

RISK ADVISORY

Helping our clients evaluate, manage and mitigate risk

Issue 2, May 2003

Chief Executive's Note

In this, our second edition of **Risk Advisory**, we seek to assist our clients in two ways. First, by providing practical advice and solutions; and second, by providing expert analysis on two specific topics on which we have been asked to advise in the last three months.


The first four articles provide practical advice on a series of diverse issues ranging from electronic discovery in litigation to the practical issues surrounding entering the Iraqi business market following the end of large scale hostility.

In the second two articles we review the impact of the Iraqi war on business relationships between France and the United States, and finally reflect on changes to attitudes towards corporate governance in Russia and the implications there for Western business.

We hope you find the articles interesting.

May I thank those of you who provided both positive and negative feedback to the first edition of **Risk Advisory**. Your feedback helps us to improve our offering and we welcome it.

Finally, should you have any questions concerning the issues raised please do not hesitate to call me.



Bill Waite
Chief Executive



Recovery and disclosure of digital information

In cases of commercial litigation, there are requirements for both the claimant's and the defendant's sides to disclose to each other material information relating to the case. Increasingly, this involves stored electronic documents. Recent high profile cases such as Enron have shown that these documents can be vital evidence. Unfortunately, there are still very few rules to specify how electronic documents should be disclosed, and English Civil Law makes no general distinction between paper and computer-based records. There are, however, very substantial differences. This article explores the principal features of digital document disclosure and suggests a few ways in which companies can either avoid embarrassment in court or add weight to their case. These steps need proactive action. If you wait until the summons arrives, it will almost certainly be too late. But getting the fundamentals right is not difficult.

What are the legal obligations?

There is no doubt that standard disclosure includes electronic documents – specifically including spreadsheets, databases, emails and word processing documents – irrespective of the media in which they are stored, such as laptops, mobile phones, CDs, computer back-up tapes and so on. The problem is how to extract the information in a form whose integrity cannot be challenged by the other side's experts later. It is here that we can help.

What makes digital documents different?

The most striking characteristic of computers is the ease with which new documents can be created, modified and transmitted. There is hardly a transaction or communication within any company that has not at some stage in its life existed inside at least one computer. An e-mail is probably the most extreme example. Most people believe that an e-mail is reasonably private, ephemeral and informal. None of these things is true. For example, between an originator and a remote recipient there will be at least 10 identical copies of the same message. So even if the originator's workstation has disappeared there are still plenty of places in which we can look for evidence. From our perspective as investigators, the cavalier behaviour of most people in respect of e-mails presents a superbly rich seam of evidence: most people say things in an e-mail that they would never dream of committing to a letter.

Documents such as e-mails can be deleted – or so the originator might think. Again, most so-called deleted documents can be restored given the appropriate skills and tools. The size of hard disk memories in most machines today means that re-use of any area of hard disk is very low and files are sometimes not overwritten for years. The delete key is a fraud!

How far do we have to go?

Although there is no procedural distinction between paper records and those held in a computer, the sheer volume of computer files can potentially result in a huge and costly exercise. The law recognises this and a degree of 'proportionality' is applied. This is determined by lawyers for both parties who will decide where a reasonable line can be drawn. Among the tests for reasonableness are the:

- Cost and ease of retrieval
- Number of documents
- Nature of the case and the complexity
- Significance to the case of any document that might be found

Despite the application of common sense, the scope of the search and the organisations and sites concerned has recently been expanded. In October 2002 the Court of Appeal ruled on the BCCI banking failure case that disclosure could apply to the agents and suppliers of the principal players as well as the players themselves. This means that PR advisers, lawyers, third-party suppliers etc can also be caught up in this process.



'There is hardly a transaction or communication within any company that has not at some stage in its life existed inside at least one computer'

How do I make sure we are covered?

There are many detailed components that need to be got right. The two most important high level issues are:

- **Policy:** ensure that your firm has a clear policy on information archiving. There should be one focal point for all related decisions and the policy should be coherent across the firm. Back-up tapes and documents archived to CD should all comply with the same basic rules.
- **Asset Management - Workstations:** These machines are vital links in the information chain. They provide by far the best source of evidence and searching them forensically is a well understood science. But most firms are weak at managing these assets. It is vital that inventories of all PCs and laptops are maintained so that the ownership of each machine can be established historically.

The pitfalls of document disclosure are legion. We can help in two ways: to ensure that you are well positioned – just in case; alternatively, we can help to recover information in conjunction with legal advisers in a way that is evidentially sound once the legal process is in motion. This is an expert and too little understood field; 'Get help' is the best advice we can offer.

Bob Fletcher

Bob Fletcher is a Director of The Risk Advisory Group. If you would like to know more about digital investigations, please contact him at

bob.fletcher@riskadvisory.net

Money laundering – spotting the red flags

In the wake of 11 September, President Bush announced plans to introduce new legislation against money laundering as a means of cutting off funding to terrorists: within two months the Patriot Act was signed into law. This was followed in the UK by the Terrorism, Crime and Security Act 2001, which came into force in February 2002, and the Proceeds of Crime Act 2002 (POCA), which received Royal Assent in July 2002. Although the two Acts serve to reform UK criminal law on money laundering, there remain substantive issues concerning their implementation, and particularly of POCA. Not least of these is the onerous and potentially far-reaching requirement of the regulated financial sector to report suspicions of money laundering; more than this, the obligation to report where there are reasonable grounds to suspect. On 14 February 2003 the Joint Money Laundering Steering Group (JMLSG) released the Revised Supplementary Guidance for the Proceeds of Crime Act. When approved, courts will have the assistance they need to determine where 'reasonable grounds' exist. In this article we consider the red flags of money laundering and contrast them with those prescribed by the Guidance.

An expansion of the regulations and the regulated

Part Seven of POCA, which deals with money laundering offences and potential avenues of defence, introduces a number of changes for the regulated financial sector. It is worth noting that in addition to the new law on the reporting of suspicious transactions, the principal provisions introduce the following changes:

- A revised reporting requirement: failure to report, without a reasonable excuse, will carry a possible five year prison sentence and/or a fine;
- Reports should be made, in the form that is prescribed, to the National Criminal Investigation Service (NCIS) only;
- Insufficient training can provide an employee of a firm with a defence against a non-reporting charge. However, the employee is still subject to the objective test of reasonable grounds. Failure by the firm to provide appropriate training is both a separate criminal offence under the Regulations and a potential breach of FSA Rules;

- A Money Laundering Reporting Officer will commit a separate offence under the reporting laws if, upon receiving an internal report, he or she fails to make the required report to NCIS as soon as is practicable; and
- The amended guidance issued by the JMLSG must be taken into account by the courts when deciding whether an offence has been committed.

A further reality is that the 'regulated sector' has been significantly extended to include, among others, auditors, real estate agents, legal professionals, dealers in high value goods, cash businesses and casinos. For most, however, the reasonable grounds test will demand the greatest attention.

The courts and their red flags

Having no suspicion that another person is engaged in money laundering will no longer offer financial institutions a defence. Indeed, 'reasonable grounds to suspect' has a broad reach: from 'turning a blind eye', to negligence through inappropriate enquiries or assessment of the facts available. In short, firms must be able to spot the red flags and act. The guidance notes offer the following general advice: '[conduct] inconsistent with a customer's known legitimate transactions or with the normal business activities for that type of account or customer' as the basis for a suspicious transaction. They go further, and list illustrations that might give rise to reasonable grounds. It is these illustrations that will help the courts determine when an offence is committed. The types of situations listed are:

- Transactions which have no apparent purpose and which make no obvious economic sense;
- Where the transaction is being requested by the client without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the firm in relation to the particular customer;
- Where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
- Where the customer refuses to provide the information requested without reasonable explanation;
- Where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;
- The extensive use of offshore accounts, companies or structures in circumstances where the customer's needs do not support such economic requirements;
- Unnecessary routing of funds through third party accounts;
- Unusual investment transactions without apparently discernible profitable motive.

Red flags in business

On-the-ground firms see more defined red flags, for example: a client makes frequent deposits or withdrawals of large amounts of currency which seem at odds with the client's normal type of business; a client seeks to invest or transfer funds of a third party with whom the client has no fiduciary duty; or a client exhibits an unusual lack of concern regarding risks and commissions or other transaction costs. These suspicious activities fit nicely into the list of guidance notes.

In fact, the illustrations are necessarily generic. However, this will give financial institutions little encouragement. If money laundering has been perpetrated through a financial intermediary, then lurking among the prescribed situations a case could be brought to suggest the firm had failed the objective test. The illustrations certainly do not give the regulated sector anything to hide behind.

Avoiding the red flags

So while the role of law enforcement in the battle against money laundering has been given added effectiveness, the requirements on those regulated have shifted once again and are seemingly ever more onerous. But while corporate entities revise their risk strategies and wrestle with resource allocation to meet the challenge, how will the laundrymen react? Some of the possibilities are considered below:

'...failure to report, without a reasonable excuse, will carry a possible five year prison sentence and/or a fine'



- At least the first stage of money laundering (placement) by international organised criminals appears to be migrating towards emerging market economies, where law enforcement, regulations and corporate governance are still taking shape. Banks in these jurisdictions are often 'controlled' by the criminals themselves, and mechanisms are set up to circumvent the legislation. Such mechanisms might include companies set up in transparent jurisdictions such as the UK, with a Ukrainian bank account which is then controlled by launderers via a power of attorney granted by the UK nominee directors to associates of the criminals based in, say, Russia;
- Use of foreign currency to settle purported international trading arrangements using inflated invoices and individuals acting as money exchangers (as part of the second stage, layering);
- Use of incorporated entities being used as vehicles through which normal banking transactions are channelled to avoid scrutiny under correspondent banking regulations;
- Use of complex investment banking instruments as part of financial engineering by 'front' companies;
- Use of loan-back method to repatriate foreign illegal funds;
- Use of Hawallah, Hundi or Chitti banking commonly encountered on the Asian sub-continent and the most likely mode for the movement of terrorist funds;
- Planting of employees or corruption of senior employees within financial institutions to circumvent normal checks and balances. This method was used by Lucy Edwards and her partner Peter Berlin at the Bank of New York to move more than \$7 billion in 42 months.

White flags instead of red

The support POCA provides to the Patriot Act was necessary but not sufficient. Even if the Act removes the hiding places for terrorist money in the UK, a wider international obligation exists. There must be no safe havens in the world if money launderers are to raise the white flags of surrender. As Gordon Brown announced in September 2001: "If we cannot get this international action then what you can do in one country will be rendered ineffective." – and on this battlefield at least, of that there is no debate.

Hitesh N Patel
Hitesh is the Head of
Financial & Special
Investigations. If you
would like to know
more about
corporate
investigations and
fraud related issues
please contact him
at
hitesh.patel@riskadvisory.net

Winning the peace: risks and rewards in post-war Iraq

It's been a funny old war. Even George W Bush admitted that he so enjoyed the briefings by Saddam's information minister 'Comical Ali' that he interrupted his meetings to watch him. All of us who have watched the dramatic events in Iraq (and at home) unfold on television have felt something of the strangeness and multiple ironies of the war.

And it's likely to be a funny old peace. The powerful images of rejoicing Iraqis toppling a statue of Saddam in Baghdad appeared definitive enough to many British and American eyes, and most Iraqis are very glad Saddam has gone. But President Putin, Dominique de Villepin, much of the Arab media and many ordinary people in both the West and the Middle East remain doubtful about the war's achievements. Something fundamental has shifted in international relations but it is not yet clear how the Middle East will benefit. Risk and regional analysts in universities, firms and institutes all over the world are working hard to build a clear understanding of the new situation. Janusian is no exception.

But regardless of the bigger picture it is time for business to get busy helping Iraq get back on its feet. The quicker businessmen can get trading, the quicker Iraq will become a thriving country once again and the less likely that civil war and extreme Islamism will be able to knock the country further off course. The opportunities for those firms that can assist with the logistics and supply of aid, as well as the rebuilding of Iraq's neglected and damaged infrastructure have been well publicised, and President Bush is said to be encouraging leading US firms to use British and Australian companies as major subcontractors. The normalisation that will inevitably follow reconstruction will see Western airlines, car showrooms, banks and manufacturers seeking to establish themselves in a new marketplace.

Janusian has been on the ground in Baghdad and Basra to assess the new situation. Gary Wood, Janusian director responsible for security, visited Iraq in late April to complete the setting up of Janusian's operation which will offer a full security service to companies wishing to do business in Iraq. By going to see for himself he was able to cut through the journalistic hyperbole which has obscured the reality on the ground and make a proper assessment of both the political situation in parts of the country and the logistics of setting up our operation. Gary's reconnaissance elicited some practical advice:

- The situation is still unstable. Unreconstructed pro-Saddamists, Islamists of various types and even jumpy US soldiers pose serious threats to safety;
- Basra is likely to settle down more quickly than Baghdad;
- Anti-US feeling, particularly in Baghdad, has been exaggerated in the media. The British seem genuinely popular in much of Basra;
- The smarter residential parts of Baghdad and Basra are physically intact and largely trouble-free. There are numerous attractive villas and apartments for rent at very good prices;
- The nature of the coalition's precise targeting means that many government buildings have been damaged or destroyed but the main commercial and business areas in both cities are relatively unscathed. However, communications are difficult: the landline telephone network is down and the regime prevented the establishment of a mobile network in Iraq;
- The exchange rate of the Iraqi Dinar to the dollar is gradually stabilising;
- Civil servants in non-security ministries have been asked to restart work;
- Most Iraqis are friendly and keen to do business but care needs to be taken – people are (naturally) hiding links to the Ba'ath party and the previous regime.

Janusian continues to receive daily intelligence updates from our local business contacts by satellite telephone.

At this stage security dominates our plans and assessments. Law enforcement is currently a real problem: rival gangs are shooting at each other in the streets and there have been terrorist-style



'Janusian continues to receive daily intelligence updates from our local business contacts by satellite telephone'

attacks on US forces. But some order is starting to return: both traffic police and fire services are returning to normal in Baghdad. In Basra local policemen are patrolling with the British army. And none of these problems is bad enough to stop the initial stirrings of the local commercial culture. For every resourceful bank robber there are ten resourceful and educated Iraqis keen to sell and trade and rebuild.

We are not suggesting that commercial operations will be without risk, however. On the physical side, expatriate staff in particular will be at risk from hostile elements in the population, and from possible terrorism and criminality. Selecting local partners and suppliers will also be risky: anyone with a connection to the Ba'athist regime will be *persona non grata*. These connections are unlikely to be obvious to Western companies which lost touch with their contacts during the 1990s sanction regime and are unfamiliar with the Iraqi business environment. Nevertheless, the Janusian view is that provided businesses take active measures to manage the current security and commercial risks and make sure that they partner appropriate Iraqis, they can move in now and get on with the job.

Crispin Black
Stuart Seymour is a
Director of Janusian
Security Risk
Management. If you
would like to know
any more about
security threats
consultancy, please
contact him at
black@janusian.com

Data protection – don't rely on employee consent

The principles underlying the Data Protection Act 1998 apply in all circumstances where personal data is processed, not least where a company holds and processes data about its workforce. Indeed, the processing often starts before the employment relationship is formed when an applicant's CV and application form are evaluated and information from interviews and tests is assessed. The position for companies which outsource background checking is further complicated because they are providing personal data, and sometimes sensitive personal data, from the candidate to a third party conducting the verification.

The principles include:

- Finality: data must be collected for specified lawful purposes and not further processed in any way incompatible with the original purpose (e.g. you can't use your employee records as a marketing database);
- Transparency: workers need to know what data is being collected, and to what purpose this data is being processed;
- Proportionality: personal data must be adequate, relevant and not excessive (e.g. you should not request driving licence details unless driving is a requirement of the job);
- Accuracy and Retention: data must be accurate, up to date and held no longer than necessary.

Where, as part of its recruitment process, a company takes up references or adopts more rigorous pre-employment screening, it therefore has to make its processes absolutely clear. Most firms require written confirmation from the candidate to signify understanding and consent, since the consent of the data subject is one of the conditions which may be relied upon to legitimise the processing of the information.

Or can it? Not necessarily. Firstly, national law may prevent the collection of the data: in the UK an employer may request ethnic origin or disability information in order to demonstrate compliance with anti-discrimination legislation; other European states make the collection of such information unlawful. Secondly, the European Data Protection Working Party, established under Article 29 of the EU Data Protection Directive¹, is of the opinion that consent should be a fall-back position. This means that where there is a real or potential relevant prejudice arising from not consenting the

'...personal
data must be
adequate,
relevant and
not
excessive..'



¹ Directive 95/46/EC

consent is not valid. Far better, the Working Party says, to rely upon one of the other conditions²: in an employment situation the most likely are that the processing is necessary for the purposes of legitimate interests pursued by the employer or, as would be the case for a regulated financial services firm, for compliance with a legal obligation.

This means that much care is needed in the design of documentation used for pre-employment screening. In many examples we have seen forms which ask for next of kin when an emergency contact number is what is really needed, ability in foreign languages (normally self-declared, rarely verified or used and usually not kept up to date), and details of children's age and sex (for employee benefits purposes). Our advice is that if you want your application form to collect information to be used for varying purposes it should be structured in such a way that this is clear, and that data fields which are not subject to verification in screening should be stripped out before the form is sent to the screening agency.

In summary: don't ask for information you don't need, make it clear what you are going to do with the personal data you have collected, and only keep the data for as long as you need it. To meet the Information Commissioner's code of practice on recruitment and selection, we are routinely purging our files six months after a candidate has been screened and recommending to all our clients to review carefully what personal data is being retained and for how long.

Alan Beazley
Alan Beazley is a Director of Zephon Employee Screening. If you would like to know more about employee screening related issues, please contact him at alan.beazley@zephon.com

Entente commerciale? How the US and the French do business...

French opposition to the Bush administration's war on Saddam Hussein has brought French-US relations to a new low. Animosity between the 'cheese eating surrender monkeys' and their transatlantic ally is by no means new, however. Since the disintegration of the bi-polar world successive French governments have been increasingly suspicious of their American counterparts. There are two widely held perceptions in France. First, that the US is attempting to impose its vision of democracy and free market economy on the rest of the world; and second, that it is willing to attempt to abuse both these concepts in its efforts to do so. Likewise, ever since de Gaulle pulled out of NATO in 1966 and the French became one of the driving forces behind the European Union, the Americans have regarded them as a troublesome and unreliable ally. These differences have led to continued discord between the two permanent Security Council members.

This distrust has affected private business on both sides of the Atlantic. Some causes of friction between the two countries have been vented through international institutions such as the World Trade Organisation. However, many trade disputes go unresolved: the EU is still considering imposing trade sanctions on a list of US exports worth \$2 billion, retaliating against tariffs imposed by the US government on steel imports in March 2002. The Americans for their part are fighting an EU ban on US beef from hormone-treated cattle as well as a lengthy 'banana war'. One particularity of French and US disputes has been a backdrop of accusations and counter-accusations, each side blaming the other of fighting a global, covert and dirty economic war.

No one contests that industrial espionage is a serious and costly issue. In 1999 Thomas Donahue, US Chamber of Commerce president, said there was no greater threat to global business competitiveness. He added that the cost of industrial espionage to US companies in 1999 was estimated at \$2 billion a month. The same year a study sponsored jointly by the American Society for Industrial Security and PricewaterhouseCoopers stated that the theft of confidential and proprietary business information had cost Fortune 1000 companies more than \$45 billion.

US governmental institutions have always singled out France as one of the main perpetrators of economic espionage. [Economic espionage in this sense must be differentiated from corporate or industrial espionage. In the former, a foreign government is the culprit, gaining access by covert means to economic intelligence such as proprietary information or technology. In the latter, only

² Data Protection Act 1998, Schedule 2

private sector entities are involved.] James Woolsey, a former director of the CIA, is quoted in Duncan Campbell's book, *I Spy An Ally*, saying that of the countries who spy on the US "from Germany to Korea, France heads the list". Woolsey later claimed he was misquoted but there are many echoes of this view to be found in Washington.

On their side, the French have led the way in denouncing the American global eavesdropping network Echelon. [The Echelon network is run by the National Security Agency (NSA) with the co-operation of Canada, Britain, Australia, and New Zealand. The British element is based at the GCHQ station in Morwenstow, north Cornwall. It reportedly intercepts communications worldwide and, according to one source, the system 'is capable of listening to and processing the equivalent of the entire content of the US Library of Congress in ten hours'.] In March 2000 Woolsey distinguished himself again by formally acknowledging the existence of the Echelon system in an open letter published in the *Wall Street Journal* entitled 'Yes, my Continental European friends, we have spied on you'. He argues that the US had been forced to do so in order to enable American companies to compete fairly with European firms who 'resort to bribery to compete'. To date the US government has officially refused to confirm the existence of Echelon. In April 2000, before the House Permanent Select Committee on Intelligence, George J. Tenet (current director of the CIA) restricted himself to saying that allegations that 'the so-called Echelon program of the National Security Agency' was involved in economic espionage were untrue: "The notion that we collect intelligence to promote American business interests is simply wrong. We do not target foreign companies to support American business interests."

So what has this war of words between France and the US actually meant for private business? A few high profile examples of economic espionage involving both countries have been widely reported in the international press. In 1992 several press articles reported that the FBI was warning American travellers away from Air France, claiming microphones were built into the headrests of business class seats and that undercover agents were posing as stewards. In 1994 Boeing and McDonnell Douglas were said to have beaten Airbus to a \$6 billion contract to supply jets to Saudi Arabia, thanks to Echelon intercepts of faxes and phone calls. In the same year and for the same reasons Thomson-CSF (now Thales) was reported to have lost a \$1.3 billion contract in Brazil to the US defence contractor Raytheon. In 1995 the DST (French Directorate of Territorial Surveillance) was reported to have unmasked and expelled a Paris-based CIA spy ring allegedly collecting sensitive commercial information. In 2000 US intelligence sources foiled a French secret service attempt to sabotage the trials of British Challenger 2 tanks competing for a £1.2 billion tender for the Greek government. More recently, on 19 March 2003 the discovery of sophisticated bugging devices in EU offices led the French press immediately to blame American services³.

Who is at risk? Technology industries appear to be the most frequent targets, specifically aerospace, biotechnology, defence technology, telecommunications and energy research. A review by the Canadian Security and Intelligence Service lists various indicators of economic espionage. These include: unsolicited requests for proprietary information, inappropriate conduct during visits, suspicious work offers, targeting at international exhibits and conventions, and the co-option of former employees. The review concluded: 'Many companies do not report incidents of economic espionage out of embarrassment, or for fear of stock market or other negative consequences for the company.'

To try to protect private enterprises, France and the US have introduced various pieces of legislation. In 1996 the US Congress enacted the Economic Espionage Act (EEA). This addresses and criminalizes both domestic and foreign economic espionage. By 2001 twenty-three cases had been prosecuted under the EEA. In France EU legislation and a 30 September 2001 amendment of the Code Pénal addresses FCPA and economic espionage issues. However, the 2002 OECD anti-bribery report points out deficiencies in both countries' legislation and the difficulty and political implications of enforcing these laws.

Before 11 September 2001 the US spent an estimated \$26.7 billion annually on its combined intelligence staff. During this time the combined yearly budget of the DST and DGSE (General Directorate for External Security) stood at around \$166 million. With the end of the Cold War security

³ *Le Figaro*, 19 March 2003

'Technology industries appear to be the most frequent targets...'



services had increasingly focused on economic espionage and counter-espionage, especially in industries deemed important to national interests. The American administration's war on terrorism has reversed this trend and there are signs of better cooperation between France and the US in terms of intelligence gathering. In early 2001 the DST apprehended Zacarias Moussaoui, a French Algerian, who had taken flying lessons in Boston and passed his file to the FBI (which ignored it). This increased cooperation in the face of new terrorist threats, the embarrassment of getting caught and the tightening of legislation in both countries should reduce the political will to use espionage as an economic tool.

At the same time private businesses have taken the threat of economic and industrial espionage much more seriously, developing in-house departments or using external business intelligence firms to respond to such risks. For the moment, though the French business community is waiting to see what sanctions the US might impose on them in retaliation for President Chirac's refusal to accept American motives for the war on Iraq.

Kevin Braine

Kevin Braine is an Associate of The Risk Advisory Group. If you would like to know more about due diligence, please contact him at kevin.braine@riskadvisory.net

The Potemkin Village - is Russian corporate governance being overrated?

In the majority of investigations we carry out in Russia, companies cite transparency in shareholding and other corporate disclosures as the key obstacles in finalising transactions, be they an acquisition, merger or joint venture. Those most concerned with this lack of transparency are institutions considering private clients, partners in joint ventures and potential equity investments.

Given that companies in Russia are keen to access foreign financing and markets, the trend has to move towards greater openness in Russian corporate disclosure. But what are the obstacles still discouraging investors? Russia has made a number of theoretical improvements to its laws and corporate procedures, but there is a sneaking suspicion among many investors that the changes are cosmetic in nature and have made little impact on real transparency. For example, Russia has been removed from the Financial Action Task Force list of countries with critical deficiencies in tackling economic crimes such as money laundering, yet we still see the prolific use of offshore companies to conceal ownership, hide capital flows and engage in asset stripping. In this article we examine the degree to which standards of corporate governance and transparency have changed in recent years.

The legal framework

The Russian legal framework has attempted to encourage greater transparency through requirements to disclose information, trends in company registration and improvements in availability of information. However, we consider these changes to lack 'teeth'. We would highlight the following:

- There is allegedly tougher control over share (joint stock companies) companies by the Federal Commission for Securities Market (FCSM). It now charges higher fines for the delayed submission of reports. Standard & Poors and other lobbyists have persuaded the FCSM to adopt The Corporate Governance Code as a set of recommendations rather than as a law – therefore, they have very little control over the degree of information disclosure itself.
- Russian banks will soon be requested to disclose beneficial owners of companies to the Central Bank. This is a draft law prepared by the Ministry of Finance. Although this is an extremely positive development it still needs to be approved by parliament, where bank owners have a strong lobby capable of blocking any motion.
- Company registration has been centralised and handed over to the Tax Authority instead of regional registration chambers. This has generally been perceived as a failure. The Russian Tax Ministry lacks the infrastructure, IT systems of the required



'...companies cite transparency in shareholding and other corporate disclosures as the key obstacles in finalising transactions...'

number and capacity and the operators to enter the data. The new system is simply not in place.

Evasion and opacity

At The Risk Advisory Group we have not seen a significant drop in the nature and scale of problems encountered by clients investing in Russia. These may take the form of:

- 'Grey' techniques being used by managers to defraud investors, or by groups of investors to deceive other groups of investors. These include the use of nominee accounts, front companies or puppet directors.
- 'Tax minimisation' schemes – for import, export, retail trade, salaries and so on – are still highly prevalent in Russian business. It is often very difficult to distinguish these from straight fraud. The Russian government is reputed to collect RUR500 billion of annual VAT and then loses RUR100 billion in annual VAT-reimbursement fraud.
- 70 percent of the commercial banks in Russia (by number, not by combined assets) are estimated to thrive on 'tax minimisation', VAT fraud and other similar types of transactions through 'Black Hole' jurisdictions. These zones include Russia's inshore tax havens – Kalmykia, Ingushetia, Dagestan – and offshore destinations – Montenegro, Liechtenstein, Latvia etc.

The future

So what is the future for Russian corporate disclosure and openness? Russian companies which are genuinely interested in attracting international investment and in increasing their own asset value have realised the importance of higher transparency and better corporate governance. The same trend has been shown by owners of private Russian companies who have realised the limits of growth for their companies if they remain privately controlled. These owners are willing to sell their businesses or significant stakes in them, and they are interested in getting a higher price.

Yukos, Vimpelcom, Wimm-Bill-Dann, Norilsk Nickel, Sibneft and some of the new regional venture capital funds operating outside Moscow are perceived as models for good corporate governance. Yet away from the headlines Sibneft, for instance, has not been forthcoming in disclosing its ownership structure. Are the market favourites as transparent as they claim – or are some simply being pushed by their stockbrokers?

Talking 'corporate governance' has become fashionable at a senior government level, making it easier to pass related changes to the legislation. The Kremlin, for instance, cannot achieve a higher degree of control over the Russian oligarchs without greater corporate transparency. But as one prominent Western investor remarked recently: if you make an effort to be a good corporate citizen, "you can keep what you stole. The world is very forgiving of wealth."

If you have any comments or feedback regarding any articles in this issue of *Risk Advisory* please contact Sal Remtulla in marketing on 020 7578 0000 or email at sal.remtulla@riskadvisory.net

Philip Worman
Philip Worman is a Director with The Risk Advisory Group. If you would like to know more about any issues related to emerging markets, please contact him at philip.worman@riskadvisory.net

Oleg Babinov
Oleg Babinov is a Director with The Risk Advisory Group, Moscow. If you would like to know more about any issues related to emerging markets, please contact him at oleg.babinov@riskadvisory.net