



# COMMERCIAL CRIME

## International

September 2008

Volume 26 No 4

### IMB urges more 'on the water' action to curb escalating Somali pirate attacks

UN Security Council Resolution 1816 (passed 2nd June for an initial six months) may have called on all states to join together to combat piracy off Somalia's coast, but the evidence of recent attacks reported to the IMB Piracy Reporting Centre (PRC) strongly suggests the initiative is not working as planned.

In fact, so worried are German shipowners about the rising number of attacks on vessels passing through the Horn of Africa, some have raised the issue in their parliament and called for a change to the country's constitution to enable the deployment of German naval ships to the region to pursue pirates.

Insurers, too, are not happy, and are reported to be worried about the 'grey zone' between piracy and terrorism the current situation presents. Indeed, many have already raised premiums for ships visiting Gulf of Aden ports that they consider high risk. This not only increases the burden on shipowners, it also threatens to affect trade in other countries in the region who, amongst other things, are being urged to do more to protect their interests by being willing to prosecute pirates, as Kenya did in 2006.

While the German shipowners association has advised its members to sail around – and not through – the affected region, or if they must to sail faster, the ICC International Maritime Bureau (IMB)

last month issued a fresh piracy warning to vessels in the Gulf of Aden. The IMB currently advises that all Masters operating in this area maintain strict 24-hour piracy watches and be especially wary of any approaching small craft. It is also urging that all actual or attempted attacks, and any suspicious vessel movements, be reported to the PRC.

PRC reports indicate there has been a rise and not the expected fall in pirate attacks in the Gulf of Aden in the months since UN 1816 came into force. Importantly, as well as the documented hijackings the PRC says the pirates, now calling themselves the Gang of Somalia, have attempted to attack a large number of vessels in the area using rocket propelled grenades and automatic weapons. And although reports indicate that coalition warships in the area intervened to prevent attacks on two occasions, their presence does not seem to be stemming the rising tide of attacks in the region.

The Centre says there are currently three vessels being held for ransom by pirates. They include the Stella Maris, at 55,000 tonnes the largest vessel ever captured in the Gulf of Aden, which together with its 21 crew is being held at Eyl on the Puntland region border pending ongoing negotiations. Another is a Nigerian tug captured off Bossasso in August during a delivery run from

the Middle East. The third vessel, attacked on August 12th en-route to the Red Sea, is a Thai-flagged 16,000 tonne general cargo ship with 28 crew aboard. She is also being held in Eyl whilst negotiations for her release continue.

"1816 is clearly not working as envisaged," says IMB Director Pottengal Mukundan, whose organisation has been monitoring the situation closely. "Far from coalition warships disrupting pirate activities the pirates actually seem more emboldened and determined to escalate their attacks, which are notably more violent," he adds.

Captain Mukundan believes that unless there is a more active

*Continued on page 6/*

#### In This Issue of CCI

##### FRAUD

Olympic ticket scam	2
Global website a front for fraud	3
Banks accused of fraud in auction rate securities selling scandal	4

##### COMMERCIAL CRIME

Using email analysis to detect fraudulent activity	6
--	---

##### NATIONAL PROFILE

India moves against deeply engrained commercial crime	8
---	---

##### CYBERCRIME

Impacy and working or organised criminal organisations	10
Backing behavioural analysis	12

## Corporate legend the place to look when documents arouse suspicion

BANKS finding it difficult to verify documents presented to support finance proposals are being advised to extend their investigation and look into the authenticity and capability of the parties apparently behind the deal.

This is a technique regularly used by investigators working for the ICC Financial Investigation Bureau (FIB) and in the majority of cases it provides sufficient information to reach an appropriate conclusion.

For instance, a member bank recently asked the FIB to look into a proposed deal to finance a construction project in Papua New Guinea. Two companies based in the Far East had offered to provide the necessary finance, using as collateral the negotiable instruments of a well-known international financial institution based in the US.

Although suspicious because of the large sum involved, the bank was unable to determine the bona fides of the proposal with certainty based on just the documents provided, so it asked the FIB to check out the parties involved. And although the parties and their principals were not previously known to the FIB, or on its database, the checks very quickly revealed enough information to stop the proposed deal from going any further.

FIB investigator Debbie Hull was intrigued when she couldn't find any information on one of the companies in its home country. If the company was legitimate and of sufficient size to finance a project in excess of a hundred million dollars, it would be reasonable to find some evidence of its existence.

The second company was listed, but only since last year, and was very unlikely to have developed

the financial capacity to underwrite such a big deal within the timeframe. Evidence to support this could be found on its website, which claimed it was well established but contained no contact details and was peppered with spelling mistakes. Moreover, the website was not even registered.

"We regularly conduct deep enquiries of this nature for clients and have become quite adept at delving behind the scenes and spotting the flaws," says Ms Hull. "As this case demonstrates it is often relatively straightforward to discover gaps in a company's profile. However, others have a much more professional legend and present a much greater challenge. But if they do make a mistake there's a pretty good chance we will find it," she adds.

## Money laundering fine

IN a first case of its kind, America's SEC has fined E\*Trade Financial Corp \$1 million to settle allegations that it failed to abide by US anti-money laundering rules, which require that broker-dealers verify the identities of their customers and document their procedures for doing so.

The SEC found that E\*Trade Clearing LLC of Jersey City, New Jersey, and E\*Trade Securities LLC in Menlo Park, California, failed to accurately document certain customer identification program practices and verify the identities of 65,442 of its customers as required by the USA Patriot Act and SEC rules.

It also said that E\*Trade's compliance failure was "systemic" and resulted from a "lack of a cohesive organisational structure [and] lack of adequate management oversight."

## Olympic ticket scam

LAST month's Beijing Olympics have been hailed a great success but it now seems that defeated competitors were not the only losers. Hundreds were apparently caught out by an international internet tickets scam when they booked seats at venues on [www.beijingticketing.com](http://www.beijingticketing.com).

The International Olympic Committee received hundreds of complaints after the elaborate sham website lured thousands of sports fans from US, Britain, Canada and Australia to buy fake tickets over the internet. It is believed some victims paid more than \$60,000 for tickets to Olympic sports and only realised there was a problem when the tickets never arrived.

The professional and sophisticated website boasted offices in Sydney, London and New York, but the tickets it sold never existed. Apparently, it was so well laid out it even duped IT workers that specialise in online fraud. But the good news, according to Visa International, is that card holders should be able to recoup their money as the bank which granted merchant facilities to the website would be liable for the fraud.

Meanwhile, it appears the scam's operators vanished just days before the opening ceremony in Beijing. The only address on the website led to an office in Phoenix, Arizona, but desperate fans hoping to travel to Beijing discovered another dead end when they visited the office, which was empty. And the telephone number listed on the website was constantly engaged.

Revelations of the scam come after a series of similar scams launched in the past year in China. Three scammers were earlier arrested in Fujian province for operating a sham Olympic tickets website called 29th Olympics.

## Global conglomerate website claims were just a front for fraud

AUSTRALIAN Robert Bassili's global conglomerate Radisson Maine once boasted on its website that it offered "all aspects of strategic financial strategies and wealth creation...under the one roof."

In fact the 'one roof' was just that, a house in a Sydney suburb where he and his partner concocted their fraudulent property schemes.

Last month Bassili was jailed for three years after being convicted on two counts of fraud. He was arrested at London Heathrow Airport in May and extradited to face trial. Law enforcement had been pursuing him since he left Australia for Ukraine in 2004 when regulators wound up Radisson Maine, which at the time owed 30 investors Aus\$ 3.3 million.

The website was key to the scam. Its spiel was flashy but without substance. Investigators found little evidence to support Radisson Maine's claims to have offices in Geneva, New York, Toronto, London, Melbourne or Canberra. They certainly were not in the

telephone book, nor accessible via international directory assistance. The whereabouts of "Radisson Maine Airlines" and the precise location of the head office of "Shipping & Cargo" (which was said to be in Singapore) also proved impossible to find. The container ship pictured on the conglomerate's website had to be docked somewhere and the Boeing 737 surely had a hangar?

According to the website, Radisson Maine was a "global to global" business and at first glance it did appear to command significant resources: no less than 78 regional general managers, sales managers, marketing managers, marketing co-ordinators and strategic client advisers - world-wide, of course. But few apparently noticed that Bassili and his partner were not even born in 1964 when the website claimed the company was established.

In the end, it turned out to be nothing more than a front for a mortgage-broking operation run by the two men.

## 'Secret' HYIP touted by man claiming to be an attorney and former FBI agent

POLICE in America last month arrested an 'attorney' and charged him and others with fraudulently promoting a high-yield investment program scheme that promised an extremely high return at little or no risk to principal.

The accused also allegedly boasted to undercover FBI agents about their ability to place them into a "safe... no risk, secret program." The undercover agents were told they would have to undergo a "compliance" process and be subjected to a "due diligence" scrutiny by the Central Intelligence Agency, among others.

Richard Pundt and the others claimed their investment program was a "Fed Trade Program" regulated by the "Fed" and they had to follow strict "Fed guidelines," according to the indictment. Once the investor passed the compliance they would become "registered in Washington, D.C. with the Fed."

Pundt, who claims to be a former FBI agent, is the president and CEO of a company called enlighten technologies. The company's website also says he is an attorney in Cedar Rapids, but he isn't listed as practicing on local bar association sites.

## SEC says WexTrust was Ponzi scheme

AMERICA'S SEC has filed a major case against WexTrust Capital (a Chicago-based private equity firm), its partners and various investment affiliates, that allegedly ripped off an estimated 1,200 investors to the tune of up to \$100 million using a classic Ponzi scheme.

The defendants are accused of fraudulently raising money in various offerings, each of which purportedly is for a particular investment, without disclosing that funds raised were actually being used to pay prior investors in unrelated offerings and to make unauthorised payments to fund the operations of the Wextrust Entities, which were operating at a deficit. An internal Wextrust combined "balance sheet" shows that as of December 31, 2007, Wextrust Entities "borrowed" at least \$74 million from the LLC entities and also "lent" at least \$54 million to various LLC Entities.

Altogether, the SEC alleges that WexTrust Capital conducted at least 60 private placement offerings and created approximately 150 entities in the form of limited liability companies or similar vehicles. Throughout the process, the SEC alleges, WexTrust Capital partners didn't disclose material information and never purchased the properties it promised to investors.

And while it is thought likely WexTrust Capital will attempt to defend itself by saying that investments simply went south and it's "buyer beware, the SEC evidence suggests otherwise. It has an email from one of the defendants, who has a prior conviction for bank fraud, to a business partner that shows they both were aware their activities were fraudulent.

*Suspicions of fraud are rapidly becoming accusations as more is revealed about several banks' alleged manipulation of America's Auction Rate Securities market, which collapsed earlier this year. As the US House Financial Services Committee prepares to hold a hearing later this month in a bid to find out what went wrong, **Andy Holder** collates media reports to relate the tale of alleged wrongdoing and deception to date.*

## Preacher's pyramid scheme netted \$330m

AMERICAN preacher Neulan Midkiff was found guilty on 21 counts of mail and wire fraud and tax evasion last month. The 66-year old got many of his friends and neighbours involved in an Atlanta company called Horizon Enterprise, which promised high returns on an overseas banking deal but was actually a pyramid scheme that took in as much as \$390 million. The scam paid investors "interest" using their own principal or money from new investors.

Offshoots, Central Financial Services and Joshua Tree Group, also run by Midkiff meanwhile scammed another 519 people from Minnesota and Louisiana out of \$30 million.

Midkiff testified that he was duped by Horizon's founder, Travis Correll, and didn't know he was involved in anything illegal. Correll, of Atlanta, pleaded guilty to charges against him and was sentenced to 12 years in prison. Midkiff is due to be sentenced in October.

## Litigation ramps up accusations of securities fraud by major banks

Numerous recent lawsuits accuse some of the world's largest banks of collusion, market manipulation, miss-selling and misrepresenting the risk of investing in Auction Rate Securities (ARS), resulting in an estimated \$40 billion loss that has hit around 250 public companies and thousands of individual investors.

Amongst the most litigious to date are the US states of New York and Massachusetts, who have both filed law suits against Swiss bank UBS. Meanwhile, it is reported that the SEC and state attorneys from 12 states are also investigating the ARS activities of several others, including Merrill Lynch, Citigroup, Bank of America and Wachovia.

As well as emerging evidence that they duped clients into investing in a market they knew to be collapsing in a bid to reduce their own exposure, it is now alleged the banks colluded for up to two years to prop up the weekly auctions that were supposed to set the rates on these securities. As a result, when the market collapsed in February, many customers faced losses or were stuck with securities they could not sell.

### 'Safe' bonds?

Auction Rate Securities or 'safe bonds' – issued by municipalities, student loan companies, charitable organisations and others – are long-term securities that the banks engineered to have short-term features. Their interest rates were reset at weekly or monthly auctions run by the banks, who assured investors that the frequent auctions made these securities as safe and liquid as cash, because they would always be easy to sell quickly.

However, demand for ARS started to evaporate during last year after an accounting ruling determined they should be classified as long term, and not short-term investments. Corporate cash managers stopped buying them, and companies started liquidating them – some \$70 billion worth in the second half of 2007 alone.

In normal times, when the weekly auctions of ARS's failed to generate sufficient demand, the banks would step in to support the market, buying the instruments themselves. But as they became constrained by other problems, notably the fallout from the Credit Crunch, they stopped supporting the market with their own bids. By February, nearly every auction was drawing insufficient buyers and the securities became illiquid, making it impossible for investors to cash in. And the banks who had encouraged clients to buy into the \$310 billion ARS market were nowhere to be seen.

### UBS allegations

At the root of the fraud claims are the allegations that the banks foresaw the problem in the ARS market, but instead of acting in the interests of their clients they actively sought to rid themselves of the troublesome financial instruments by aggressively pushing them to customers whilst playing down the severity of the problems rippling through the market.

In its complaint, for example, the state of New York alleges that several high-ranking UBS executives sold roughly \$21 million of their own ARS

holdings amid the turmoil and left over 50,000 UBS customers holding \$37 billion worth of the struggling investments.

The complaint filed by the state of Massachusetts against UBS meanwhile presents alleged email evidence of the action senior executives were taking to liquidate its \$11 billion worth of ARS by pushing them onto customers. Even as late as January, when the bank had effectively pulled out of the market, it is alleged UBS continued to provide sales staff with marketing materials to promote the investment.

The email evidence suggests that UBS, which sold \$42 billion of ARS between 2002 and 2007 and earned fees from underwriting and managing the auctions, identified the hazards of ARS as early as August 2007 and began to immediately mobilise its staff.

Noting in one email that “the pressure is on to move inventory,” bank executives are alleged to have held more than one dozen conference calls with sales staff and sent them new marketing materials to promote the securities, raising their commissions but without telling them how risky they were. This appears to be underlined in an email to those leading the sales force who were told “We need them to walk out and believe this is a strong credit with strong UBS commitment to support the liquidity.”

The emails apparently also show that UBS officials considered pulling out of the ARS market in September, five months before the bank actually stopped supporting the programs.

“This is a huge albatross,” said one email from a UBS executive apparently being pressurised to unload \$1 billion worth of ARS as the bank sought to free up capital. “We need to move this paper and have to explore all angles possible. We need to do this as quickly as possible,” said another email from the same person a few weeks later.

And the emails apparently also reveal that the bank was able to exploit a new opportunity when the market did eventually collapse and hundreds of auctions failed in February. Facing having to pay interest rates approaching 20%, many of the municipalities holding ARS called their bankers looking to refinance the debt, giving the banks a chance to generate new underwriting fees.

“We have a money making opportunity. They are desperate,” said one email from an investment banker. Later the same day (February 14), in another email, a UBS executive allegedly wrote that “the refinancing of the bonds is the single greatest opportunity in decades for us to leverage our banking relationships,”

and described the situation as “a bankers dream market.”

With its reputation on the line, UBS has responded to the numerous allegations and lawsuits saying it will vigorously defend itself against the complaints. UBS does not believe that there was any illegal conduct by any employee. And it adds that an internal investigation into personal sales of ARS only found cases of poor judgement by certain individuals, for whom it is currently evaluating appropriate disciplinary measures. So far, all the other banks being investigated have declined to comment.

### **‘Sudden’ collapse claims discredited**

UBS is not the only bank under the ARS spotlight. The Massachusetts Secretary of State has also accused Merrill Lynch of misleading investors about the stability of the market, and in particular of publishing reassuring research about ARS just days before it pulled out.

“This company was aggressively selling the securities and its auction desk was censoring the research analysts to make sure they downplayed risks in the market,” said William Galvin in a July statement. “They knew the market was in trouble, but the investors were the last to know,” it added.

The Massachusetts complaint alleges that Merrill Lynch made around \$90 million profit from its auction rate program during 2006 and 2007, and quotes one of the bank’s executives as saying in a November 2007 email: Market is collapsing. No more \$2k dinners.

Whilst the ARS fraud debate has a lot further to run, what is becoming clearer is that the banks earlier claims of ‘sudden’ failure in February are beginning to look weak. The email evidence is compelling, and Financial Week revealed last month that the ARS auctions began failing as early as September 2007. Indeed, it now appears the writing may have been on the wall as early as 2005, when ARS were reclassified from cash equivalents to short-term investments. In 2006, it turns out, the SEC fined 15 broker dealers for intervening in the bidding process, i.e. they took the place of customers in supporting the auctions.

More revelations can be expected, but in the meantime the banks are starting to face the consequences. Last month UBS was fined \$150 million by regulators and forced to buy back \$19.4 billion worth of ARS. Citigroup Inc agreed to buy back \$7.3 billion in illiquid auction-rate securities and pay \$100 million in civil penalties, whilst Merrill Lynch is reportedly set to buy back \$10 billion worth of ARS beginning in January. At the time of writing, JP Morgan Chase, Morgan Stanley and Wachovia were also reported to be close to agreeing deals with government regulators to buy back auction rate securities.

New ways of analysing emails are making corporate crime more likely to lead to punishment says **Alan Woodward**, Chief Technology Officer at the business and information technology consultancy Charteris plc.



## Somali piracy

from page 1

response the pirates will continue to push the boundaries and mount ever more audacious attacks. Along with the IMB's new piracy warning he is therefore urging the naval units in the area to make more use of the powers UN 1816 provides and send a clear message to the pirates that their activities will not be tolerated. "If they don't, we can expect more attacks and hijacks of even larger vessels. Ignoring such audacious crimes in a country without an accountable central government may lead to greater instability and other sinister forces taking control," he says.

"Diplomatic measures are not enough. The main action has to take place on the water and I urge those with navies in the region to take a more robust stance while there is still time to make a difference," he adds.

## Using email analysis to nip corporate crime in the bud

The movie *Minority Report* depicts a future society where a 'pre-crime' police department uses the services of a team of savants to arrest murderers moments before they would have committed their deed. Its science fiction, but modern analytical techniques being applied to corporate email communications may soon be facilitating the spotting of serious impending crimes before they actually take place, bringing the world of *Minority Report* a step closer.

If you want to see in action the moral decadence that could so easily imperil Western civilisation, and if you also want to enjoy some interesting entertainment at other people's expense, you could do a lot worse than log on to [www.enronexplorer.com](http://www.enronexplorer.com). The site provides more than 200,000 emails sent to, from and between Enron employees during the period 1999 to 2001, when Enron finally collapsed.

The little known Federal Energy Regulatory Commission (FERC) of the United States has made these emails public to stimulate research into how corporate email data could be forensically analysed. The Enron Explorer website gives one way of conducting just such a forensic analysis, as well as offering the results of some particularly interesting suggested searches. Its extraordinary how hubris, coupled with an apparent sense that no-one would ever discover what was really happening at Enron, led many executives who were doubtless originally perfectly respectable professionals to commit a whole host of serious errors of judgement and, eventually, crimes.

The Enron emails were investigated with a great deal of laborious forensic work once the authorities had access to Enron's corporate email records. Increasingly, however, there's a feeling that the importance of email inside the corporate environment is so great that a more efficient way needs to be found to vet emails.

The very fact that the emails they use at work do constitute a record of such behaviour may be a surprise to many people, not least those who are happy to chronicle their misbehaviour by email in the first place.

### A permanent reminder

Many people are unaware that emails can be a *permanent* record. We may be tempted to think that because emails themselves often seem highly ephemeral, and can be written in a matter of moments, they aren't a permanent record. But they are. Emails are in most cases as permanent as any written document. With many companies archiving emails for long periods of time, one that may take only a moment to send can survive for a long time.

If the enormous database of Enron emails teaches us anything, it is that people will often write something in an email they would never dream of putting in a formal hard-copy memo. Yet emails and memos are really equivalent and indeed emails are in a sense even more permanent as they can so readily be copied or forwarded electronically.

According to a survey conducted in March 2008 by Proofpoint - a company that offers unified email security and data loss prevention services - over one third of UK businesses with more than 20,000

employees regularly read or otherwise monitor emails going out from their corporate systems. In the US it is over 40%. Of course, the numbers of emails leaving the corporate network are only a small fraction of the total number of emails sent between employees every day. As the vetting process is currently primarily manual it's not practical to monitor all internal emails as well as looking for the obvious breaches of confidentiality that might occur by sending sensitive information outside the corporate network.

### Email searching techniques

So how do you find the needle of incriminating evidence in the haystack of all the innocuous emails circulating within a large business?

In a digital age, it is not surprising that forensic investigators are trying to find ways to use digital techniques to sift through emails more efficiently. It's logical that in a world where modern internet search techniques are so powerful, it should be possible to devise some way of searching through emails with similar effectiveness. After all, we've all done web searches that produce extremely rapid results based on searching for a key word or phrase.

It's already possible to use modern search tools to locate emails that contain key words or are from or to specific individuals. Any email system administrator can easily use the tools that come as standard on email servers to conduct such a task. These currently-available search techniques are proving highly effective in analysing evidence for cases where (as is usually what happens) people still do not try to conceal what they are saying and say the most injudicious things in emails.

For the future there are emerging techniques, using technologies from state-of-the-art, leading-edge developments in areas such as natural language processing, which involve search engines being programmed not only to look at specific *words* used in a dialogue but also at *the way in which the words are used*.

The result of these new techniques, if properly deployed, is that meaning can be inferred and relayed to the searcher. Such methods may initially operate in a rather clumsy fashion, but there is little doubt that the programs performing these types of searches will to some extent be capable of self-learning and self-improvement.

Of course, the above techniques work best when you already know that a situation needs detailed forensic analysis. What if you don't know that a specific crime has taken place but want to see if there is suspicious behaviour underway? This is where a relatively mature technology known as 'link analysis' comes in.

### Link analysis

Link analysis is where you use the information stored in all corporate email systems that shows who sent a message to whom and when. By studying these patterns you can build up a picture of the interactions between people using the corporate infrastructure, and from there try to deduce who may have been involved in the sort of activities that resulted in the downfall of Enron.

Today, link analysis is being combined with 'text mining' (deriving patterns and trends from words used in text through statistical analysis) and 'data visualisation' (presenting the results of any data analysis in a graphical or diagrammatic form rather than as a list of numbers or further text) to try to find signs of errant behaviour. These techniques will surely become more refined in time. Ideally, future Enrons will be nipped in the bud.

Certainly, applying these techniques retroactively to the Enron dataset shows beyond doubt that the behaviour that shocked the world could have been spotted early on if the right technology had been monitoring Enron's email system.

However, if the executives within a business are the very people committing the crime then one is bound to ask:

1. Who exactly should be carrying out the analysis and monitoring the findings?
2. As the emerging technology begins to show who may be *about* to commit a criminal act, when should they be challenged?
3. Should users of corporate email systems be allowed to treat their emails as private? Most companies of any size these days have a policy that clearly states that any email sent using the company system is subject to scrutiny. But how many people realise this, and would they start to object if they felt there was active monitoring of all emails rather than just retrospective analysis of 'incidents'?

The technology to vet emails successfully from a range of powerful perspectives is coming. Indeed, some of it is already in place. And, as is so often the case, company executives, the law, and regulatory bodies, will need to ensure that they are not only keeping up with the technology but are, in a very real sense, ahead of it.

Otherwise, make no mistake, the bad guys - and girls - are going to win.

More information: Tel: 020 7600 9199.  
E: [alan.woodward@charteris.com](mailto:alan.woodward@charteris.com) [www.charteris.com](http://www.charteris.com)

*The rapidly growing Indian economy is experiencing a sharp rise in corruption, money laundering and various other financial crimes.*

*However, the central government is trying to curb fraudulent activities and make the system more transparent.*

**Raghavendra Verma**  
*reports from New Delhi.*

## CCS to launch IFAN for accountants

CONTINUING the successful concept established with the creation of FraudNet, the international network of specialist fraud and commercial crime law firms, ICC Commercial Crime Services (CCS) has announced the launch of IFAN – the International Fraud Accountants Network.

IFAN aims to bring together a number of small to medium-sized specialist fraud accountants in different parts of the world and provide a network to which victims of fraud and their professional advisors can turn to seek assistance and redress. The network will also enable fraud accountancy specialists to share information and best practice, and relate to other organisations who can provide both assistance and referrals of work.

IFAN will be run by CCS from its London office, and apart from being a point of reference for contact and liaison will also bring IFAN members the International Chamber of Commerce seal of approval and backing. Memberships costs £1,600 per annum and includes a number of benefits that are already proven to bring synergy and brand awareness, increasing the opportunities to win new business. For more information on IFAN and how to get involved, contact Peter Lowe: Tel: +44 207 423 6960, email [PLowe@icc-ccs.org](mailto:PLowe@icc-ccs.org) or see [www.icc-ccs.org](http://www.icc-ccs.org)

## India starting to move against deeply engrained commercial crime

India is a “fraud haven” says a recently released survey (March 2008) by the US-based accounting giant KPMG. From 12,374 in 2005, the number of detected economic frauds (as per government data) rose to 22,280 in 2007, and the country is now listed at 74<sup>th</sup> position in the Corruption Perception Index of Berlin-based Transparency International.

Focusing on the corporate world, 60% of the firms covered in the KPMG survey detected fraud in past two years, and at least 5% lost more than \$2.5 million each. According to India Forensic, a private fraud examination and forensic accounting organisation, Indian companies lose around \$40 billion every year to frauds committed by their own employees.

The situation might be still worse, as according to another survey released in October 2007 by PricewaterhouseCoopers (PwC), nearly 50% of frauds in Indian companies are discovered by chance, and there are many harmful after-effects caused by reporting a fraud that deter many companies from making them public.

These factors, however, become irrelevant when the perpetrators of the crimes are the owners themselves. A senior executive in a Delhi-based multinational joint venture told Commercial Crime International on condition of anonymity that in his company, contractors are engaged with an understanding to inflate their bills by 12% and remit this money in cash to the Indian promoters. Furthermore, these Indian partners have sold personal assets at highly inflated prices to the company.

The executive said: “Even after billions of dollars have been pumped in by the foreign company, the joint venture is run, for all practical purposes, by the Indian promoters and there are hardly any checks and balances.”

Many foreign partners live with the situation because of a government regulation that requires foreign companies to get a ‘No Objection Certificate’ from their joint venture partners before starting operations.

### Changes expected

However the situation might soon change, as according to a July 19 news report in the Economic Times newspaper, the central government is planning to scrap this regulation (known as ‘Press Note 1’), having concluded it hinders foreign investment. The move, whenever it comes, would be consistent with the recent steps taken by New Delhi to curb overall corruption and enhance fair play in the corporate world. A key step has been the establishment of a Competition Commission of India, charged with reviewing anti-trust and monopolistic risk prior to large mergers and acquisitions. Also, in January, the stock market regulator, the Securities and Exchange Board of India, issued strict guidelines on curbing insider trading. And to check money laundering activities, India now has a functioning Financial Intelligence Unit (FIU), which scans through millions of bank transactions every year, and has been a member of the international Egmont Group of FIUs since 2007.

One piece of national legislation that has made the most important impact on corruption has been the Right to Information Act, implemented in 2005. Under this law all government departments

## Organised cybercrime

*from page 11*

breach is on the rise as well. A recent example is the international gang of 11 cybercriminals who stole 45.7 million credit/debit cards from customers in the UK, US and Canada by breaching TK Maxx's computer systems.

Executives and managers need to deal with the risk of successful data breaches, which will impact the performance and profitability of the organisation.

An excellent way for executives to protect themselves and their organisations against this kind of cybercrime is to opt for a multi-layered security solution, such as Finjan's active real-time content inspection. To prevent Crimeware and Web 2.0 attacks, malicious inbound and outbound content is detected based on the code's intended criminal action; not on signatures, URLs or reputation attributes. With the use of real-time code inspection, enterprises can be sure that no malicious content enters their networks and steals their valuable business data.

For more information telephone +9729 864 8200, email info@finjan.com or see www.finjan.com

have to furnish any information (excepting specified state secrets) demanded by citizens within 30 days against small fees of \$1.20 (Indian Rupees 50). In 2007, government even reluctantly agreed to allow hand-scribbled notes by the officials on the sidelines of documents to be released. As NGOs and media are making extensive use of this provision, many cases of favouritism and corruption have been exposed.

### **Fraud exposed**

It is probably because of this changed environment that long-standing frauds are now coming to light; for example one audacious corruption case exposed in February. An administrative officer at the Ghaziabad district court – neighbouring New Delhi – was arrested for siphoning-off nearly \$1.75 million since 2001 from the provident (pension) fund account for sweepers and peons (low level office staff) working in various courts. He forged identity documents and created fictitious accounts to withdraw the money, but this could not have been done without the sanction of his seniors. During interrogation he named 26 sitting and retired judges as a party to the crime.

In June, after initial investigation, the state police approached the Chief Justice of India for the mandatory permission to question these judges. Though the Supreme Court has since issued new guidelines for the financial conduct of the lower judiciary, permission for this questioning is still awaited.

It is likely the new transparency laws will expose more public corruption, as bribes to government officials are the most common economic crime in India, according to the PwC survey: so much that companies have devised special ways to handle these payments in their accounts.

The foreign companies that are covered by their home laws, like United States' 'Foreign Corrupt Practices Act' are somewhat careful about making under-hand payments, said Mayur Joshi, chairman of India Forensic. However, "for accounting purposes, all companies take the help of their chartered accountants by getting a consolidated invoice, which show bribes as consultancy fees," he told CCI.

And in India, white collar crimes can also come laced with violence. Take India's banks: they know that most defaulters tend not to heed polite calls and therefore hire local musclemen, usually called goons in India, to impose the fear factor.

"Our judicial system is very slow and we do not have any [consolidated national level] data on defaulters, who regularly approach different banks for new loans," said Shyam Raghuwani, a private consultant and a former banker, "so there is no alternative to hiring agents."

But after numerous physical assaults on loan defaulters and a few suicides driven by extreme harassment by loan recovery agents of private banks, in May this year the Reserve Bank of India – the country's central bank – issued strict guidelines for the conduct of these agents. These have not gone down well with commercial banks and their standard business model of aggressive marketing with least due diligence, backed by an assured means of recovery.

However, in response to the central bank's new strictness, some banks have stopped giving personal loans of around \$700 to their not-so-wealthy clients, although the incidents of criminal assault by the agents are still making headlines.

Cybercrime is a fast-expanding, global industry, operating in a major shadow economy that closely mimics the real business world and where money, not ego, is now the driving force behind the growth of targeted attacks against financial institutions, enterprises and governmental agencies. In this article

**Yuval Ben-Itzhak,**



Chief Technology Officer, Finjan, details the parallels between profit-driven cyber-crime groups and organised criminal groups. He also explains how they work, outlines what their security breaches are costing business and suggests what can be done to try to contain them.

## Organised cybercrime organisations: their impact and modus operandi

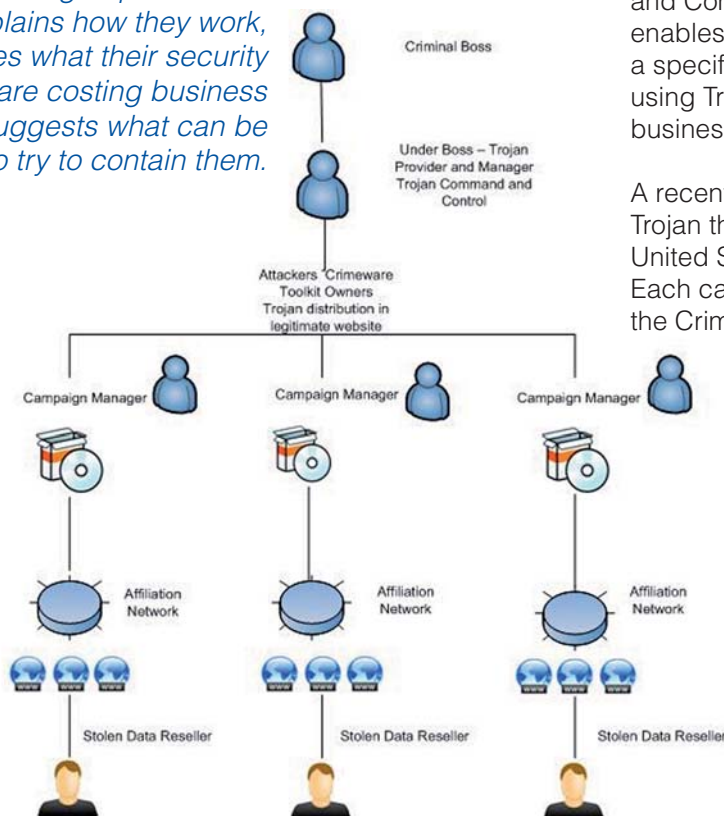
The transition of cybercrime from amateur hacker attacks to highly professional cybercrime business models is reflected in the new organisational structure of cybercriminals. Individual hackers operating independently, or groups of hackers with common goals, have been replaced by hierarchical cybercrime organisations where each cybercriminal has their own well-defined role and reward system.

Current cybercrime organisations bear an uncanny resemblance to organised crime organisations such as ‘La Cosa Nostra’.

- In both cases, the “Boss” is the head of the organisation. He operates as a business entrepreneur and doesn’t commit the (cyber) crimes himself.
- Directly under him is the “underboss” acting as the second in command and managing the operation. In cases of cybercrime, he is the one that provides the Trojans for attacks and manages the Command and Control (C&C) of those Trojans.
- Similar to the mafia, where several “capos” operate beneath the underboss as lieutenants leading their own section of the operation, “campaign managers” lead their own attack campaigns. These campaigns enable the criminals to operate in a market that is highly sensitive to location, language and regional economic trends. Since they cannot use a ‘one-scheme-fits-all’ approach, their attacks focus on specific geographic regions and target selected businesses. Each attack (called a ‘campaign’) incorporates Crimeware toolkits, Trojans and Command and Control (C&C) servers. It enables the cybercriminal to drive traffic from a specific region, with specific characteristics, using Trojans designed for targeting selected businesses.

A recent example is the highly effective ZeuS Trojan that stole \$6 million from banks in the United States, United Kingdom, Spain and Italy. Each campaign was responsible for distributing the Crimeware Trojan to specific “territories” based on the type of compromised websites (e.g. financial), the location (e.g. banks located in the City of London), etc. It illustrates how today’s cybercriminals are deploying the “think global, act local” business strategy.

- They use their own “affiliation networks” to perform the attacks and steal the data, the same way “soldiers” are used in a mafia family to do the “dirty work”. These affiliation networks act as distribution channels, and are especially created to promote infections.



They provide incentives to attackers who hack into legitimate sites and insert a reference to malicious code operated by other attackers. Once the malicious code runs, participants are paid according to the amount of achieved infections. The rate usually depends on the country of origin of the infected computer.

- The stolen data is then sold by “resellers”, similar to the Mafia’s “associates”. These resellers are not involved in the Crimeware attacks, but trade the stolen data similar to a “fence” dealing with stolen goods. They use pricing models for the different kinds of products they offer. Commodities, such as standard credit cards, are priced at a lower rate (e.g. \$15 for a US standard Master or Visa credit card) than the more premium articles (e.g. \$90 for a EU or UK Visa credit card). Since credit cards and bank accounts are being commoditised, the prime targets are now healthcare related information, single sign-on login credentials for organisations, email exchanges, Outlook accounts and FTP accounts. These are considered premium goods in the criminal economy, and can be traded for high prices. The resellers also provide service and give guarantees to their (potential) buyers, again uncannily similar to legitimate business practices.

## **Crimeware business models**

For their operations, cybercriminals use sophisticated *Criminal-2-Criminal* (C2C) Crimeware business models. These crime pros use robust and scalable Crimeware that gives them maximum flexibility in terms of command and control for stealing and trading data. They use the latest Trojan technologies, silent installations and drive-by downloads for their attacks, successfully infecting PCs and networks around the world.

*Crimeware Toolkits* consist of “how to...” software packages that instruct users step-by-step how to infect a system and then retrieve data for financial gain. Using such a \$100-\$200 off-the-shelf “Do It Yourself” toolkit, cybercriminals can easily gain access to the balance sheets of companies and manipulate stock behaviour; locate payroll information; get hold of corporate bank statements and transfer money from that business or make transfers between accounts; gain access to companies’ budgets and private financial statements; steal companies’ product road-map and R&D work-plan for industrial espionage; capture companies’ credit card numbers for purposes of fraud; or steal Intellectual Property (IP).

Crimeware toolkit creators are also copying the *SaaS* (Software as a Service) business model – often referred to as *CaaS* (Crimeware-as-a-Service). In the beginning of this year, we saw a new version of the notorious NeoSploit Crimeware toolkit that contained a delivery system for the Trojan upon a successful exploitation. It could be configured to provide a different version of

the Trojan according to the country where the victim was located.

Cybercriminals also deploy the *data supplier model* - criminals just need to log into their “data supplier” and download any information suitable for them to conduct their crime – be it financial fraud, industrial espionage or identity theft.

Once the data is stolen, hackers use *Crimeware servers* as a command and control for the Crimeware that was executed on infected PCs. They also use these servers as “drop sites” for private information being harvested by that Crimeware.

## **Effects of Cybercrime**

Although web attacks use security holes in Internet browsers, the problem has become a major business one, compromising enterprises and organisations around the world. The damage that Crimeware attacks inflict is widespread and long-lasting, for victimised organisations and individuals alike.

Financial damages resulting from Cybercrime 2.0 will keep on running into millions of dollars, and no organisation, company, enterprise or business with Internet access is safe. This vision is confirmed by Marcus Alldrick, responsible for Information Protection and Continuity at Lloyd’s. He pointed out that targeted attacks perpetrated by organised crime are on the increase due to the high return on investment. ([http://www.lloyds.com/News\\_Centre/Features\\_from\\_Lloyds/Cyber\\_crime\\_provokes\\_new\\_security\\_concerns\\_130308.htm](http://www.lloyds.com/News_Centre/Features_from_Lloyds/Cyber_crime_provokes_new_security_concerns_130308.htm))

Successful data breaches can result in a wide range of business damages, including: loss of existing customers; difficulties in acquiring new ones; loss of intellectual property; loss of R&D data, including product designs and road maps; brand name and corporate image damage; negative impact on competitive position; loss of market share; potential lawsuits and class actions; non-compliance with rules and regulations; loss of productivity due to downtime, investigations and damage control.

According to the 2007 Ponemon Institute Annual Survey, the average cost per data breach incident last year was \$6.3 million, while the cost of lost business per incident was estimated at \$4.1 million, an increase of 30% compared to 2006. The average cost of each compromised record was \$197, while the average cost of a data breach in the highly regulated financial sector was \$239 per compromised record. The average cost of a third-party breach (cybercrime attack) is estimated at \$231 per compromised record.

The total amount of compromised records per data  
*Continued on page 9/*



Cybercrime

## E-banking research supports case for behavioural analysis

RESEARCH by the University of Michigan has discovered that 75% of e-banking sites have at least one design flaw that leaves customers exposed to cybercrime.

The research, which surveyed some 214 US e-banking sites, is notable as it reveals that many of the site flaws cannot be fixed by a software patch, but are structural in nature. This means that short of many of the site operators designing their portals from the ground up its likely there is no short-term fix.

What it demonstrates is the need for businesses and providers to install behavioural analysis security technology if they make use of online banking services, as many firms now do.

The conclusion is supported by Geoff Sweeney, chief technology officer with Tier-3, who says "E-banking offers companies a high degree of convenience, but the risks for businesses are far greater than for consumers, as business balances held in bank accounts can easily run into four or five figures.

"Now that the details of this in-depth research have been published, it will be interesting to see how the report is received.

"Some banks are reported to have reworked their sites as a result of the Michigan team notifying them of their problems, but I suspect that many will take time to change their portals," he added.

Against this backdrop, Sweeney says that companies that use online banking services should install behavioural analysis security technology to add an intelligent layer of technology to interpret their data and protect their systems against e-banking cybercrime - and any other form of unknown security threats.

"We've said for some time that behavioural analysis is an intelligent safety net for companies looking to protect themselves against unknown - as well as known - security threats.

"This is an example of that type of threat, which can easily escape the attentions of conventional security software. This research clearly confirms the vulnerability of any enterprise that chooses not to monitor the behaviour of their systems and users for unusual activity," he said.



# COMMERCIAL CRIME

## International

### Subscription Order Form

**I would like to subscribe to Commercial Crime International.  
I understand that I may cancel my subscription at any time and receive a refund of the unexpired portion.**

**£95/\$160**       **£75/\$120 (ICC members)**

**Name** \_\_\_\_\_

**Job Title** \_\_\_\_\_ **Organization** \_\_\_\_\_

**Address** \_\_\_\_\_

**Postcode** \_\_\_\_\_ **Country** \_\_\_\_\_

**Tel No** \_\_\_\_\_ **Fax No** \_\_\_\_\_

**E-mail** \_\_\_\_\_

**Nature of Business** \_\_\_\_\_

**Please charge my Mastercard/Visa/Delta Card**

**Card number** \_\_\_\_\_

**Expiry Date** \_\_\_\_\_

**Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**I enclose a cheque payable to Commercial Crime Services (drawn on a UK bank)**

**Please invoice me/my organisation at the address above**

*Please return the completed form to: Commercial Crime Services  
Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK.  
Telephone Hotline +44 (0) 20 7423 6960*

*Commercial Crime International* is 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  
E-mail: ajholder@gmail.com  
Website: www.icc-ccs.org  
Editor: Andy Holder  
Editorial Tel: +44 (0) 1903 877081

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 2008. All rights reserved.