



Global Fraud Report

- 2 Corruption and anti-corruption:
Raising the stakes
- 3 "Just when you thought it was safe
to go back in the water..."
- 4 Italian style fraud: Conflict of interest
as common practise
- 5 The relationship between public and
private sector fraud
- 6 Fraud and D&O Liability Insurance
- 7 Germany's stronger anti-corruption enforcement
- 8 Fraud at the breakfast table: A recipe for confronting
product adulteration in agribusiness
- 10 The FCPA landscape has changed:
Trends in enforcement
- 13 Fraud in bankruptcy in the USA
- 14 How to survive and thrive in corrupt markets
- 16 The ASEAN-China Free Trade Agreement:
An IP protection challenge for everyone
- 17 Fraud news
- 18 Kroll contacts

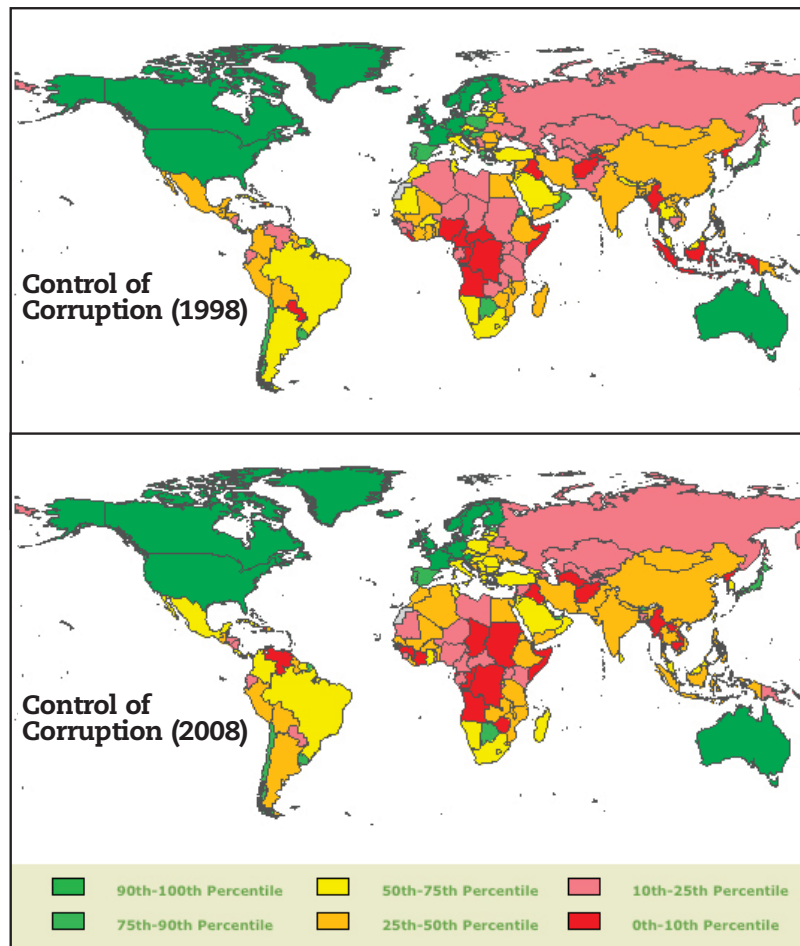
Corruption and anti-corruption: Raising the stakes

In 2009, Transparency International's Global Corruption Barometer found that 69 percent of worldwide respondents believed that their national political parties were corrupt and 61 percent said the same for legislatures. Political parties and civil servants were listed as the most corrupt institutions within society.

Across the globe, corruption paints a consistent picture. Corruption disproportionately impacts the least well off in all countries and afflicts worst in the poorest states. In spite of multilateral efforts to tie aid to good governance and rising awareness levels, corruption levels have barely altered in the last 10 years, evidenced by the two maps here.

Two recent trends bode ill for the combat of corruption. The global financial crisis and the stimulus spending that emerged in dozens of countries around the world improved the conditions for fraud.

Even more significantly, the financial crisis has helped accelerate a decade long shift in the world's economic center of gravity from a "Western" economic omnipotence to a world whose growth is driven by emerging markets. With a few notable exceptions (e.g. Chile, Qatar, Uruguay), emerging markets are still characterized by comparatively high levels of corruption. In many cases, efforts to reduce corruption in emerging markets is stymied by a lack of political will or a weak judicial system that is too easily manipulated by more powerful economic interests. The generation of wealth in emerging markets, by and large, is outpacing the speed at which these countries can reform the judicial and civil society infrastructure needed to combat corruption. In several resource rich nations, the recent commodity bonanza that endured from 2003 to 2008 may have in fact undermined a lot of positive reforms undertaken in the 90's. Globally, the fight against corruption is as challenging as ever.

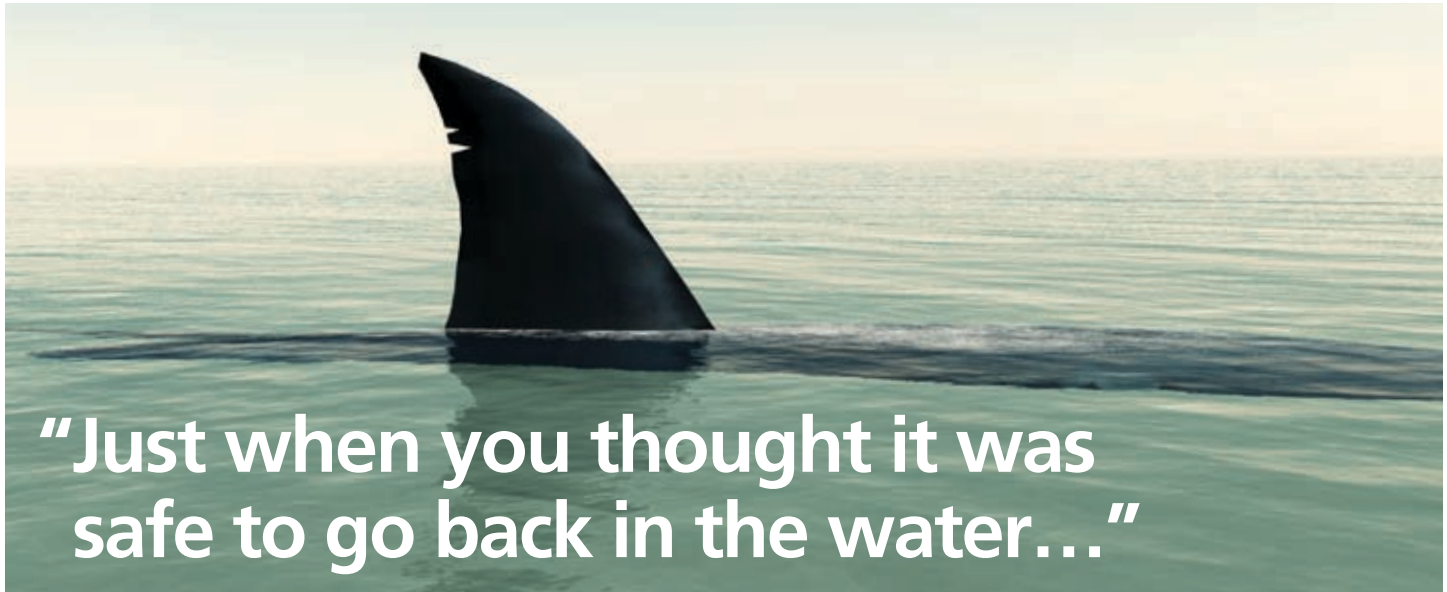


Source: Kaufmann D., A. Kraay, and M. Mastruzzi 2009: Governance Matters VIII: Governance Indicators for 1996-2008

Meanwhile, though, Western countries are doing more to crack down on corruption by their domestic companies, including their operations overseas in emerging markets. The best example of this trend is the rapid expansion of US enforcement of its Foreign Corrupt Practices Act (FCPA). American authorities are not only increasing their number of prosecutions, they are going after a wider variety of companies – small and large, public and private. Moreover, they have indicated that they will use links with the United States to pursue cases where they find evidence of corruption. This puts almost any sizeable non-US firm within their grasp. In late 2008, the German multinational, Siemens, agreed to pay a total of US\$1.6 billion in fines to United States and German

authorities to settle an investigation. In February 2010, British defense supplier BAE Systems agreed to pay nearly US\$450 million to American and British authorities. The net result is that, even as globalizing companies face increasing opportunities to engage in corruption, particularly in emerging markets, the risks and costs of doing so are rising dramatically.

This issue of the Global Fraud Report is designed to help readers better understand the changing dynamic of global corruption. Of course, this is but one challenge facing companies so we have dedicated content to addressing other timely concerns including: the intellectual property fraud implications of the new China-ASEAN Free Trade Agreement; and some of the ongoing implications of the economic downturn.



Tommy Helsby

You have carefully designed your Foreign Corrupt Practices Act (FCPA) compliance program, making sure that all staff know their obligations under the law; then you hear that the new UK Bribery Act has a different set of restrictions. You have developed a state-of-the-art know-your-client anti-money laundering system; then you find you are being prosecuted under data protection laws for losing a memory stick containing customer details. You've been working through your trade association to ensure your operations exceed health and safety and environmental standards, whereupon you get raided by EU investigators for suspected anti-competitive behaviour. It's just not safe out there any longer.

Regulators have started regulating again. For years, the regulated seemed to have the whip-hand, whether through lobbying at the legislative end or the best professional resources at the investigation and prosecution end. From numerous conversations with regulators and with clients, it's clear that the days of regulatory capture are gone: there is a strong public interest in aggressive application and pursuit of existing rules and laws, and the introduction of new ones to strengthen the regulators' position. The most visible example today is in anti-bribery measures.

No legitimate company could view giving (or receiving) bribes as acceptable; but for a significant minority, it may sometimes have been viewed as a necessary evil. Others sometimes just turned a blind eye: "don't ask, don't tell". Certain parts of the world were seen as irredeemably corrupt: West Africa or Central Asia¹, for example. The US passed the FCPA in 1977 but ten years ago there were only a handful of investigations underway. For many years, foreign bribes were tax-deductible in Germany under certain circumstances². All this has changed dramatically: today, the US Department of Justice (DOJ) has 140 FCPA cases under investigation, and several of Germany's largest corporations have been prosecuted.

In the UK, the new Bribery Act has finally become law and, in many respects, is broader than the FCPA. Even without this new legislation, the Serious Fraud Office (SFO) has started to devote substantial resources to corruption investigations, and has already achieved a number of settlements with UK companies.

The SFO, like the DOJ, has made it clear that companies which come forward with a full independent investigation of problems that they have discovered will be treated more leniently. Part of the new regulatory agenda is to put the onus on the regulated to do the work, and then to demonstrate that it was done thoroughly. In our experience

of a number of such internal investigations, this works well. It does require the company to approach the problem positively and resolutely; half measures will undermine the credibility of the effort.

Most often, we see these problems come with an acquisition, either because the acquired company does not have adequate compliance procedures (often the case with private companies) or because the new broom of the acquirer stirs up dust from some forgotten corner of the acquisition. In other cases, it is the actions of an agent, inadequately scrutinized and supervised, until someone else – a journalist, a whistleblower, a competitor – points the finger. Thorough integrity due diligence, of acquisitions and of agents, is critical (traditional legal and accounting processes will probably not be enough) to spot the risk areas and warning signals, to focus attention into the right places and, if all else fails, to provide some defense in the event of a problem.



Tommy Helsby is Chairman of Kroll Eurasia based in London. Since joining Kroll in 1981, Tommy has helped found and develop the firm's core due diligence business, and managed many of the corporate contest projects for which Kroll became well known in the 1980s. Tommy plays a strategic role both for the firm and for many of its major clients in complex transactions and disputes. He has a particular interest in emerging markets, especially Russia and India.

1 http://www.transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table
2 <http://www.oecd.org/dataoecd/58/10/41353070.pdf>

Italian style fraud: Conflict of interest as common practise



Marianna Vintiadis

Few might be surprised to learn that fraud in the shipping industry differs dramatically from a financial sector scam. Nobody would expect a logistics company to be hit by a Ponzi scheme and banks rarely suffer from excessive inventory scrap. But would a fraud in France typically differ from one in Italy? Surprisingly, yes. Local, legal, institutional, and cultural norms do help differentiate fraud schemes. This impacts the frauds themselves as well as the optimal detection practices and post-fraud investigative tactics.

Kroll's experience in Italy shows that the questionable management of conflicts of interest by the corporate sector, an endemic problem, opens the door to many types of fraud, regardless of business sector, location within the country, company size, or ownership structure. It begins at the top with the issue of interlocking directorships.

At the end of 2008, the Italian Antitrust Authority (Autorità Garante della Concorrenza e del Mercato or AGCM) published a report on the relationship between competition and corporate governance in the financial sector. It revealed that interlocking directorates are common among Italian banks and insurance companies. Individuals holding directorships of competing companies were present on the boards of approximately 80 percent of the

financial groups examined. One board had a staggering 16 directors with multiple positions. If non-listed competitors in the industry are included, the figure rises to 90 percent.

According to the AGCM, interlocking directorates are a peculiarly Italian phenomenon. The percentage of listed, competing companies connected by personal links in Europe is, on average, far below 80 percent. In the United Kingdom, the figure is 47 percent, in Germany 43 percent, in France 26 percent, and the practice hardly exists at all in the Netherlands.

Formally, the Italian Civil Code protects competition. However, the relevant article on directorships, Article 2390, is in fact very weak: a corporate general meeting decision can allow a company director to become a shareholder or director of a competitor, or even to set up a new competitor. Appropriate self-regulation rarely compensates for regulatory weakness in preventing or neutralizing the effect of such personal links.

What the AGCM reports for the financial sector is just one part of a much broader web of interwoven interests reaching to other blue-chip companies, the media, and beyond. It is not surprising, then, that frequent requests are made in Italy to investigate managerial conflicts of interest, with the most common outcome being that the manager in question owns - in his name or that

of a family or friend - one or multiple suppliers who sell to the company.

Detection can be difficult if the supplier company is owned by a friend or a relative by a different name. The presence of fiduciaries is also common in more sophisticated, deliberately fraudulent attempts to hide the beneficial owners.

It is very difficult to prove this kind of conflict of interest in the current climate. To start with, people do not always consider owning a share in a supplier - directly or through a relative - as a serious offense or even a problem. Moreover, the tools at the disposal of investigators or lawyers are often insufficient to pierce the corporate veil and judges will not authorize requests for ownership disclosure in the absence of hard evidence of fraud.

Our advice is that the answer lies in prevention. "Know your supplier" policies - requiring ownership disclosure at the time a contract is signed - and clear codes of ethics can go a long way in avoiding this all too common problem.



Marianna Vintiadis is Kroll Country Manager for Italy and Greece. A trained economist with experience in policy making and analysis, she works on business intelligence and complex investigations in these countries. Her specialist areas include market entry, shipping, piercing the corporate veil, and Internet investigations.

The relationship between public and private sector fraud

Javier Cortés

Working on fraud and corruption investigations, Kroll has seen that the private sector in most countries is a reflection of the public sector. Legislation, legal safeguards, and especially control of public corruption define how the private sector deals with the issue. Regardless of the varying forms in which official corruption appears from country-to-country, it inevitably seeps through to the business world.

Take Spain, for example, where corruption in the real estate sector began when regulators started accepting favors from the private sector in exchange for granting construction permits. This *quid pro quo*, in turn, encouraged the private sector to think that it had to offer “favors” outside of the business framework in order to get things done. In the face of government inaction, private capital from organized crime groups flowed into the financial system via money laundered through private companies. The cycle of corruption continued, as the lack of sanctions within the system created a perception of impunity. The damage spread further as consumers ended up with housing of lower quality, and at a higher price, than market value. As the problem spread, the public sector acted more like a passive audience than an active participant.

The problem is not limited to those firms that are directly infected by public sector fraud and to their customers. Indices that measure the perception of public sector corruption have a direct impact on foreign investment and market confidence in a country, as the image that outsiders have of a country’s civil service is often transferred to that nation’s private sector. High levels of perceived corruption make foreign firms reticent to invest.

It is of no small concern that official corruption seems to be on the rise globally, according to Transparency International (TI), which compiles data on perceptions of public sector corruption. From 2008 to 2009, every region of the world outside of the European Union/Western European zone, witnessed increases in perceived corruption among public officials and civil servants. Within Europe, improved perceptions of civil servants in Norway, Poland and Lithuania slightly offset declining attitudes towards their counterparts in Italy, Greece, and, of course, Spain (among others). Only in the Middle East and North Africa – home to many of the highest ranked countries for perceived corruption – has the problem remained relatively unchanged. Perceptions of public sector corruption grew fastest in the countries of Eastern Europe and Central Asia.

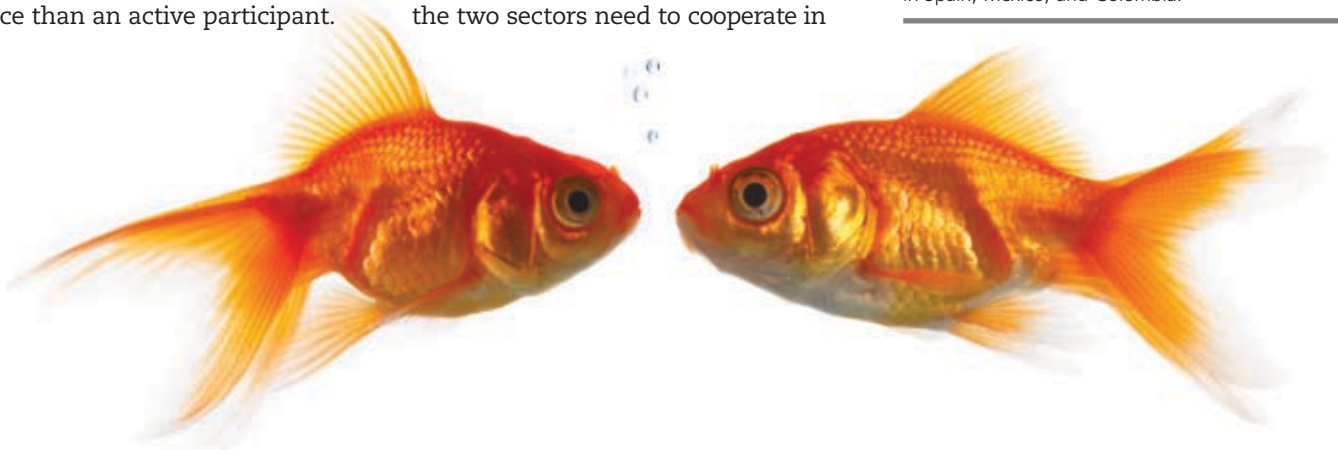
Public and private bodies must, of course, ensure that their own houses are in order on corruption. Ultimately, however, the two sectors need to cooperate in

order to replace the current negative dynamic with a more positive one.

The opportunities for improving the situation appear to be growing. The International Chamber of Commerce, the Organization for Economic Co-operation and Development (OECD), TI, and the United Nations Global Compact all promote such public-private cooperation. The Basel Institute on Governance, based at the University of Basel, Switzerland, brings together private and public organizations in its Centre for Governance and Anticorruption and its International Centre for Asset Recovery, both of which deal with specific, technical details of the fight against the problem. Meanwhile at the national level in Spain, cooperation between the two sectors is led by the Office of the General Anti-Corruption Attorney. It runs seminars, training sessions, and workshops, and works with private sector risk officers as well as law enforcement organizations in order to enhance anti-corruption efforts. Both the public and private sectors have much to gain from working together on an ailment which, if left unchecked, inevitably infects both.



Javier Cortés is a Director in Kroll’s Madrid office. He has worked in projects with the National Police of Nicaragua and Colombia, running organizational restructuring and anti-corruption programs in conjunction with the Spanish Cooperation Agency. Prior to joining Kroll, he also worked in several fraud prevention projects for banks, the distribution sector, and the pharmaceutical industry in Spain, Mexico, and Colombia.





Fraud and D&O Liability Insurance

John Batch

The current economic climate is exposing firms to an increased risk of fraud and corruption. Frequently, when fraud does occur, senior managers are left facing the fallout.

Companies which have not traditionally considered fraud to be an area of particular risk now face a different reality. In hard economic times, senior managers in every organization need to understand that such crime is increasingly likely to occur internally. In fact, their organization may be targeted specifically if investment in fraud risk management and hard-wired security systems has in the past been less of a priority.

Dean White, a managing director in Marsh's financial and professional practice, notes, "Any instability or volatility in a person's life or personal circumstances can increase the motivation for committing fraud. The need to safeguard a financial position or a lifestyle is just as powerful a motivation as the need to fund gambling or a drug habit. An economic downturn is often the root-cause of behavior that can ultimately lead an individual to turn to fraud."

Meanwhile, changing business practises bring with them new risks. Internal fraud – where individuals have detailed knowledge of company

systems, processes, and controls – has traditionally been the principal concern of most senior managers. However, outsourcing, off-shoring, project working, using joint ventures, and external partnering can lead to more complex systems and create more "technical insiders" with knowledge traditionally reserved for employees. Key knowledge and oversight can be lost or abused as companies tend to supervise these extended systems less.

Too often executives and businesses are unprepared for these growing risks. For example, Britain's Fraud Act of 2006 significantly clarified the relevant law, but many commercial crime insurance policies neither reflect this legislation, nor do they consider increasingly sophisticated criminal activities and the resulting financial consequences. Instead, coverage remains stuck in the past, with protection that provides an indemnification for a physical manifestation of loss – something closely associated with theft – rather than for a financial loss resulting from theft, fraud, or dishonesty. This gap leaves businesses with a significant risk exposure.

Senior managers have a key role in working with insurers and risk advisors to determine the efficiency of their existing cover and analyze any potential gaps. Directors' and Officers' (D&O) insurance is particularly relevant in that it protects directors and officers

from suits related to their actions or inaction. It does not cover dishonest or fraudulent acts by these executives themselves, but most policies do include legal defense costs until the matter is decided by the courts.

Despite the economic environment and changes in business practice, D&O liability insurance has been getting less expensive for many companies, with the notable exception of financial institutions. Although the frequency of smaller claims has increased significantly, mainly due to more investigations by regulators, larger claims are not materializing. Meanwhile, increasing competition among insurers is helping to keep premiums down.

In today's volatile market conditions, adequate D&O cover for senior managers is essential. Regulators and politicians are now holding individuals accountable, so people are more acutely aware of their personal vulnerability. As a result, directors and other executives are more sensitive to risk than they were in the past. Executives would do well to take stock of their firms' exposure to fraud as well as their own resultant personal liability.



John Batch is a Senior Vice President for Marsh's FINPRO practice, with a focus on Management Liability, including Directors and Officers Liability. He advises several FTSE 100 companies and major European countries on these classes of insurance.

Germany's stronger anti-corruption enforcement

Alexander Keselica

For years, German commentators have written about the roles bribery and corruption play in business transactions. Estimates suggest that German companies pay a collective total of US\$33 billion in bribes abroad annually, much of which goes unaccounted for and unpunished. Recently, however, anti-corruption enforcement efforts have become front page news.

In February 2010 it was reported that Daimler was close to reaching a settlement with the US Department of Justice and the Securities and Exchange Commission regarding an investigation into breaches of the Foreign Corrupt Practices Act (FCPA). This comes on the heels of the well-publicised Siemens bribery scandal settled at the end of 2008.

German companies are not falling foul of only international anti-corruption regulations. The country's national authorities are becoming just as active, and if not more so, than many counterparts worldwide. Transparency International's 2009 Progress Report on the OECD Anti-Bribery Convention rated Germany as having "Active Enforcement" of the treaty, making it one of only four countries with that status out of 36 surveyed. By the end of 2008, Germany also had the second highest number of foreign bribery cases being tried (110), slightly behind the United States (120) but well ahead of third place Hungary (24). Statistics from the German Federal Crime Agency (Bundeskriminalamt) also indicate pronounced activity. In 2008, 8,569 corruption offenses took place in Germany and the authorities undertook 1,808 preliminary investigations into such crimes. Enforcement is also

taking place regionally. Many of the German Länder have established their own anti-corruption units.

Coming from one of the world's leading exporters, German companies find themselves doing business in all corners of the world, often in countries where authorities turn a blind eye to bribery, therefore increasing corporate exposure to various risks. These domestic enforcement efforts, along with foreign ones, are forcing German companies to take a closer look at where and with whom they do business.

Enforcement efforts are also bringing to light the potential costs of corruption. In Germany, convicted individuals face possible fines or imprisonment. Companies can be fined up to one million euros, plus potentially far higher amounts to confiscate any economic advantage proven to have been gained through the bribes. Other international legislation, including the FCPA and Britain's proposed Bribery Bill, also have steep penalties for both companies and individuals, including unlimited fines and prison. Further risks include:

- potential downsizing or termination of certain business lines;
- interdiction of government contracts; and
- tarnished reputation.

German authorities have also shown a greater willingness to cooperate with their peers around the world, making it harder for bribe payers and receivers to avoid being caught. Moreover, such cooperation means that companies can be punished multiple times for similar violations.

As German anti-corruption enforcement efforts strengthen, the country's companies must adapt.



Regulators will be looking for evidence of a robust compliance program promoting a certain level of ethical standards among all employees. Moreover, companies must show that they are making an effort to stay out of trouble by reviewing their business partners; understanding the political and commercial culture of the jurisdictions in which they operate; and monitoring key red flags, such as significant payments to offshore jurisdictions or the unusual use of third parties, agents, or intermediaries. Finally, companies must be pro-active in investigating any potential wrongdoing that may be identified. They need to gain an understanding of all its aspects – including its cause and the parties involved – and determine how best to prevent a re-occurrence.

Enhanced systems and processes may not prevent corruption, but implementing them goes a long way toward mitigating the growing regulatory risks that German companies face.

Alexander Keselica is an Associate Director for Kroll based in London. He joined Kroll in 2005 and co-heads Kroll's business intelligence work in German-speaking countries. During his time at Kroll, he has worked on a wide variety of assignments, including FCPA due diligence projects, international fraud investigations and asset recovery exercises.



Fraud at the breakfast table: A recipe for confronting product adulteration in agribusiness

Vander Giordano

Humans need food to survive. Businesses that produce food touch the lives of billions of people and generate billions of dollars in annual revenue. Yet despite – or perhaps because of – their key role in the global economy, agribusinesses can be vulnerable to fraud in the form of product adulteration.

To illustrate the threat, consider the kinds of food that wind up on your family's breakfast table each morning:

- The coffee industry often sees unscrupulous competitors manipulate products by mixing in impurities like cornmeal and other cheaper substances.
- For milk producers, the fight is against companies that add whey or water to the product in order to increase the volume and obtain inappropriate gains.

- Grain producers can be the victims of fraud when they purchase liquid pesticides for use on their crops. In some cases, these concoctions contain no active ingredient and can be completely ineffective against pests.

The consequences of fraud and product adulteration are numerous and serious. Most obviously, product adulteration poses a public health risk. It can also compromise the reputation of exporters, damage the credibility of importers, and erode the sales and market share of legitimate companies.

Agribusinesses have a choice in how they deal with the threat of adulteration and other fraud. One approach is to wait passively for signs of fraud to emerge – accidentally discovering adulterated products in the marketplace, for example, or learning of a problem through employee or customer complaints.

The other approach is to set up an advanced detection program to uncover telltale signs of adulteration before the fraudulent activity occurs. Kroll's investigations have found that product adulterators tend to fit a certain profile. They are generally new to the market and do not participate in important industry associations. They tend to conduct business using a convoluted network of corporate entities and disclose little information beyond a post office box address. These "bottom feeders" price their products far below industry averages, shy away from established retailers, fail to pay taxes, and, of course, use low-quality or ineffective products.

After conducting an investigation, agribusinesses should take decisive action to confront the fraud and communicate with key stakeholders. Consider the approach taken by a



leading agriculture company to the fake pesticide problem mentioned above. After learning the truth about the bogus insect repellent, company leaders worked with the firm's sales staff to design a publicity campaign. Their campaign sought to clarify the situation for customers and to mitigate brand risk associated with the pesticide source. In this example, the company also created a taskforce to notice patterns in seasonal data and thereby anticipate risks associated with the seasonal nature of pesticides.

Cooperation within the agribusiness industry could also be effective against fraud. Coffee and milk producers – whose products are often used in tandem – face similar issues and might consider working together to fight adulteration practices. Their respective trade associations could gather data from a broad range of retail sources, get ahead of adulteration trends, and

respond more rapidly to a common threat. Such data could also be used to convince regulators to step up enforcement activities. The creation of "seals of quality" – which has been used to good effect by the coffee industry and could be copied by milk producers – can help corral adulterers by helping consumers differentiate between good and bad products.

Adulteration is, of course, not the only fraud risk facing the agribusiness sector. The number of companies, for example, that obtain financing via false guarantees is growing. These practices generate mistrust in the industry as a whole and increase the cost of borrowing, thereby harming legitimate firms that may need financing to maintain their competitiveness. Unlike the frauds discussed above, however, resolution of this issue lies largely in the hands of the banks. It can only really be

remedied through stricter client selection criteria as well as enhanced know-your-client policies and due diligence.

Regardless of the type of fraud, identification and prevention activities conducted by companies will be always guided by the quantity and quality of information gathered. Kroll's recent investigations into product adulteration have helped clients develop comprehensive programs that have led to recovery of losses. Investigation and prevention are essential ingredients in the recipe for beating product adulteration in the agricultural industry.



Vander Giordano is a Managing Director based in Kroll's São Paulo office and specializes in business development for Latin America. He is a member of the Brazilian and International Bar Associations and has worked in a number of areas in the airline industry.



The FCPA landscape has changed: Trends in enforcement

Jeffrey Cramer

On 18 January 2010, 22 business executives were arrested and over 100 FBI agents conducted related searches. These actions were based on sealed federal indictments handed down by a grand jury several weeks earlier, which in turn stemmed from a two-and-a-half year undercover operation. The indictments claimed

that the defendants believed that they were involved in a scheme to acquire a US\$15 million defense contract to outfit the presidential guard of an unnamed country. They allegedly agreed to pay a 20 percent bribe to a sales agent, supposedly representing the defense minister but really an undercover FBI officer. This was the first large-scale use of undercover law enforcement techniques to investigate

Foreign Corrupt Practices Act (FCPA) violations.

With those indictments, federal law enforcement officials announced to the world that the FCPA landscape has changed. Although perhaps the most dramatic shift, the use of undercover operatives is only one of several new FCPA enforcement techniques. The legal and business communities now



know that the Department of Justice (DOJ) is making good on its promise to crack down on companies which seek to bribe foreign officials in the course of business.

What is the FCPA?

The FCPA makes it illegal for any person acting on behalf of a domestic or foreign company listed on a United States stock exchange to give anything of value to a foreign government official in order to obtain or retain business, or to secure an improper business advantage. Under certain circumstances and in some countries, nearly every aspect of the approval, manufacture, import, export, pricing, sale, or marketing of a product will involve a “foreign official” as defined by the Act.

While the FCPA’s record-keeping and internal control provisions apply only to “issuers” – companies with securities traded on a United States stock exchange or otherwise required to file periodic reports with the Securities and Exchange Commission (SEC) – its anti-bribery provisions apply equally to “domestic concerns.” These include “any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship” with a principal place of business in the United States or organized under its law. Thus, these provisions apply to public and private companies. Indeed, several recent FCPA enforcement actions targeted foreign activities by private American firms.

Enforcement trends

The FCPA came into force in 1977, but was initially rarely used. Since 2005, though, several enforcement trends have appeared. First, the DOJ and SEC have increased the number of FCPA prosecutors and investigators and brought more cases. Second, the investigations have grown more aggressive, targeting individuals as well as companies. Third, companies have begun to disclose potential violations to law enforcement officials before an investigation has begun. Finally, and more recently, officials are looking more at small and mid-sized companies.

More cases: Since 2005, the DOJ has brought over 60 FCPA cases – more than the total between 1977 and 2005. The Fraud Section of the DOJ’s Criminal Division has developed a group of experienced prosecutors who specialize in this work. Separately, in 2007 the FBI created in its Washington Field Office a squad of dedicated FCPA agents which has since grown in size and experience. The SEC has also created a specialized FCPA unit to focus on new and proactive approaches to identifying violations. At the end of 2009, the DOJ and SEC combined were pursuing more than 120 FCPA investigations.

The penalties can sometimes be dramatic, such as the US\$1.6 billion in fines, penalties, and profit disgorgement that Siemens paid in 2008 for FCPA and bribery violations.

Federal officials are not only bringing cases for FCPA violations; they are also charging firms with lying to federal officials about compliance programs. For example, in early 2010 BAE Systems entered separate settlements with the DOJ and Britain’s Serious Fraud Office to settle long-standing investigations of improper payments. The criminal information filed in the American case claimed, in particular, that the company had made certain false and incomplete statements to the US government and failed to honor its undertakings to scrutinize payments to consultants, consistent with the FCPA. On 1 March 2010, a federal judge approved the settlement in which BAE pleaded guilty to conspiracy and false statements about its FCPA compliance plan. The company agreed to pay US\$400 million to the US and US\$47 million to British authorities.

More aggressive enforcements: As the example at the beginning of this article shows, law enforcement is not simply waiting for a whistleblower or competitor to inform on a company’s overseas activities. The DOJ is employing tactics usually reserved for drug or organized crime investigations. After this success, prosecutors and agents will likely maintain this proactive stance, and undercover operations, wiretaps, and other covert

law enforcement tools will be brought into more investigations.

Officials are also increasingly targeting individuals. The number of individuals prosecuted by DOJ under the FCPA has increased 700% from 2006. Acting Assistant Attorney General Matthew Friedrich has emphasized that “corporate executives who bribe foreign government officials in return for lucrative business deals can expect to face prosecution.”

Indeed, the list of executives going to prison after FCPA convictions is growing. Mark Mendelsohn, Deputy Chief of the DOJ’s Fraud Section noted in 2008 that the number of individuals prosecuted “has risen – and that’s... quite intentional on the part of the Department. It is our view that to have a credible deterrent effect, people have to go to jail... This is a federal crime. This is not fun and games.”

The damage to companies does not end with high fines and jailed executives. Shareholders have begun to bring civil actions against companies based upon FCPA violations. They alleged that poor oversight and lack of internal controls enabled a pervasive environment of misdeeds and corruption, resulting in enforcement actions and substantial government penalties that have severely damaged investors’ holdings.

Other countries are also stepping-up their enforcement. The United Kingdom recently passed its “Bribery Act” which is even broader in scope than the FCPA.

More self-disclosure: Law enforcement officials have stated that companies self-disclosing potential FCPA violations will be treated favorably when prosecution and fines are determined. While the US Sentencing Guidelines allow for mitigation of a sentence based upon a company’s self-disclosure, a firm cannot predict what benefit it will receive.

The goal is a deferred prosecution agreement with the DOJ. This allows a company to enact reforms in exchange for the case being dismissed after a period of time. There have been few

such agreements related to FCPA cases, but they do exist. In 2005, for example, Monsanto settled FCPA charges by agreeing to pay US\$1.5 million in criminal and civil fines and penalties and to be bound by a three-year deferred prosecution agreement.

Despite these uncertainties, companies are better off coming forward once a violation is discovered – usually through pre-merger or other due diligence efforts – rather than waiting for a federal grand jury subpoena. Since 2005, approximately 70% of FCPA cases initiated by the DOJ have been based on self-disclosure. The number of self-reported FCPA violations will rise as law enforcement continues its focus on the FCPA and as small and mid-sized companies begin to scrutinize their overseas work [see below].

Court-enforced monitor relationships may also increase. On 12 January 2010, the US Sentencing Commission voted to propose changes to the Sentencing Guidelines when probation is ordered. These include not only the retention of an independent corporate monitor to be paid for by the organization, but also unannounced examinations of

corporate books, and an amendment to the Guidelines' application notes – which can be relied upon by a court – to clarify the expectation that, in order to avoid any legal liability, high-level personnel must conform to any policy that is part of an effective compliance program. In short, the proposals indicate a renewed spotlight on corporate compliance arrangements and their ability to uncover violations.

More focus on small and mid-sized companies: As part of their increased FCPA-related efforts, the DOJ and SEC are expected to look more at small and mid-sized firms which do business overseas. The majority of such companies have a small established compliance program, or none at all, yet some may conduct billions of dollars in foreign transactions. Companies that are not household names have long believed that they were under law enforcement's radar. Smaller firms have also thought that the DOJ would not expend the resources to investigate their overseas sales. That comfortable illusion no longer exists. The companies involved in the January sting operation described above, for example, are not well known.

In another recent case, John W. Warwick and Charles Jumet pleaded guilty to conspiring to make corrupt payments to foreign government officials in order to secure business for Ports Engineering Consultants Corporation (PECC). The company, incorporated under Panamanian law, was affiliated with a U.S engineering firm. According to the indictment, PECC was created so that Warwick, Jumet, the firm itself, and others could corruptly obtain certain maritime contracts from the Panamanian government. Court documents claim that the defendants – participated in a conspiracy to pay money secretly to Panamanian government officials in return for a no-bid 20-year concession to maintain lighthouses and buoys along Panama's waterway.

What makes this prosecution interesting is the small amount of money involved. For six years, the conspirators made corrupt payments totaling approximately \$331,000 to the former administrator and deputy administrator of the Panama Maritime Authority and to a former high-ranking elected executive official of the Republic of Panama. That figure pales in comparison to other FCPA cases the DOJ has brought. It clearly demonstrates that the authorities are prepared to seek criminal indictments for individuals and companies that violate the FCPA, regardless of the size of the company or the suspected illegal payment.

American law enforcement officials have signaled to the world that they will aggressively combat FCPA violations. More investigations, indictments, and corporate executives being sent to prison are certain to follow. Companies that do not ensure compliance with the FCPA run a great risk to their organizations, as well as to their executives and directors.

It's not just the FCPA: New SEC enforcement activity

The SEC is getting more aggressive in investigating a range of frauds, not just FCPA violations. In October 2009, criminal and civil charges were brought against Raj Rajaratnam, founder of the multi-billion dollar hedge fund Galleon Group LLC, and several others, in what the prosecutor dubbed the "largest hedge-fund insider trading case ever charged criminally." This appears to be the first time that law enforcement officials used court-authorized wiretaps to gather evidence in an insider trading case.

In addition to a willingness to use wiretaps more broadly, the SEC has established specialized teams in addition to the new FCPA Unit, including: an Asset Management Unit, a Market Abuse Unit, A Structured New Products Unit, and a Municipal Securities and Public Pensions Unit. Moreover, the commission has announced that it will begin to use cooperation tools traditionally associated with criminal prosecutors, such as proffer agreements, cooperation agreements, deferred prosecution agreements, and non-prosecution agreements, to advance its investigations.

Meanwhile, the Treasury has proposed allowing the SEC to triple the financial incentive for whistleblowers to 30 percent of sanctions imposed. All of this portends more aggressive enforcement of a range of complex fraud cases.



Jeffrey Cramer is a Managing Director and head of Kroll's Chicago office. Since joining Kroll, he has worked with companies to draft their compliance plans and lead due diligence investigations into foreign intermediaries throughout the world. He was previously a prosecutor in New York and Chicago and has investigated several FCPA cases during his 13 years in law enforcement. Most recently he was a Senior Litigation Counsel for the Department of Justice in Chicago.

Fraud in bankruptcy in the USA



Jeffrey L. Baliban

Businesses are filing for bankruptcy at a record pace: in the United States corporate bankruptcies were up nearly 35 percent in 2009 after rising 30 percent the year before. More bankruptcies will likely lead to more instances of bankruptcy fraud.

Debtor fraud most often involves concealing or undervaluing assets. Insiders, with their detailed knowledge of the failing company's finances and their ability to manipulate records, are well-positioned to commit fraud. Assets, particularly non-operating ones – such as interests in non-debtor entities or real-estate – can simply go unreported or be grossly understated on asset schedules in the hope that creditors will not notice.

Indicators of potential asset concealment might be a large claim of “theft” just before the bankruptcy filing, or the inability to reconcile these listings with previous ones, for example on insurance policies. Also you need to look for failure to disclose prior bankruptcies, failure to file current tax returns, and incomplete or frequently changed responses to creditor questions.

Pre-petition asset transfers are frequently used to retain assets improperly. If such transfers take place typically two, and up to five, years prior to a bankruptcy filing, they can be deemed fraudulent and subject to recovery by the estate, even transfers that were made without conscious intent to do

wrong. Many transfers though are intended to defraud creditors. These might be made for non-commensurate consideration or be accompanied by agreements that the property will revert to the debtor after the bankruptcy closes. Investigators should look for pre-filing relationships with transferees, hidden or indirect debtor interests in such parties, and collusive involuntary bankruptcies.

More ambitious bankruptcy fraud can involve business transactions to loot stable companies. In bankruptcy “bleed-outs,” for example, a corporate raider might acquire a firm with easily transferrable assets, extract these assets, and then dump the near-worthless husk into bankruptcy for creditors to squabble over. Also, insiders at a struggling company can create a new business in the same industry and serving similar markets to which they can methodically transfer assets or “sell” them for a small percentage of their value. Such an entity might even be created post-bankruptcy to provide a vehicle to liquidate the debtor's assets. This kind of activity often involves complex transactions designed to confuse trustees and creditors.

Other common bankruptcy frauds involve transactions when business failure is inevitable. In a simple “bust-out” scheme, a fraudster obtains merchandise which it then resells – often for cash at below-market prices. Suppliers go unpaid and the business declares bankruptcy. A frequent

variation sees the business making some initial small transactions where suppliers are paid quickly. Convinced of the fraudster's good intentions, suppliers increase credit facilities and ship large quantities of merchandise, whereupon the fraud is perpetrated.

Sometimes failing companies try to entice investors with Ponzi, or pyramid, schemes. These involve obtaining investor contributions through the promise of above-market returns and then creating, through the allocation of new investor money to older investors, the false impression of the firm's ability to provide those returns successfully, which in turn serves to attract even more capital. Upon the scheme's eventual collapse, bankruptcy protection is sought.

In these difficult economic times, even those who have historically transacted business fairly and honestly might have incentives to resort to less-than-legitimate business methods. Awareness of the telltale signs of bankruptcy fraud can help creditors, investors, and business partners protect themselves from additional losses associated with the failure of a company.



Jeffrey Baliban is a Senior Vice President at NERA economic consulting. He is a CPA, Certified Fraud Examiner and has spent 27 years resolving complex commercial disputes and is an accredited business valuations analyst. Prior to joining NERA he spent time at KMPG and other CPA firms specializing in forensic accounting and economic damages analysis.



How to survive and thrive in corrupt markets

Andrés Otero

The United States government has made the fight against corruption a top priority in recent years by reviving and reinforcing the Foreign Corrupt Practices Act (FCPA). President Barack Obama, in a speech at the WTO negotiations in Doha in February 2010, pledged that the country would lead the way in this struggle and asked for the collaboration of all world leaders. The US administration recognizes that corruption undermines economic opportunity and sustainable development in emerging markets. While this thinking is not new, the US Government's current commitment to – and level of – enforcement is.

Despite all this many corporations doing business in emerging markets continue to turn a blind eye to behavior that might violate the FCPA, either because of business interests or simply to avoid opening a Pandora's box that could lead to business interruptions, sanctions, and legal action by the Department of Justice (DOJ). They rationalize this posture by invoking competitive pressures, cultural differences and norms in foreign markets, or convenient legal

opinions that absolve them of any blame for misbehavior.

Whether simply an excuse or not, it is true that corruption remains common in many countries, especially where the rule of law and democratic principles are not government priorities. This allows some companies to pretend that offering bribes and taking shortcuts is not cheating. Many of these businesses have taken advantage of corrupt regimes to generate substantial profits and to take market share from competitors unwilling to break the rules.

Now that the anti-corruption heat is on, the question for companies not wanting to break the law and become the subject of an FCPA investigation by the DOJ is: how do we conduct business and thrive in corrupt markets? It is not easy, but neither is it impossible.

During a recent Global Ethics Summit held in New York, Mark Mendelsohn, Deputy Chief of the DOJ's Fraud Section, noted that companies will have to respond in 2010 for corrupt practices from 2005 under the ethical and compliance standards expected to be set for 2015. As a result, companies

need to adopt new thinking about their operations in emerging markets.

The DOJ has made clear the importance of companies that are aware of corrupt practices in their own operations, voluntarily notifying the department before it finds out through a whistleblower, competitor, or disgruntled employee. Before a business proceeds with self-disclosure, however, it should conduct an internal investigation to understand the depth of the problems and any weaknesses in its compliance program. Otherwise, executives might inadvertently create a situation that could spiral out of control.

Most people are aware of the trouble Siemens faced in 2008, including the fine of over one and a half billion dollars the company had to pay because of FCPA violations, as well as other high-profile criminal prosecution pursued and sanctions imposed. Nobody, however, can predict the broader long-term effects of this case, such as the toll it might take on corporate reputation, what legal actions other countries might take, and how much business firms will lose because of past behavior. Despite these great uncertainties, Siemens was helped by its dealing with the problem, its willingness and capacity to

collaborate with the authorities, and its adequate management of different stakeholders with respect to the issue.

While no country or industry can be painted with one broad brush, investors, high-level executives and board members will benefit from identifying and understanding red flags related to their operations in markets where this problem is common. For example, if a company's sales are thriving and its return on investment is increasing, while competitors are leaving because the government is expropriating their assets, somebody should begin to ask questions.

Once the hard questions have been asked and blemishes detected, what comes next? Neither the DOJ sentencing guidelines nor the expected amendments to the OECD Anti-Bribery Convention provide a clear road map to avoid sanctions. However, they are a good starting point.

Some companies involved in recent FCPA sanctions had robust compliance programs in place before the corrupt practices were detected. Even so, those compliance programs were not enough to avoid the fines and the criminal prosecution of key executives imposed by the DOJ. To avoid a similar fate, some organizations now recommend conducting due diligence on every deal, transaction, or business opportunity in emerging markets. Corrupt practices, though, are often seamless and difficult to detect. And how much due diligence is enough? More experienced emerging market organizations recommend a risk-based approach. They believe that firms, before committing to intensive due diligence, should seek to understand better each market, its competitive landscape, and the culture in which they are doing business in order to identify the different areas and levels of risk.

The biggest challenge today is for those businesses that know they are operating in a high-risk environment. Should they do business in some of these markets? Should they leave the country and cede the market to their competitors? Should they continue to

conduct business as usual and hope that the DOJ is too busy to catch on to them? Or should they hold their ground and not surrender their corporate ethics to the corrupt practices that have dominated the market in the past? The answer seems obvious, but the consequences of that decision are not so simple.

Kroll can help companies make a decision about which approach is best for their particular situation. The reality is that in some industries, the best opportunities arise in some of the most complex markets and high-risk countries. Not being present in these countries is not an option for many multinational companies. As a result, many companies want to know where to begin to understand the risks they face. The country Corruption Perception Index produced by Transparency International is a good point of reference. Other publications, such as the World Bank's Doing Business Report, which also ranks countries based on corruption standards and red tape, may help companies understand the environment in which they are doing business. It is also important for a company's ethics and compliance function to understand the reality of doing business in emerging markets. It is vital to travel to these regions in order to understand the culture and how an industry does business in that market.

Once a company understands its operations abroad, it will be in a better position to deal with bribery and corruption issues. Companies will have a better understanding of what is really happening and can give an informed report to the authorities where necessary. It will also help companies develop a more realistic compliance program more suited to the realities on the ground, and the time spent in these countries may assist compliance executives in making allies in the business instead of enemies. Most important, such in-depth knowledge is necessary for an organization to comply with new regulations and to protect its brand name and reputation, while being able

to conduct business in many of these complex and hostile markets.

Corporations face many difficult questions when doing business in China, Brazil, Russia, Venezuela, or other emerging markets. Should the company report any bribes it may have paid in the past? What if the company is still paying bribes or has been taking part in other irregular activities? What if it is aware that other competitors are engaged in corrupt activity? What if its suppliers or third-party agents are paying the bribes? If there has been questionable behavior, the company's top executives and board members must decide what course of action to take.

The question has become more straightforward and practical: Bribery is bribery, wherever you are. Judges in developed countries are not on an ethical crusade to judge and stymie the practices – and success – of rising economies. However, combating bribery and other forms of corruption has become the top priority for the DOJ in its attempt to change the corporate culture in the United States. More importantly, the DOJ is expanding its capability to pursue companies that exploit corrupt foreign officials no matter where they are located. One DOJ representative recently explained that the department will try to seek jurisdiction and prosecute any company accused of corruption with any sort of link to the United States.

A company's best option is to come clean before someone reveals its secrets, know in detail what the company reveals, work with local teams to ensure that this behavior does not continue to take place in the organization, deal with the consequences, and move forward – seizing new opportunities to thrive in corrupt markets.



Andrés Otero is a Managing Director in the business intelligence and investigations division and head of the Miami office also responsible for the Caribbean, Colombia and Argentina. Previously he ran the office in Bogotá, Colombia and is an expert in a variety of investigative and intelligence services, including fraud and corruption control, money laundering investigations, government relationships, conflict resolution, and other related matters.

The ASEAN-China Free Trade Agreement: An IP protection challenge for everyone

Nicholas Blank

In January 2010 the ASEAN-China Free Trade Agreement (FTA) came into effect. It eliminates barriers to investment and tariffs on 90 percent of products between China and the six ASEAN countries – Brunei, Indonesia, Malaysia, the Philippines, Singapore and Thailand. Although the negotiations took years, one key area which the agreement still overlooks is the protection of intellectual property (IP).

Over the last 15 to 20 years, some Chinese companies have become national brand champions and others have acquired well-known foreign brands. In footwear, for example, aggressively marketed Chinese sports brands, such as Anta or Li Ning, will likely grow in popularity in many ASEAN countries. Now, because of the FTA, China's share of the Indonesian footwear market is expected to increase to 60 percent, eliminating forty-thousand Indonesian jobs. An Indonesian sneaker factory might well consider making fakes of Chinese brands as part of its survival strategy. Thus, for the first time, China may wish to enforce IP rights beyond its borders, joining the United States in putting pressure on ASEAN governments in this area – a seismic shift which might lead to better IP enforcement in Asia, including in China itself.

Western companies might find themselves reliant on such increased protection because the FTA will also add to their difficulties in Asia. With the agreement covering some 9000 duty free products, a Chinese manufacturer who has previously

violated a Western company's IP while making goods for the domestic market might well now be able to sell these products across all ASEAN markets, where there is little chance of any IP enforcement. This is no longer simply a question of pirated DVDs from China smuggled into Thailand and sold in Bangkok: such commerce might involve sophisticated products and materials being manufactured in Shenzhen and transported through efficient logistics routes to Vietnam.

Indeed, counterfeiters have already proven themselves capable of utilizing far more complex supply chains. Kroll was recently called in by a company which had realized that bad copies of its medical devices were being sold in the United States. If not stopped, this IP theft might have led to patient deaths and a serious blow to the company's reputation. Kroll traced the counterfeits back to a Chinese manufacturer and found that the products went via Dubai and Latin America before reaching the United States. In order to stop the counterfeiters at both ends of the supply chain, Kroll, through its relationships with enforcement authorities in America and China, successfully coordinated simultaneous raids in multiple jurisdictions.

In many ways, the future of the FTA remains uncertain. The deal may still provoke a public backlash in less competitive ASEAN member countries.

It is critical, however, that companies act to protect their IP now rather than wait for the possibly devastating financial and reputational impact of its theft. Useful steps include:

- Develop a relationship with local enforcement agencies in the jurisdiction of your factory or OEM supplier.
- Carry out background checks on your employees and vendors. If your firm is heavily involved in research and development, find out if any staff members have partners or close contacts who would benefit from receiving your technology.
- Carry out an IP audit of your facility. Review your information technology, human resources, and fraud prevention procedures and protocols to determine if they are still effective and up-to-date. Conduct a physical security assessment to ensure that employees are prohibited from simply walking out of the factory with a laptop storing trade secrets.
- Ensure that the local in-house legal and compliance team has a direct reporting line to the CEO in the head office. This will allow immediate action in a time of crisis without layers of bureaucracy slowing things down.



Nicholas Blank is an Associate Managing Director in Kroll's Hong Kong office. He has worked in a number of capacities at Kroll and is well-known for his work in the IP field, having been a guest speaker on IP issues for the United States Patent and Trademark Office.



FRAUD NEWS

BAE pays nearly \$450 million to settle corruption investigation

The United States Department of Justice (DOJ) and Britain's Serious Fraud Office (SFO) and have simultaneously announced global settlements with BAE Systems. In return for paying £30 million (US\$47 million) and pleading guilty to accounting failures in an arms deal with the government of Tanzania, the SFO is winding up corruption investigations relating to a series of arms sales dating back 10 years with Tanzania and several other African and European states. BAE has also agreed to pay the American authorities US\$400 million and admitted to making false, inaccurate, or misleading statements with regard to its anti-corruption compliance standards, in return for the DOJ concluding an even broader investigation. The company has not admitted to corruption and, since 2008, has been implementing a thorough overhaul of its anti-corruption arrangements.

Fraud embarrassments for the Indian military

Lieutenant General Avadesh Prakash, one of India's eight top military officials, is facing a court martial over alleged involvement in illegal land dealing. AFP reports that, although the General is the highest ranking Indian officer ever to face court martial, this is just the latest in a series of embarrassing fraud cases for the military. These include the sale by officers of weapons on the black market, and an officer in search of promotion whose efforts to fake a gun battle with militants included sprinkling ketchup on civilians.

Brazil: New proposed legislation, new arrest

President Luiz Inacio Lula da Silva has sent a bill to the Brazilian Congress that would toughen the country's anti-corruption measures. Under the proposal, companies convicted of bribing domestic or foreign public officials would be liable to fines of up to 30% of gross income and possible closure. The bill comes against a backdrop of allegations: several key presidential advisers have resigned amid claims of corruption. Meanwhile, in a separate scandal, the governor of Brasilia – an opposition politician – was arrested in February for alleged corruption. The latter explained a video in which he apparently accepts a bribe by saying he was taking the money to buy panettone for the city's poor.

Haitian earthquake brings out fraudsters

On 13 January, the day after the earthquake in Haiti, the FBI warned that the event was likely to bring out fraudulent appeals for funds, especially over the Internet. The concern has quickly proved justified. According to Symantec's February 2010 *State of Spam and Phishing Report*, in January emails seeking to perpetrate frauds and scams accounted for 21% of global spam, up from 11% the month before. Meanwhile, a BBC investigation easily uncovered two criminal gangs in London using the earthquake to make false donation appeals to defraud people.



Bank of America settles one Merrill Lynch suit, ex-directors face another

The Bank of America has agreed to pay the Security and Exchange Commission (SEC) US\$150 million and to improve its governance practices in settlement of two lawsuits alleging poor disclosure of the losses Merrill Lynch faced, and bonuses it had paid to employees, before Bank of America's takeover. In the meantime, New York's Attorney-General has filed a civil fraud lawsuit against former CEO Kenneth Lewis and former CFO Joe Price for allegedly misleading shareholders about the acquisition.

Phishers net carbon credits

A phishing attack hit the European Emission Trading Scheme in early February, forcing the temporary suspension or closure of emission permit registries in 12 countries. German authorities reported that 6 companies from that country had a total of 250,000 carbon permits – worth about US\$4 million – stolen.

More Madoff aftermath

The Wall Street Journal reports that Mark and Andrew Madoff, Bernie Madoff's two sons, as well as Peter Madoff, his brother and a former compliance officer at his firm, are being investigated for criminal tax fraud by Manhattan federal prosecutors. Meanwhile, Britain's Serious Fraud Office announced that it would not be taking action against Madoff Securities UK. After a year's search, it had not found enough evidence to provide "a realistic prospect of conviction."

Disclaimer The information contained herein is based on sources and analysis we believe reliable and should be understood to be general management information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. This document is owned by Kroll and its contents, or any portion thereof, may not be copied or reproduced in any form without the permission of Kroll. Clients may distribute for their own internal purposes only. Statements concerning financial, regulatory or legal matters should be understood to be general observations based solely on our experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which we are not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas. Kroll is a subsidiary of Marsh & McLennan Companies, Inc (NYSE:MMC), the global professional services firm.



Kroll contacts

North America

Consulting Services

Robert Brenner
New York
1 212 593 1000
rbrenner@kroll.com

David Holley
Boston
1 617 350 7878
Dholley@kroll.com

Jeff Cramer
Chicago
1 312 345 2750
jcramer@kroll.com

Ken Mate
Los Angeles
1 213 443 6090
kmate@kroll.com

Bill Nugent
Philadelphia
1 215 568 2440
bnugent@kroll.com

Betsy Blumenthal
San Francisco
1 415 743 4800
bblument@kroll.com

David Hess
Reston, VA
1 703 796 2880
dhess@kroll.com

Kroll Ontrack

Jason Straight
New York
1 212 833 3208
jstraight@krollontrack.com

Identity Theft

Brian Lapidus
Nashville
1 615 320 9800
blapidus@kroll.com

Background Screening

Phil McVey
Nashville
1 615 320 9800
phil.mcvvey@kroll.com

Latin America

Consulting Services

Andres Otero
Miami
1 305 789 7100
aotero@kroll.com

Vander Giordano
São Paulo
55 11 3897 0900
vgiordano@kroll.com

Matias Nahon
Buenos Aires
54 11 4706 6000
mnahon@kroll.com

Glen Harloff
Grenada
473 439 7999
gharloff@kroll.com

Sergio Diaz
Mexico City
52 55 5279 7250
sdiaz@kroll.com

Ernesto Carrasco
Colombia
571 317 5737
ecarrasco@kroll.com

Asia

Consulting Services

Chris Leahy
Singapore &
South East Asia
852 2884 7728
cleahy@kroll.com

Richard Dailly
India & South Asia
91 22 4244 0501
rdailly@kroll.com

Tadashi Kageyama
Greater China
852 2884 7725
tkageyama@kroll.com

Tsuyoki Sato
Japan & Korea
81 3 3218 4875
tsato@kroll.com

Background Screening

David Liu
Hong Kong
852 2884 7716
dliu@kroll.com

Kroll Ontrack

Legal Technology
Scott Warren
Tokyo
81 3 3218 4594
swarren@krollontrack.com

Europe, Middle East & Africa (EMEA)

Consulting Services

Richard Abbey
London
44 207 029 5000
rabbey@kroll.com

Brendan Hawthorne
London
44 207 029 5482
bhawthorne@kroll.com

Bechir Mana
Paris
33 1 42 67 81 46
bmana@kroll.com

Tom Everett-Heath
Dubai
971 4 4496700
teverettheath@kroll.com

Marianna Vintiadis
Italy
39 02 8699 8088
mvintiadis@kroll.com

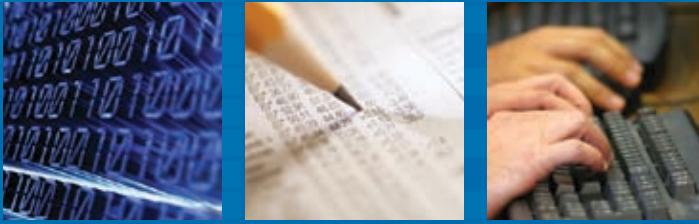
Alfonso Barandiarán
Madrid
34 91 310 67 20
abarandiaran@kroll.com

Background Screening
Tony Shepherd
London
44 7917 857913
tshepherd@kroll.com

Kroll Ontrack

Tim Phillips
London
44 207 549 9600
tphillips@krollontrack.co.uk





Experts in fraud intelligence and investigations

For over 35 years, we've helped our clients to prevent, investigate and recover from fraud. We specialize in investigation, forensic accounting and computer forensics.

We design solutions to your problem, whether global, local or cross-border.

Our services include:

- Corporate Internal Investigations
- FCPA, Regulatory & Corporate Governance Investigations
- Forensic Accounting
- Compliance Monitoring
- Asset Tracing & Recovery
- Intellectual Property Protection
- Litigation Support
- Fraud Prevention Training
- Computer Forensics
- Process & Internal Controls Assessment
- Expert Testimony
- Investigative Due Diligence
- Electronic Discovery
- Government Contractor Advisory Services
- Identity Theft Restoration
- Real Estate Integrity Services
- Anti-Money Laundering Programs
- Loss Prevention

Kroll also provides services in

- Security Consulting
- Background Screening
- Data Recovery & Legal Technologies
- Business Intelligence
- Hostile Takeover, M&A and Hedge Fund Intelligence
- Employee & Vendor Screening