



COMMERCIAL CRIME

International

April 2010

Be wary of 'jack of all trades' online commodity traders says FIB

ICC Commercial Crime Services has issued many warnings about the dangers of sourcing commodities from unknown parties off the Internet. A recent case seen by the agency's Financial Investigation Bureau (FIB) underlines these dangers and serves to prove the maxim 'buyer beware'.

A South African buyer in Durban advertised for washing powder on alibaba.com. He was contacted by a trader in Cape Town who said he could provide the quantities required – 20MT per month for 12 months: 240MT in total. Prices were provided, the imported powder being considerably cheaper than that domestically produced, despite the cost of transport from an unnamed manufacturer in Asia or Europe. Top quality washing powder was promised.

In a flurry of email exchanges, the buyer asked for the price to be reduced. It was. He asked again and after "checking with guys in the UK" was virtually asked what he wanted to pay. This was agreed. Then he asked if it could be bagged in 1kg bags. No problem; included in the cost. Could he have his own branded bags? Yes; no extra charge. Could the manufacturer include the buyer's own perfume choice? Once again, no problem. All this for just 20 MT per month delivered from abroad to the buyer's warehouse from a never named manufacturer who just happened to produce for existing SA brands. Add in SGS reports on every shipment and that's a great deal.

It's all the more remarkable when you consider the trader only registered his company in 2007 with the South African companies and intellectual property office, albeit at a different address to the one he is using now. He's also apparently been very successful in the intervening period. His logo claims business interests in South Africa, UK, Iraq, Dubai, USA, Switzerland, Korea, Sierra Leone, Mali and Ghana. Quite an eclectic mix, as is his claim to supply crude oil, diesel, petrol, coal and cement.

Interestingly, the trader has the same name as someone associated with another company called the King of Bling in Cape Town. On that company's site he boasts a degree in drama, acting and scriptwriting from Stellenbosch University. If it's the same person, he's certainly put on a class act. But he was undone by his lack of attention to detail and obvious lack of knowledge about international trading.

As soon as the documents arrived for signing, the buyer became suspicious. They included an ICC NCND & Working Agreement document. There are numerous examples of these documents on the Internet, but such documents do not exist. The buyer went online and found the warning about them on the ICC website disclaimers page. Then he contacted CCS, who confirmed his suspicions.

He went back to the trader to ask about the NCND document. The trader claimed he had provided it

to offer extra security to the deal and as a means of ensuring both buyer and seller perform successfully. When challenged, he accepted that he was at fault for not ascertaining the document's correctness. He welcomed it being reported to the ICC, adding that he had got it in a previous sugar trade that had come from a good seller. But he hasn't been in contact with the buyer since that email.

A second document sent for signing was a warning letter on new measures in respect of buyers and sellers conducting oil and commodities transactions, supposedly giving buyers the option to contact the FBI, ICC and Interpol if a 'not real' ICPO, LOI, RWA or BCL is issued. The purpose of the letter is allegedly to protect the commodities industry, but it is a complete fake and only used to add credibility to the deal.

continued on page 2/

In This Issue of CCI

FRAUD

- Loan fraud firm exposed 2
- Fraudster explains why and how 4

COMMERCIAL CRIME

- Sri Lanka a potential crime hotspot 6

CORRUPTION

- Fighting Bribery: new UK legislation explained 8

CYBERCRIME

- Website targets Madoff losers 9
- Legal consequences of data loss 10
- New online fraud reporting system 11
- \$25m ticket cyberscam 11
- Threats from hacking automation 12

Fraud

Time to name and shame loan fraud firm

TOUGH economic times are forcing companies down unknown routes in a bid to get the necessary funding to complete their various projects. The banks won't lend, but plenty of fraudsters will. The reality is that these loans don't exist; they are just a cynical attempt to generate an advance fee. As soon as this has been paid all manner of obstacles to completing the loan emerge.

A California-based company recently reported its experience of one of these loan companies to ICC FraudNet. The ICC Financial Investigation Bureau (FIB) has been examining the case, which involves a firm called the London Securities Company. This outfit is well known to FIB, having first been reported to the agency by one of its members in 2006, and several times since. It's time the dangers of dealing with this company were made known to a wider audience.

As with most loan frauds, London Securities Company has an impressive website (www.londonsecurities.org.uk) to pull people in. The website says proudly that the company is located in the financial capital of Europe and is thus well positioned to take advantage of this unique and exciting business environment. It claims to work

through an established network of business associates that can meet the needs of its worldwide clients. It boasts of providing assistance to get projects fully funded by leasing yearly renewable bank instruments. The named contact is Mr John Hainsworth.

There is plenty to attract the desperate. "Credit enhancements can be obtained at minimal expense to the borrower compared to other banking options. Our credit enhancements, corporate and debt instruments include Bank Guarantees, Insurance Guarantees, Medium Term Notes, Standby Letters of Credit and Third Party Guarantees such as a standby forward commitment to purchase or a standby loan." True to its word, London Securities explains the simple process to get this done. It works like clockwork until the deposit is paid. But then the complications set in.

Warning signs

Before discussing the particular case under review, it is worth mentioning a few things about London Securities that any applicant should pick up in basic due diligence, or get an independent agency to check.

1. No company with this name

has ever been registered with UK Companies House.

2. Its address in St John Street, London, is an accommodation address that had been linked to and allegedly used in numerous other financial frauds. A quick Google search reveals this.

3. The 870 phone number listed for London Securities is one that automatically redirects callers to another phone.

4. The company claims to be owned by a UK bank, but has never been registered with the UK Financial Services Authority, which it would be required to do.

5. Just typing into Google the words 'London Securities' brings up numerous warnings about the scam from previous victims.

6. The website warnings allege the people behind London Securities are in fact based in Canada.

7. A "Who is" domain name search (remember [.org.uk](http://www.org.uk)) indicates the website is registered in Virginia, USA. Moreover, it was registered by a Mr Eli Phipps. The documents examined by FIB show a Mr Elijah Phipps as the Public Trustee at PCL Financial Trust, supposedly the independent escrow agent used by London Securities to whom applicants send their deposits. Moreover, the letterheads and letter styles of correspondence from London Securities and PCL are identical, right down to the spurious 'Corporate Seal' used in both.

8. The London Securities contact John Hainsworth had his FSA registration as a financial advisor revoked several years ago in connection with a firm in Gloucester, England, that went into liquidation.

Application flaws

With evidence like this, a prudent person would be forgiven for walking away. For those that continue, the problems are just starting. The California applicant clearly saw none of this coming, even though claiming to have previous banking experience and to have previously

Washing powder fraud - from page 1

The supplied contract, meanwhile, was a complete work of fiction, which looks as if it were cobbled together by a dyslexic 10 year-old. The figures are confused and in cases wrong. Buyer/seller responsibilities are mixed up. No product origin is named, yet a price of \$1.2/kg is quoted CIF for a 20Mt load. Finally, there is the classic fraudster's reference to a Letter of Credit that is 'Irrevocable, Transferable, Devisable' (misspelt). On top of all this, the buyer has since discovered that the bank account nominated for payment is a Bank of South Africa savings account that has not been used in over a year. Very professional!

The FIB suspects this trader is more amateur chancer than seasoned commodities fraudster, but there are plenty of others out there better prepared. The buyer in this case withdrew before paying any money. He now says he has negotiated a new deal with a Chinese company that he is sure is legitimate. Based on its past dealings with online commodities traders, the FIB remains to be convinced.

negotiated Bank Guarantees for clients. They were apparently introduced to London Securities by someone known and trusted called Eli Liebowitz, who convinced them the firm had the background and experience in these matters they needed. He, in turn, introduced them to Gene Mercier, with whom the transaction was conducted.

A Leon Siltzer also features in some of the correspondence.

The applicant agreed to the terms of London Securities' 'Memorandum of Understanding – Lease Program' and signed the document. They should have taken some time to understand what they were agreeing to. An independent bank document expert points out the following:

1. The Lease Program Memorandum of Understanding almost immediately refers to a Credit Enhancement Program (line 2). Leasing money in this way does not exist in the real world. Transactions of this nature historically turn out to be frauds.
2. It also refers to the granting of a US Treasury (Note) using standard updated ICC formats, but ICC formats have no connection to US Treasury Notes.
3. The applicant agrees to wire transfer the required security deposit to a designated independent escrow agent (PCL Financial Trust) in order to activate the transaction, which will hold them in accordance with the terms and conditions of the agreement. Importantly, the amount remitted will only be returned to the applicant if all parties meet their contractual obligations. In reality, this never happens. Importantly, any request to wire a fee to an escrow account is suspicious.
4. The security deposit required is Euro XXX Dollars. There is no such thing. The applicant in this case wired \$50,100 to PCL, which is allegedly located in Nevis.
5. The applicant agrees that if a pre-advise SWIFT message is required,

it will cost extra. Moreover, the deposit for the pre-advise is fixed and not refundable. The mention of SWIFT and the code line numbers MT760 should be a concern. Such phraseology is not used in genuine transactions and provides no additional value. Also, MT760 a legitimate code usually used to hold/block funds, not transfer them.

6. The agreement says the total cost of the Asset Lease service is 10% plus 2% commission, to be paid no later than 10 banking days after delivery. The applicant agrees an irrevocable undertaking to return the instrument to the providers designated bank, 'free clear and unencumbered' 15 days prior to the agreed maturity. This phrase has only ever been seen in suspect documents.
7. The applicant's agreement that the provider can contact his bank to conduct due diligence and pre-qualify the applicant for the delivery of the instrument provides an open opportunity to find fault with the application after the deposit is paid.

Wearing down the victim

Once the agreement is signed, the rest of the fraud is able to play out. In this case the issue turned out to be the applicant's proposed use of a private equity investment group to fund the \$12m fees due on the requested \$100m loan. London Securities insisted this firm did not have the financial support required to support a \$100m loan transaction. The applicant is adamant they made clear their intention to use a private lender from the outset, and was assured that the term 'Bank' in the agreement was generic. But once the deposit was paid this lender in the British Virgin Islands was deemed unsuitable, and the applicant was told the lender must get its bank in Hong Kong to guarantee to pay the fee and to return the bank instrument within the time period specified in the agreement. This was despite London Securities assuring the applicant they had worked successfully with private

lenders in the past to secure loans under the scheme.

To encourage this to happen, London Securities sent notice that the US Treasury Note was ready and waiting to be dispatched as soon as the applicant's (lenders bank) made the required undertakings, which it refused to do. Claim and counterclaim followed. London Securities admitted they did not own the loan instrument, but wouldn't say who did. They refused to supply information about the company to the lender's bank. A second private lender was put forward to London Securities, and once again their bank would not guarantee to pay the fee or return the instrument. There is no reason why they would.

Going round in circles and getting nowhere, the applicant finally asked for the deposit back. That was never going to happen. London Securities maintained PCL was independent and that they never touched the money. That is clearly not true. PCL maintained the deposit was non-refundable, which of course was always going to be the outcome.

The upshot is that the California company now reluctantly accepts they are unlikely to get their money back. But they have engaged a lawyer to keep trying. The victim hopes that by telling their story, others will come forward and that they can get together to tackle London Securities and its principles.

They may have one more reason to do so. The victim mentioned in correspondence another company said to be based in Lausanne, Switzerland, that a client had paid a \$150,000 deposit to and who, six months later, has still not received the promised bank loan instrument. That company's website, inactive since last year, has a domain registered in Gloucester, England. Is it just coincidence that John Hainsworth, the main contact for London Securities, used to run a financial services business in the same county?

Fraud

Committing financial fraud: accident or design

An article in last October's CCI told the story of how Stephen Greenspan became one of Madoff's victims. This month it's the turn of a fraudster to explain why and how. You will be able to hear more about fraudsters and why they commit their crimes at the 10th CCS Annual Lecture, entitled "Learning from Fraudsters", which will be presented by leading criminologist Professor Martin Gill in London on the 17th June.



Jamie P Lake (pictured above), who operated an investment service in America, is off to prison for 45 months after his recent conviction for mail fraud. In just over two years he stole more than \$600,000 from 33 people using a computer, a little knowledge of the financial markets and a lot of trust. Before he went, he said in interview he was surprised by how easy it was to commit the crime.

Lake, 37, a registered securities broker-dealer, was the owner of JPL Financial Services, a successful business that at one time had more than 100 clients. But he was spending more than he earned so, in December 2006, he devised a scheme to pilfer money from his clients. The fraud lasted until March last year, when, aware questions were being asked by one of his customers, he reported his wrongdoing to the company for which he worked. The company, Questar Capital Corporation, has since repaid all Lake's victims.

Expressing remorse for his actions, and vowing to repay the money and to take whatever action he can to make amends, Lake has spoken about his thefts in the hope that he can help other investors avoid the pitfalls that ensnared his victims.

Apparently, it started out as basic greed, with Lake firmly believing he could make the money back and that nobody would ever know. But it became too easy to do, because his clients put too much trust in him and did too little independent research. He said that among their key mistakes they wrote cheques

directly to him, rather than the company from which the financial instrument was purchased, and they failed to independently verify the accuracy of the account information he provided to them. They didn't question because they had confidence in him. In addition, he was likable, a smooth operator and a fast talker; the typical characteristics of a financial fraudster.

An early victim gave Lake \$10,000 to help him expand JPL Financial and was promised a good rate of return on his money. Other customers came via weekly radio spots on two local stations, and periodic appearances on a local TV station where Lake discussed general topics, such as the benefits of investing in an Individual Retirement Account. As a direct result of this, one victim gave him \$70,000 to invest in an annuity.

Speaking about that, the woman said she and her husband had several other, legitimate investments with Lake that were not part of the scam. Importantly, those were making money, so when he approached them about buying the annuity, they had no qualms and she wrote the cheque out to JPL Financial.

Exploiting an opportunity

Lake's crimes have been described as relatively unsophisticated compared to most other scams involving securities brokers. The majority of his victims purchased fixed rate annuities – a financial instrument sold by insurance companies that typically pays the owner a set sum of money each month after a specified time period elapses.

But Lake never purchased the annuities. Instead, he created documents on his computer that looked like annuity contracts, and then delivered them to the clients. He was adept at making the documents appear authentic because he had access to the letterhead of the brokerage companies for which he worked. It was simply a matter of cutting and pasting within a common computer program.

Lake said he didn't worry his clients might catch on because in most cases they didn't read the contract in its entirety, if at all.

"People break one golden rule: They don't check their facts and they don't look at the paperwork they're given," he said. "The policy is so many pages; they look at the first or second page, then shut it up and say OK."

Once the policy was issued, Lake then sent periodic statements – again fictitious documents he created on his computer – to show the client how their "investment" was performing. Most apparently took these on trust because they trusted him, and didn't stop to consider whether they were getting the proper information.

Lake's case differed from the typical

Fraud

securities fraud scam – some form of Ponzi scheme - because he didn't have to worry about paying out dividends since the financial instruments he sold had not yet matured. That also helped him avoid detection.

But there are things the investors could have done to protect themselves, he said. For instance, his clients would have known he had not purchased their annuity if they had called the insurance company that issued it to verify the purchase, rather than relying on the documents he provided them. Most companies also offer online access to the accounts that allow customers to verify information.

Suspicious

The beginning of the end for Lake's scheme came when one of his clients became suspicious that she had not received a tax document regarding her investment. The woman called Lake seeking the information. When he did not respond, she phoned the insurance company to obtain the document and was told the annuity did not exist.

At his trial, prosecutors contended that Lake only volunteered information about his scam because he feared the woman who sought the tax document was about to go to authorities. But Lake says she had no impact on his decision. If he wanted to, Lake said, he could easily have fooled her by providing a fake tax statement, which would have allowed him to avoid detection and continue the scam.

Instead, he claims he went to the authorities when he realised just how much he had stolen and that he had no chance of making it back.

As well as going to prison, Lake must now pay the money he stole back to Questar. He says he will do this by driving a tractor-trailer when he is released! And the SEC has permanently barred him from selling securities.

Date for the Diary

10th Annual CCS Economic Crime Lecture

Learning from Fraudsters: key risk indicators, lessons and solutions by Professor Martin Gill

Thursday 17th June 2010
Dickens Inn Conference Room,
St Katharine's Dock, London EC1.

Sponsored by



Getting inside the mind of a financial fraudster is both intriguing and exciting. Why do they do it? How do they do it? This year's lecture aims to answer these and many other questions about how fraudsters work, what they think, and how they respond when the game is up. Lecturer, Professor Martin Gill, is a leading criminologist who has studied fraudsters for many years, and has sought to understand how they operate. He will be accompanied by a convicted fraudster who will give insights into how and why he got into fraud, the impact of prison etc, and delegates will have an opportunity to ask questions. The Lecture should be both fascinating and illuminating, and potentially one of the most interesting CCS has ever staged.

There's a new venue and new sponsors this year too. The conference room at the Dickens Inn looks out over the picturesque St Katharine's Dock in the heart of the city and will be the ideal location to spend a few hours on a pleasant summer's evening.

Co-sponsor QEB Hollis Whiteman, is widely recognised as one of the leading sets of barristers' chambers in the country, specialising in crime, fraud and regulatory law.

Co-sponsor PCB Litigation is a firm of internationally renowned lawyers that specialise in fraud and international commerce litigation, and corporate fraud risk management. The firm is one of the founding members of ICC FraudNet.

Now widely regarded as a must attend event, this year's CCS Annual Lecture gets underway at 4.00pm with the main presentation at 6.00pm. There's a wine reception afterwards to discuss its content and ample opportunity for networking or simply enjoying the ambiance of St Katharine's and the buzz of the Dickens Inn.

As usual, attendance is by invitation only and there is no charge for attending. CCS members should receive their invitation in the coming weeks, which will include details on how to register.

Sri Lanka: a commercial crime hotspot in the making

*Sri Lanka is hoping to capitalise on its natural beauty to become a tourist hotspot, given that its three-decade long bloody civil war is now over. But **Munza Mushtaq** reports from Colombo that because of ignorance on the part of local authorities, the country could become a hotspot for something far less welcome - commercial crime.*

With peace in place after the Tamil Tigers were destroyed as a fighting force last May by the Sri Lankan army, this island nation has just begun to recover from civil war and work towards economic stability.

Colombo is already the country's commercial as well as political capital and is aspiring to be an Asian commercial hub for some of the world's leading multinationals, as well as local conglomerates. Yet back-to-back large-scale financial frauds running into billions of dollars have rocked the country over the past few years, and with the chief culprits yet to be apprehended risk analysts warn Sri Lanka is becoming increasingly vulnerable to large-scale scams, corruption and embezzlement. Despite this growing menace, many Sri Lankans including the recently re-elected President Mahinda Rajapaksa and his government appear complacent about the risks posed by commercial crime.

Financial scams

As the war started its violent end game, 2008 was a bad year for Sri Lanka regarding business crime – it was rocked by two back-to-back financial scams, which made headlines even abroad. In September 2008, thousands of unsuspecting depositors fell prey to a Ponzi-scam fraudster who fled abroad after duping thousands of people into depositing money with his firm by promising high returns.

The fraudster, Sakvithi Ranasinghe, currently on Interpol's wanted list, had offered returns as high as 30% on his investments, in contrast to the general 18% and lower offered by recognised banks and financial institutions. He defrauded around 5,000 unsuspecting depositors of more than Sri Lanka Rupees 1.5 billion (US\$13 million), police estimate.

Just two months later, in December 2008, a similarly shocking fraud of larger proportions unfolded, this time involving the Golden Key Credit Card Company, a well recognised and highly respected company on the island.

This fraud has been highlighted as the biggest white collar scam in the history of Sri Lanka, where thousands of depositors were allegedly defrauded of approximately 20 billion Sri Lankan rupees (US\$175 million) in another Ponzi-style scheme that was uncovered as the global financial crisis struck hard. Several officials of the company, including the chairman of the group Lalith Kotelawala, have been remanded in custody

facing fraud charges. Kotelawala is now out on bail but his wife, who also functioned as the deputy chairman of the group, fled the country and is still in hiding. To date, none of the depositors from both cases have been refunded.

Absconding abroad is an effective tactic by Sri Lankan commercial crime suspects, beyond the reach of the national police's Criminal Investigations Department (CID) and Fraud Bureau. A senior police officer, who spoke on the condition of anonymity, stressed that while action could be taken if fraudsters were in the country, it was "impossible" to go after them outside the island. "Even though we seek the assistance of Interpol, in comparison to more 'important issues' such as terrorism, focus on apprehending such fraudsters is still at minimalist levels," he noted.

Political influence

Political interference can also undermine the independence of police investigations into commercial crime. According to the officer, often, when a person is taken into custody or an investigation is launched into a 'close associate' of a high level politician (maybe from the ruling party), the police come under immense pressure to sweep the case under the carpet.

The law enforcement officer's concerns were echoed by a leading Sri Lankan lawyer and anti-corruption activist Nihal Sri Ameresekere, who is a member of the International Association of Anti-Corruption Authorities.

"The police are often not allowed to take action against the offenders simply because they belong to an influential group," Ameresekere pointed out. He added that even though Sri Lanka had laws against commercial crime, the failure by the authorities to implement these laws to the book have led to a situation where fraud, corruption and scams are rampant.

"We have laws but there is no proper law enforcement in the country. Only if it is politically motivated and pushed will there be an investigation and even prosecution, not otherwise. If the politicians don't want a certain individual prosecuted, there are times that the investigation is scuttled clandestinely," Ameresekere claimed.

He also insisted that neither of Sri Lanka's main two political parties are serious about fighting corruption or commercial crime; simply because they are funded and financed by the commercial world.

Commercial Crime

“There are people above the law, and the law will not touch those people, no matter what fraud they commit,” the anti-corruption activist declared.

And this is a problem: “Failure by the authorities to take stringent measures to address this growing problem will lead to a general setback in business confidence the world over. Serious foreign investors will rethink before coming and investing in Sri Lanka if they think the rule of law does not apply to all in a fair manner,” he said.

Despite his misgivings over policing, Ameresekere argued that it was still worth Sri Lanka upgrading and modernising certain existing laws. He said the country followed some criminal laws passed in the 1950s.

The lack of a multi-faceted sophisticated investigations unit to fight and combat commercial crime may also prove to be detrimental to the country, as neither the general police nor the CID generally undergo specialised training to investigate issues related to commercial crime, he said.

Rampant counterfeiting

Meanwhile, the Chief Executive Officer of the International Chamber of Commerce (ICC) Sri Lanka, Gamini Peiris disclosed that, the island nation was not far behind China and Russia in the counterfeit business. “We are now a transit point for counterfeit goods, but if the customs are educated and vigilant, then we can stop this from becoming a larger problem,” he noted.

Due to the excessive fake product circulation in the market, Sri Lanka also risks losing foreign exchange owing to branded companies not wanting to invest in the island due to the excessive circulation of fake products. “We are losing foreign exchange and employment opportunities due to this situation,” he said.

According to Peiris, some money from counterfeiting businesses may even be going for the funding of terrorist organisations, including what is left of the Liberation Tigers of Tamil Eelam (LTTE). “We are already showing signs of being a commercial crime hot spot,” Peiris warned.

However, Senior Vice President of the Federation of Chambers of Commerce and Industry of Sri Lanka, Tissa Jayaweera, who also functions as the Chairman of the International Chamber of Commerce’s Sri Lanka branch, emphasised that Sri Lanka could head off this unwelcome development if there was state vigilance.

“But the state is clueless and it is not vigilant,” he said. “We need strong laws to fight this problem,” he said, adding that implementation was still the key: “We have laws, but they are not enacted – there is political patronage, this should stop: law should apply to all,” Jayaweera noted.

Date for the Diary

CCS hosts first UK Intelligence Analysis course

ICC Commercial Crime Services has developed a new three-day course on intelligence analysis. The inaugural course will run from **7 – 9 June 2010**, at the **Tower Hotel in London**. It should be popular and places are limited, so early registration is recommended.

In today's fast moving world getting access to the right information quickly and cheaply has never been more important for commercial success. However, it is not enough to just have information; it needs to be sifted and analysed to ensure that its value is maximised and vital conclusions can be drawn.

This new course will provide delegates with:

- An overview of the intelligence cycle and the analytical process.
- Techniques for thinking creatively and for collecting and analysing raw information into intelligence.
- Awareness of networks, groups, events and critical path analysis.
- Training in financial analysis, strategies and techniques.
- Participation in a simulated exercise

In addition, each delegate will receive a comprehensive e-manual, as well as a certificate of attendance.

Highly practical and interactive, the course will be led by **Jim Devery**, a well-known and highly regarded expert with a wealth of experience in this field.

It should be of interest to a range of different individuals including:

- √ Corporate security professionals in banks, insurers and multinationals
- √ Fraud investigators, accountants and analysts
- √ Investigative analysts
- √ Competitive intelligence researchers
- √ Government and private sector investigators
- √ Law enforcement officers
- √ Knowledge workers and researchers

More information and a registration form can be found at www.icc-ccs.org/IAcourse.

Corruption

Fighting Bribery: New UK legislation explained

*The UK is stepping up its fight against bribery and corruption with new legislation due to be enacted this spring. The Bill will have a significant impact upon businesses, which are likely to have to respond by tightening up their procedures. It covers commercial bribery as well as public officials, and it makes it much easier to prosecute companies. It extends UK jurisdiction to prosecute offences committed anywhere in the world, and hospitality and facilitation payments caught by the law face penalties of up to 10 years' imprisonment if convicted. The Bill is another weapon in the ever-growing armoury of prosecutors and investigators to deal with commercial crime. **Sean Larkin**, a barrister with QEB Hollis Whiteman in London explains.*



Despite recent successes, the existing law is considered out of date and will soon be replaced by a new Bribery Bill. It is the result of many years of activities against bribery and corruption. Some recent examples of prosecutorial action include:

- ❑ BAE Systems agreed to admit criminal charges and pay fines of some £286m to settle probes by US and UK authorities. The decision has provoked controversy and is subject to judicial review.
- ❑ The prosecution of Mabey & Jonson, whose self-reported offences of overseas corruption has led to fines, reparation payments and compliance monitoring. Its former chief is currently subject to criminal charges arising from that investigation.
- ❑ The £5.25m fine by the Financial Services Authority (FSA) imposed on Aon Limited (Aon Ltd) for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption associated with making payments to overseas firms and individuals.
- ❑ The conviction and custodial sentence levied against a Managing Director from who bribes were solicited by a Ugandan official.

The new Bill creates four offences:

- ◆ providing a bribe
- ◆ receiving a bribe
- ◆ bribing a foreign public official, and
- ◆ a corporate offence. Senior management may be criminally liable if the company is found guilty and they consented or connived in the criminality. The sentence will be up to 10 years' imprisonment.

In summary, the test involves the use of an advantage [not necessarily financial] to induce or reward improper performance of a function caught by the Act, which also includes work related functions.

The main changes

Ordinarily, an offence can only be prosecuted in the UK if all or part of it was committed in the UK. For example, if one shoplifted in France, it would be a crime in France but not a crime prosecutable in the UK. The activity that

will be caught by the new Bribery Bill is much wider. Henceforth, it will not matter that the bribe may be offered/paid or received outside of the UK, have no connection with the UK, and any performance affected take place outside the UK. The UK authorities may prosecute as long as the individual responsible is ordinarily resident in the UK or, if a corporate entity, has a permanent establishment, subsidiary or other operation in the UK. The courts will disregard local custom [unless permitted or required by local law] and expectation, and apply the test of what a reasonable person in the United Kingdom would expect in relation to the performance.

Corporate implications

The corporate offence is committed where a person (A), who is associated with the commercial organisation (C) [which means he performs services for, or on behalf of C], bribes another person with the intention of obtaining or retaining business or an advantage in the conduct of business for C. Clearly, this does not just cover employees but a range of agents. The definition of a commercial organisation is wide.

There is no doubt that for many years businesses have made payments either to obtain work or to facilitate the provision of services. The new Bill will, in rough terms, make all such payments criminal. If the payment is made by a person associated with the business for business purposes, both the individual and the business will automatically be guilty. The business will have a defence if it can prove it had 'adequate procedures' in place to prevent such offences.

However, the real problem is that no one knows what 'adequate procedures' are. The sorts of issues thrown up include: Who defines what is adequate? If bribery does take place irrespective of the procedures, can they be said to be adequate? How can a commercial organisation be confident it does have adequate procedures in place before investigation?

Guidance on compliance

The government realises that guidance is essential.

Corruption

The Serious Fraud Office [SFO], the lead agency in dealing with bribery, will publish guidance that will be available before the relevant offence is enacted. Lord Bach, on behalf of the government, has referred to information from reputable organisations as being a useful source of guidance and suggested that guidance from GC100 might help inform the debate.

It is thought that some assistance may be gained from sentencing guidelines in the US, which has had a similar law for many years. According to US Sentencing Guidelines, a “compliance and ethics program shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and deterring criminal conduct.” The following elements are critical to a comprehensive compliance program:

- due diligence
- promote a culture of ethical conduct
- establishment of policies and procedures
- corporate governance oversight
- high level involvement with a specific individual assigned overall responsibility
- education and training
- monitoring, auditing, and evaluation of compliance program
- reporting hotline
- disciplinary action

Of further concern to business should be the government’s attitude towards corporate hospitality and facilitation payments. The House of Lords considered adding a defence regarding corporate hospitality but in fact no defence has been added, although Lord Tunncliffe provided some comfort by writing: ‘We recognise that corporate hospitality is an accepted part of modern business practice and the Government is not seeking to penalise expenditure on corporate hospitality for legitimate commercial purposes. However, lavish corporate hospitality can also be used as a bribe to secure advantages and the offences in the Bill must therefore be capable of penalising those who use it for such purposes.’

A ‘facilitation payment’ refers to the practice of paying a small sum of money to a public official (or other person) as a way of ensuring that they perform their duty, either more promptly or at all. The Bill provides no such exception unlike the US equivalent. Although it is unlikely that a small facilitation payment, extorted by a foreign official in countries where this is normal practice, would of itself give rise to prosecution in the UK, the matter is one that will be a matter for guidance and prosecutorial discretion.

Prevention procedures

The prosecuting authorities, particularly the SFO, wish to avoid offences being committed rather than reacting once committed. They expect that businesses will

put adequate procedures in place in advance. If in any doubt businesses should engage with the SFO. Similarly, if a business suspects a crime has been committed it may be an advantage to have conducted an internal investigation, and if an offence found the business should self-report it to the SFO.

Importantly, the fact of having self-reporting and assurance of systems in place will affect the decision to deal with it criminally as opposed to civilly, the scope of liability, and the size of the fine. The SFO has produced guidance on self-reporting by companies, which is available on their website. The Mabey and Johnson case is an example of an internal investigation leading to self-reporting and a civil settlement for the company, albeit the directors have been criminally charged.

The extension of jurisdiction means that businesses may be liable to prosecution by more than one country. Prosecuting authorities are looking to arrange global settlements [e.g. BAE case] where one country usually takes the lead and the agreement settles all liability world-wide if possible.

As can be seen, the Bribery Bill is likely to have a significant impact on many businesses, and as such it will require an appropriate response to avoid protracted investigation and prosecution.

Website targets Madoff investors

The US Securities Investor Protection Corp (SIPC), the agency that keeps a reserve fund for investors of insolvent brokerages, warned last month that a copy of its website targeting defrauded Madoff investors has been set up by a phantom organisation.

The copycat site, www.I-SIPC.com - I for International - had a link to a picture of a large stack of US currency under the headline, “ISIPC & Interpol Discovers \$1.3 billion hiding by Madoff in Malaysia.” (“Hidden” was misspelled on the site, which has since been replaced by a note that it is temporarily unavailable).

In a statement, SIPC warned investors not to provide personal or financial information on the site, which has a Geneva mailing address. One passage, with spelling or grammatical errors, claims to have interviewed Madoff. “We have being tracking this stolen fund for couple of months but after concrete information got to us that Madoff might have hiding some funds in various discrete locations our teams interrogated some of Madoff past workers and with the interview we had with Madoff last month we were able to conclude our investigation,” the site said.

SIPC President Stephen Harbeck said there were some indications the bogus site may have origins in Nigeria, and that it had some aspects of “recovery room” frauds.

Cybercrime

In an era when governments acknowledge that total security of data is impossible, and the UK Information Commissioner has described data as a potential "toxic liability" to an organisation, the protection of data has never been more critical.

Last month CCI indicated how sensitive data could be protected from malicious insiders. This month we examine the consequences of not doing so.

*This article by **Shoosmiths** solicitors, in conjunction with **Bernard Parsons**, CEO at **Becrypt**, explores the risks associated with the potential loss of confidential company, customer or employee data. It also includes an overview of the relevant UK legislation and provides advice on best practice when organisations are handling such data.*

The full paper entitled "The Legal Risks of Data Loss" is available for download from: www.becrypt.com/emea/Downloads/Whitepaper-Download/

Becrypt Ltd is exhibiting at Infosecurity Europe 2010, the No. 1 industry event in Europe held on 27th – 29th April in its new venue Earl's Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

Data Loss: the legal consequences

The possible financial and commercial consequences of the loss of sensitive customer data or confidential corporate information are far reaching. Organisations need to be fully aware of the risks of losing data, as well as how to prevent it.

Such data is typically lost through carelessness, lack of training or theft. Furthermore, the loss of employee data is likely to be in breach of the Data Protection Act. This could leave an organisation open to legal claims by the employees and customers affected (if they can establish financial loss) or, alternatively, complaints to the Information Commissioner, who regulates this area. Brand damage aside, the damage to the morale and confidence of employees and customers could be substantial, further impacting on the business.

Barely a month passes without an organisation, frequently in the public sector, suffering damaging publicity through data loss. The widespread use of service providers also causes further complications, with third parties (such as contractors or suppliers) responsible for the loss of significant data.

UK Law

The most important piece of legislation to be aware of is the Data Protection Act 1998 which, among other things, sets down a number of principles for handling sensitive and personal data, such as:

- Data should be processed fairly and lawfully
- Data should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal data

Business should be aware that an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the Data Protection Act is entitled to compensation from the data controller for that damage.

Organisations should also be mindful of the powers of the Information Commissioner to impose fines for deliberate or reckless breaches of the Data Protection Act. This power was granted to the Information Commissioner in May 2008 under the Criminal Justice and Immigration Act – a clear signal that data protection must become a priority.

Additionally, while the Human Rights Act 1998 is only directly enforceable against public authorities, private sector employers need to at least be aware of an individual's right to respect for their private and family life, their home and their correspondence.

A final consideration is any contractual obligation that might have been breached by the unauthorised disclosure of information. For example, an organisation might have entered into a contract with a third party, which incorporates terms relating to how the third party's data will be secured or processed. Should these terms have been breached by any data loss incident, then the third party may take legal proceedings for breach of contract.

Cybercrime

Guidance

The Information Commissioner (www.ico.gov.uk) regulates this area and while the Codes of Practice that are issued are for guidance and not binding legislation, they will always be considered by Courts or Tribunals in determining proceedings in relation to any breach of the Data Protection Act.

The guidance covers a number of important areas for organisations that handle personal information and stresses that any organisation should analyse the potential risks that might flow from an unauthorised disclosure of the information, including:

- Identifying specific staff who have responsibility for the security of such data
- Implementing appropriate security and organisational measures to ensure the safety of such data (both technical and physical security)
- Considering the appropriate levels of security to be applied, such as encryption or password protection

It also concurs with the Financial Services Authority (FSA), which produced a specific report as a result of a review of industry practice and standards in managing the risk of data loss, that customer data must not be taken off site on laptops or other portable devices that are not encrypted; failure to comply can see the FSA taking enforcement action.

Furthermore, it highlights that many firms do not undertake appropriate risk assessment regarding

the potential loss of data, while implementation of data security policies is often patchy. The use of third parties is also identified as a potential point of weakness, with firms generally relying too much on assumptions that contractual terms were being met, without actually checking.

Over-riding everything, it is the data controller who will still ultimately need to comply with the principles set out in the Data Protection Act.

Conclusion

Important data, whether relating to customers, an organisation itself, or its employees, is clearly necessary for any organisation to function. To paraphrase the Information Commissioner, such data can be (and often is) both a crucial asset and a toxic liability. The challenge for all organisations is to assess the risks that they face, bearing in mind the categories of the data held, consider the possible consequences of any data loss, and then put in place appropriate and proportionate protections, both technical and physical, to ensure the security of the data as much as is humanly possible.

As the Information Commissioner acknowledged in an interview he gave in October 2008; "things will inevitably go wrong, therefore you should plan for things going wrong." Organisations have to become more aware that holding large elements of personal data creates a significant risk and therefore substantial protective measures are needed in order to secure that data.

Ticket cyberscam netted \$25m

PROSECUTORS in America have indicted four California men they accuse of using a network of computers and automated software to buy up online tickets to concerts and sporting events and selling them at a profit. The four are alleged to have made more than \$25 million between 2002 and 2009 by re-selling more than 1.5 million of the "most coveted tickets" to concert performances, shows and major sporting events.

Operating as Wiseguy Tickets, the men allegedly targeted Ticketmaster, Tickets.com, MLB.com, MusicToday, and other online ticket vendors. They are accused of hiring programmers in Bulgaria to create a nationwide network of computers that impersonated individual visitors to the ticket vendor sites, flooding the sites at the exact moment that the tickets went on sale. The network of computers, dubbed Captcha bots, automated and sped up the buying process by completing Captcha tests the sites presented that were designed to keep automated bots off the sites.

The men also are accused of creating shell corporations with fake domains and email addresses and aliases to deceive the online ticket vendors.

New fraud reporting system

QinetiQ recently launched a new online system that will keep EU investigations secure and anonymous, whilst protecting communications between investigators and informants. The web-based secure Fraud Notification system is currently being operated by the European Anti-Fraud Office (OLAF). It allows the office to receive tip-offs and maintain communications during an investigation while completely protecting the anonymity of the informant.

The problem of anonymity was solved by designing a system which enables a simple and secure means of communication. On entering the OLAF website, the user is guided through the completion of a questionnaire. This is the only information that an OLAF investigator ever sees; even the IP address is masked and cannot be identified. An informant can exit the system after completing the questionnaire and is not required to have any further communication with the OLAF team. However, if they do agree to ongoing communications, a clever encryption system, which is unique to each informant and each OLAF investigator, means that the identity of the informant is protected at all times, wherever and whenever they use the system.



Cybercrime

Automation of hacking presents ever greater threat

A new report from data security firm Imperva is warning that computer hackers have become industrialised and now represent an exponentially increased threat to individuals, organisations and Government. Imperva says that today's cybercrime industry has transformed and automated itself to improve efficiency, scalability and profitability.

One example of this new 'industrial revolution' is a scheme Imperva has discovered that is infecting educational servers worldwide with Viagra adverts that infect Web users with malware when they visit the infected page on the legitimate education site. The company says that cyber-criminals are using industrialised methods to automate an as-yet unreported search engine manipulation scheme that has infected hundreds, possibly thousands of .edu and .ac.uk servers worldwide with Viagra ads.

"This attack on academic institutions highlights how hacking has become industrialised, infecting servers from major institutions including UC Berkeley, Ohio State, University of Oxford and more. Ironically, this technique is the most prevalent method used to create havoc in cyberspace, yet remains virtually unknown to the general public," explained Imperva CTO Amichai Shulman.

Elsewhere, the report outlines the organisational structure and technical innovations for automating attacks. On the organisation structure, it says that a clear definition of the roles and responsibilities within the hacking community has developed to form a supply chain that resembles a drug cartel.

The division of labour in today's industrialised hacking industry includes:

- **Researchers:** A researcher's

sole responsibility is to hunt for vulnerabilities in applications, frameworks and products, and to feed their knowledge to malicious organisations for the sake of profit.

- **Farmers:** A farmer's primary responsibility is to maintain and increase the presence of botnets in cyberspace through mass infection.

- **Dealers:** Dealers are tasked with the distribution of malicious payloads.

In addition, it says that hacking techniques once considered cutting-edge and executed only by savvy experts are now bundled into software tools available for download. Today, the hacking community typically deploys a two-stage process designed to proliferate botnets and perform mass attacks:

Search engine manipulation:

This technique is the most prevalent method used to spread bots, yet remains virtually unknown to the general public. Essentially, attackers promote Web-link references to infected pages by leaving comment spam in online forums and by infecting legitimate sites with hidden references to infected

pages. For example, a hacker may infect unsuspecting Web pages with invisible references to popular search terms, such as "Britney Spears" or "Tiger Woods." Search engines then scour the websites reading the invisible references. As a result, these malicious websites now top search engine results. In turn, consumers unknowingly visit these sites and consequently infected their computers with the botnet software.

Executing mass attacks through automated software:

To gain unauthorised access into applications, dealers input email addresses and usernames as well as upload lists of anonymous proxy addresses into specialised software, the same way consumers upload addresses to distribute holiday cards. Automated attack software then performs a password attack by entering commonly used passwords. In addition, today's industrialised hackers can also input a range of URLs and obtain inadequately protected sensitive data.

Download the report at <http://www.imperva.com/ld/industrialization.asp>



COMMERCIAL CRIME

International

Published monthly by Commercial Crime Services,
Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK.

Tel: +44 (0) 20 7423 6960 Fax: +44 (0) 20 7423 6961

Email: ccs@icc-ccs.org Website: www.icc-ccs.org

Editor: Andy Holder Email ajholder@gmail.com

ISSN 1012-2710

No part of this publication may be reproduced, stored in a retrieval system, or translated in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the publishers.

While every effort has been made to check the information given in this publication, the authors, editors, and publishers cannot accept any responsibility for any loss or damage whatsoever arising out of, or caused by the use of, such information. Opinions expressed in Commercial Crime International are those of the individual authors and not necessarily those of the publisher.

Copyright 2010. All rights reserved.