraud risk in Japan

Forensic investigations of electronically stored information in the US

Reducing the costs of healthcare disputes

The UK Bribery Act 2010
It seems that each new edition of International Forensic Files is introduced by me talking about the beginning of the end of the hard times. Whilst that appears still to be the case, the continued uncertainty in a number of our markets around the globe is palpable. Nevertheless, we remain confident of a sustained up-curve in 2011.

In this issue, we have articles from the UK on the new Bribery Act, from the US on electronic data, from Japan on fraud risk conditions and from France on healthcare disputes. As ever, I am convinced of the wider application of the issues explored than simply in the countries who have penned them.

We continue to have this newsletter available in a number of languages – French, Spanish and Chinese in addition to this version – albeit this time each edition is a separate document.
Mazars is one of many foreign entities successfully operating in Japan, having learned many lessons about this unique place in which to do business over the last decade. We have helped our clients manage diverse local business risks, including:

- wild profit swings resulting from foreign exchange movements;
- trade barriers;
- cultural and linguistic barriers; and
- the high standards of quality imposed directly by the authorities or indirectly by consumers.

Of course, one additional business risk is fraud. Mazars Japan has considerable experience of the causes of fraud and has identified some of the business and cultural practices that can contribute to this risk, resulting in a unique set of problems for foreign businesses operating in Japan. In our view, these include:

1. Japanese society is characterized by high levels of trust. For instance, in a cheque-less society, it is quite common for employees to use company debit cards to pay company bills. This situation can make for easy pickings for the occasional dishonest or malevolent employee.

2. There is a strong culture of teamwork and respect for age - Japanese culture is also not supportive of those who step out of line. As a result, it is less likely that you will find a whistleblower in Japan. When things are going well, and the right business model is in place, the business may draw strength from this. However, this strength is counter-productive when there is pressure in the opposite direction.

3. Japanese companies have a strong sense of duty to their customers and employees. This can lead to practices which are in conflict with shareholder interests. We have experienced many examples of this, including:
   - an importer of medical equipment that eventually ceased trading, as customer entertainment and donations had eliminated profits;
   - management paying a customers' branch costs; and
   - particularly lavish entertainment that eradicated all profits.

4. Japanese companies have a tendency to be rule-based and resistant to change. There is a risk that few questions will be asked if everybody follows the rules. This can sometimes allow manipulative individuals to hide beneath a veneer of compliance. We know of one case where the foreign purchaser of a stake in an electrical company discovered that illegitimate sales commissions had virtually bankrupted the company – and this despite the surface appearance that rules were being strictly followed.

5. Japanese business practices are commonly held to be very different from those in place in the rest of the world. Many foreign companies accept this as part of operating in Japan, and consequently allow a “Japanese” system to operate as an alternative to the company’s normal international best practice. Unfortunately, this attitude often reinforces differences, with local staff being rarely transferred out of Japan, as they are not seen to be ‘au fait’ with the corporation’s practices and procedures. Meanwhile, foreign expatriates who have mastered the Japanese language are all too often considered indispensable in Japan, and tend to be kept there for long periods. This inevitably leads to a disconnect between the foreign company and its Japanese subsidiary, and produces over-reliance on key individuals – both Japanese and expatriate. This combination can lead to frustration, bad business practice and the opportunity for fraud.

As well as having considerable experience of the causes of fraud, Mazars offers a unique proposition to foreign corporations in Japan, as we are the only fully licensed audit firm documenting all its work in English. We have achieved this by a joint venture with the Japanese firm SCS Global in Japan and other territories. With all of our Japanese staff speaking fluent English and being part of a global firm, we are expanding in Japan and are enjoying working with an impressive array of multinationals.

“Japanese companies have a tendency to be rule-based and resistant to change. There is a risk that few questions will be asked if everybody follows the rules. This can sometimes allow manipulative individuals to hide beneath a veneer of compliance.”
Forensic investigations of stored information in the US

Electronically stored information ("ESI") ranges from emails to digital general ledgers to databases. It almost invariably includes potential evidence in a dispute that requires disclosure and/or investigation. In order to be admissible at trial, ESI must be collected, transported, stored and investigated in accordance with procedures that preserve the integrity of the original data and electronic storage medium. The US rules that deal with electronically stored evidence are contained in the Federal Rules of Evidence, the Federal Rules of Civil Procedure, similar state rules and statutes, and in case law.

In preparing for litigation, forensic computer analysts can be hired to investigate and retrieve a broad range of ESI, including financial information, which is subject to discovery. Typically, attorneys in US civil and criminal cases will retain non-testifying forensic experts through the use of specific retention letters, called Kovel letters. These experts are typically hired to retrieve relevant electronic records which may have been encrypted, lost, deleted, damaged, or are otherwise not suited for direct analysis by any of the parties.

Under the terms of a Kovel letter, an attorney retains an expert to assist in understanding the facts or technical points of a case. This structure affords experts and their resulting work the protections of the attorney-client privilege and the attorney work-product doctrine. In this way, much of the information developed by the non-testifying expert analyst is not subject to discovery by other parties.

Discovery of ESI can be unusually costly. It is however possible (under the Federal Rules of Civil Procedure) to shift the cost of discovery to the party requesting the electronic records. As a general rule, any cost associated with producing discoverable records is borne by the party that is in possession of the records. However, where the cost of producing electronic records is expected to outweigh the benefit of any resulting evidence, the cost may be shifted to the opposing party. Cost benefit factors developed in three cases (Rowe Entertainment v. The William Morris Agency, Inc., Zabulake v. UBS Warburg LLC, and Wiginton v. CB Richard Ellis, Inc.) are applied to determine whether the cost of producing evidence outweighs its expected benefits.

These cases demonstrate the need for proper planning by the forensic computer analyst in the electronic discovery of the evidence. This includes gaining an understanding of the hardware and software used, the policies and procedures employed in processing information, and the way in which the ESI was stored. Metrics such as the size of the data, item counts and gaps in the data should be used during this process to assist counsel in estimating the costs associated with the case as well as any potential negotiating strategy.

In addition to proper planning, it is imperative that any investigation is properly controlled and executed. The forensic computer investigation can be broken down into four chronological steps each of which has its own particular issues requiring attention:

1. **ESI chain of custody**: the investigator must create a chain of custody that traces the chronological "life" of the physical evidence (hard disk drive, thumb drive, mobile device, etc.) from the time of seizure to the time the evidence is presented at trial. The chain of custody should include the identities of any investigators who handled the item, as well as the means employed to protect the integrity of the evidence while it was in storage. In criminal cases, establishing the chain of custody is generally required in order to avoid later allegations of tampering with physical evidence.

2. **ESI collection**: This step is critical in the process. The investigator must not alter the original evidence in any way. Instead, the investigator creates two exact replicas of the original storage medium. One copy is left untouched, while the second “working copy” is used for the investigator’s analysis.

In order to obtain an exact copy of the original evidence, data must be transferred from the original storage medium using dedicated forensic hardware and software. Forensic

Harry Steinmetz, Nicholas Quairel and Cody Cass in New York set out an easy guide to electronically stored information.

These experts are typically hired to retrieve relevant electronic records which may have been encrypted, lost, deleted, damaged, or are otherwise not suited for direct analysis by any of the parties.”
Reducing the costs of healthcare disputes

Luc Marty in Paris considers how reductions in healthcare costs are giving rise to a new wave of disputes.

A number of health policies have recently been developed in France which aim to reduce health costs by any and all appropriate means. An interesting side-effect of this has been the phenomenon of accelerated development of generic, over-the-counter pharmaceutical products.

The aggressive approach adopted by generic laboratories, combined with the high-calibre of regulatory officials dedicated to monitoring existing patents and registering of new patents, has led to numerous disputes in two major areas:

- opposition to existing patents (or other incorporated rights)
- the conditions under which generic, substitute products are introduced to the market

As a result, those laboratories who produced the initial, first-generation products are anxious to protect their economic rights and interests and are in direct opposition to those which are now producing the second-generation, substitute products.

Our in-depth knowledge of this sector, and the issues it is currently faced with, enable us to assist our clients in dealing with the claims that arise from such confrontations, and this in the most appropriate manner.

It is worth noting that the generic product sector represents the most dynamic market segment, with a growth rate of 12 to 15% in value per year. This compares with a growth rate of 2 to 3% for the overall pharmaceutical sector.

The French health authorities are being hyper-vigilant with regards to ensuring the safety of generic medications. Interestingly, this is having a favourable effect on European economies, whereby the rate at which these generic products are introduced to the market, as well as the desire for production to be in close proximity to their markets, is justifying conditions for developing production facilities within Europe.
The UK Bribery Act

Peter Cudlip from the UK explores the impact of the Bribery Act 2010 and provides guidance on what action boards should consider taking to implement bribery procedures within their organisations.

BACKGROUND...

Corporate and personal responsibilities

The Bribery Act 2010 (“the Act”), which comes into force in April 2011, completes the UK’s implementation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and simplifies the existing law on bribery, enabling the courts to deal more effectively with such cases.

The Act has significant implications for all organisations formed or doing business in the UK, particularly those involved in foreign trade. Several new criminal offences are created in the Act, including:

- bribing another person (active bribery);
- being bribed (passive bribery);
- bribing a foreign public official; and
- negligent failure by commercial organisations to prevent bribes being paid on their behalf. Organisations charged with this offence can put forward a defence of having ‘adequate procedures’ – this is discussed further below.

Unlike the US Foreign Corrupt Practices Act (“FCPA”) an offence of bribery may be committed whatever the monetary value of the bribe – there is no de minimus exception. This might raise some alarm bells over so-called facilitation payments, historically viewed by many as an incidental cost of doing business in some countries. Even if a bribery offence occurs wholly abroad, an offence under the Act is possible if the person committing that offence has a ‘close connection’ with the UK.

Penalties for companies and individuals found guilty of an offence under the Act are not insignificant, and include unlimited fines and imprisonment for up to 10 years.

The legislation poses a particular risk for persons charged with maintaining systems of internal control, although any director, manager or similar status employee of the organisation will be guilty if a bribery offence has been committed with their consent or involvement.

Organisations need to be able to evidence that arrangements and controls to prevent bribery exist and are operating effectively. They should benchmark their anti-bribery framework against the draft guidance from the Ministry of Justice on what constitutes ‘adequate procedures’ and be confident that their framework would stand up to scrutiny in a court of law. Failure to do so could result in draconian fines or imprisonment.”

Defence of ‘adequate procedures’

If there are sufficient controls in place, corporate entities, and their senior officials, will be able to rely on a defence of ‘adequate procedures’ to defend allegations of breaches of the Act. Draft guidance recently issued by the Ministry of Justice sets out six broad management principles that are outcome-focused and flexible, namely:

1) Risk assessment – of the current bribery risks faced by an organisation;

2) Top level commitment – to establishing a culture where bribery is unacceptable, and that a clear message conveying this is regularly delivered to all staff and business partners;

3) Due diligence – of the parties with whom the organisation does business, knowing why, when and to whom payments are made, and their having reciprocal anti-bribery agreements in place;

4) Clear, practical and accessible policies and procedures – applicable to all staff and business partners and covering areas such as gifts and hospitality, contributions, promotional expenses and facilitation payments, as well as response plans for bribery allegations;

5) Effective implementation – of anti-bribery culture, controls, policies, training, communication and other procedures so that they are fully embedded and part of day-to-day business; and

6) Monitoring and review – through audits and other internal controls to prevent and detect bribery, with regular, and possibly external, review and verification.

Consultation on this draft guidance ended on 8 November 2010, with the final guidance expected to be issued early next year ahead of the enforcement of the Act from April 2011.
Six steps to consider now

Depending on the size and complexity of the organisation, it could take a considerable amount of time and resources to ensure that adequate procedures to prevent bribery are in place, and operating effectively, prior to the legislation coming into force. Hence, although the final guidance is still to be issued, there are certain steps that organisations can take now, based on the six principles detailed above:

1) The boards of organisations should set the tone and lead by example by committing to a zero-tolerance approach to bribery. This message then needs to be communicated across the entire organisation, to both UK and overseas operations.

2) Boards must also ensure that sufficient resources are made available to ensure that an adequate anti-bribery framework is in place, and operating effectively, prior to April 2011. With a sponsor at board level, a team of internal and/or external people skilled in areas such as HR, internal audit, legal services and corporate governance needs to be put together at an early stage to ensure a successful outcome to the exercise.

3) A high-level risk assessment of overall corporate governance, including internal control frameworks and supporting policies, will identify areas where the company is most exposed to bribery and which need to be addressed as a priority.

   This review must include any third parties providing services on the organisation’s behalf (for example, sales agents or providers of outsourced services) as well as key suppliers, advisers, joint ventures, or similar arrangements in which the organisation is involved.

   A detailed assessment of the highest risk areas should draw out the key weaknesses in the current arrangements and enable a more robust control framework to be designed and implemented. The key starting point would be to draw up an assurance map of the current arrangements. Typical areas where particular focus may be required include the tendering and awarding of contracts, long-term contracts, high value projects in the UK or overseas, corporate entertainment and any areas of the business which involve interaction with government officials.

4) Governance-related employee policies should be reviewed and, if necessary, revised and re-issued, to ensure that the company’s stance on bribery is made clear. There can be no misunderstanding on what constitutes acceptable behaviour in areas such as offering and accepting gifts and hospitality.

   If policies on ethical business practices do not already exist, they must be written and issued. Organisations should be able to evidence how they have brought such policies to the attention of their staff, partners and any intermediaries.

   Contract terms and conditions should be reviewed to ensure that they also make reference to the organisation’s stance on bribery.

5) As the Act applies not just to employees but to ‘any person associated with the organisation’, agents as well as any other third parties carrying out business on the organisation’s behalf will need to be trained alongside the organisation’s own staff. Such training needs to focus on ethical business practice, including policies and procedures surrounding bribery, with a clear message of zero-tolerance towards the acceptance or giving of bribes.

6) There should be a credible mechanism for employees or third parties to report any concerns on bribery and an independent investigation process flowing from this.
Please get in touch…

…with one of our National Contacts listed below or your usual forensic contact:

Belgium
Lieven Acke
T: +32 9 265 83 20
E: lacke@mazars.be

Czech Republic
Zachary Rosen
T: +420 224 635 730
E: zachary.rosen@mazars.cz

Hong Kong
Ken Morrison
T: +852 2909 5599
E: ken.morrison@mazars.com.hk

France
Luc Marty
T: +33 1 49 97 61 85
E: luc.marty@mazars.fr

Germany
Stephan Kleinmann
T: +49 30 200774-10
E: stephan.kleinmann@mazars.de

Hungary
Zsuzsa Fekete
T: +36 1885 0279
E: zsuzsa.fekete@mazars.hu

India
Monish Chatrath
T: +91 124 4814 404
E: monish.chatrath@mazars.co.in

Ireland
Tom O’Brien
T: +353 1 449 4458
E: tjobrien@mazars.ie

Italy
Carlo Consonni
T: +39 02 5820 1321
E: carlo.consonni@mazars.it

Japan
Bruce Darrington
T: +81 3 5464 3077
E: bruce.darrington@mazars.jp

Malaysia
Kin Kheong Tang
T: +603 2161 5222
E: kin-kheong.tang@mazars.my

Mexico
Mauricio Rioseco
T: +52 5 55 980 5200
E: mauricio.rioseco@mazars.com.mx

Poland
Monika Kaczorék
T: +48 22 345 5200
E: m.kaczorek@mazars.pl

Russia
Jean-Marc Tinel
T: +7 495 792 52 45
E: jean-marc.tinel@mazars.ru

South Africa
Gillian Bolton
T: +27 21 405 4128
E: gill.bolton@mazars.co.za

Switzerland — Zurich
Franco Straub
T: +41 44 384 9371
E: franco.straub@mazars.ch

Switzerland — Geneva
Jacques Fournier
T: +41 22 708 1080
E: jacques.fournier@mazars.co.uk

Thailand
Rob Hurenkamp
T: +66 2 670 1100
E: rob.hurenkamp@mazars.co.th

The Netherlands
Aarnout de Bruijne
T: +31 10 2771510
E: aarnout.debruijne@mazars.nl

Turkey
Gokhan Almaci
T: +90 212 296 51 00
E: galmaci@mazarsdenge.com.tr

UAE
Ghassan Sakhnini
T: +971 4 357 3111
E: gsakhnini@mazars.ae

UK
Nigel Grummitt
T: +44 20 7063 4101
E: nigel.grummitt@mazars.co.uk

USA
Harry Steinmetz
T: +1 212 375 6741
E: harry.steinmetz@weisermazars.com

Please contact chris.drewe@mazars.co.uk if you would like to receive a copy of this newsletter in any of the following languages:

French
Spanish
Chinese