Alerting business to threats from fraud and corporate crime

COMMERCIAL CRIME International

March 2014

Shipowners face new dangers from spurious oil fraud claims

Concern is growing that a ruse to extort money from ship owners, which until now has been confined to West Africa, may have been taken up by fraudsters in other countries.

The ICC International Maritime Bureau (IMB) says its members need to be aware of the tactics being used, which bear the hallmarks of organised crime, as they can have significant implications to the operational capability of the vessels targeted, and may cost the owner/operator a great deal of money and time to refute. The IMB will do whatever it can to assist members who find themselves in difficulties as a result of such an approach, and is able to offer a variety of advice based on its knowledge of previous cases.

CCI reported the West African extortion attempts in March and April 2011, and also explained how the IMB was able to assist the member whose vessels were targeted on those occasions. The events were costly to resolve and caused a great deal of disruption at the time to the member's operations in the region. Similar cases have continued to be reported.

Legal redress

The West African cases mostly involved the victim of an oil fraud seeking to get their lost money back though the courts by targeting the owner/manager of the vessel alleged to have carried the cargo of oil they believed they had bought.

Despite the fact that it was often fairly easy to show that the vessel named never carried the oil, was not at the load port on the date specified in the trade documents (which were invariably fake), and in one case had even been scrapped the year before, the courts were persuaded to take the claims seriously, not least because of the historic issues of oil fraud in the region (see page 7).

As a result, whilst the victim may have initially only lost a few thousands of dollars paying out advance fees and for the (fake) documents he believed gave him title to the oil, the shipowner incurred costs that could run into the 100's of thousands of dollars from having their vessel arrested and off charter for period of time while the matter was resolved.

The shipowner also risked having to defend claims of complicity in smuggling and fraud in court (see page 2), which if proven carry large fines in West Africa, and often suffered adverse publicity in the local media as well as interrogation by national investigation agencies.

Moreover, the task of refuting the claims was complicated by the fact that the documents relating to the alleged oil shipment presented to support them were often very good fakes that passed initial inspection and could only be shown to be false after detailed analysis by specialist document checkers such as the IMB.

New approach

The new case, reported recently to the IMB, takes the problem of spurious claims to a new level, however, and presents all shipowners with a much bigger danger to their operations because it could seemingly be replicated anywhere in the world and especially in jurisdictions where the legal system is less robust.

It also gives the victims/fraudsters the flexibility to wait for the alleged offending vessel to arrive in the chosen country before lodging a claim locally. This could mean the vessel is trapped before it can act. It could also make shipowners hesitant to send their vessels into a country where such a risk is perceived, with the potential to severely disrupt their ability to carry out a voyage and/or incur a charter party default.

Continued on page 2/

In This Issue of CCI

Spurious claims cont/

The case involves a vessel that trades regularly into the Arabian Gulf. It is the first time a claim for the full value (over $50 million) of a cargo of oil has been lodged. The claimant alleges that the cargo of oil it owns, that was loaded onto the vessel in Russia, was never delivered to the designated discharge port in the Arabian Gulf. And it seemingly has the documents to prove it. As a result, a local court in the region has now been persuaded to issue an arrest warrant against the vessel named in the claim. The owner faces a dilemma. Knowing of the arrest warrant, he is reluctant to risk taking the vessel into the jurisdiction where it was issued for fear that the vessel will be arrested and he will become embroiled in litigation to get it released. But at the same time, he is obliged to enter the region under the terms of the vessel's current charter party. If he defaults, he will incur financial penalties. Further complicating the issue, the documents presented to the court to get the arrest warrant look authentic and confirm the vessel did load the oil at the Russian port although the vessel had not called into the alleged load port.

The IMB, which is helping the shipowner and has had sight of the documents, warns other shipowners to be on their guard and notes that this new variation to the West African fraud it has dealt with previously is characterised by the production of extremely credible documents that would be sufficient to provoke a similar response if presented to many other courts. "This may be the first of many other similar claims to be lodged against shipowners around the world if organised crime is involved and it is important that the maritime industry is made aware of the danger," the IMB said. "If we can build a picture of what is happening it may be possible to identify the perpetrators or at least inform shipowners what the watch out for. To this end, it would be helpful if any other member with suspicions or experience of this new type of crime contact us, so that we may be able to coordinate a suitable response."

Bank contradicts oil fraud prosecutors

A bank has refuted claims by Nigeria's EFCC in the case of an oil marketer accused of oil subsidy fraud. The EFCC is prosecuting Rowaye Jubril and his company Brila Energy Ltd in a Lagos court, claiming that he did not import 13,500 tonnes of premium motor spirit for which he was given a N963.7 million ($5.9m) subsidy. However, in court the Spring Bank Plc insisted that Jubril followed due process in the importation of the fuel for which he was given the subsidy.

A representative of the bank told the court that “The complete process of importation was complied with. As far as the bank is concerned, we have no evidence to show that the product was sourced locally. We (the bank) believe that it was imported." Under cross examination, however, he acknowledged that the bank was not physically present to witness the transaction and had relied on the documents presented for the transaction which, he said, was the standard practice.

Outlining the circumstances, he said the bank financed the transaction by granting Jubril a credit facility of $11.9 million, and appointed General Marine and Oil Services Ltd to supervise the importation and discharge of the product on its behalf. But he admitted that the company later wrote to Spring Bank admitting that it did not supervise the discharge of the product at Obat Tank Farm in Lagos. And he also admitted there were discrepancies in the shipping documents submitted by General Marine Oil Services Ltd and their corresponding bank, Union Bank UK, on the transaction.

“The document submitted by Union Bank UK showed that the mother vessel was MT Overseas Lima while our appointed agent said it was MT Gabros," he said in court. “We wrote to the supplier of the product, Napa Petroleum, who confirmed via an electronic mail that it imported the product for Brila using MT Overseas Lima,” he said, noting that all the required documents were submitted to the Petroleum Products Pricing and Regulatory Agency (PPPRA) for the processing of the subsidy payment. He added that the subsidy was credited into Brila’s account with Spring Bank and that the loan had been repaid with interest.

Fraudulent loans lead bank losses

INDIAN public sector banks cumulatively lost Rs.22,743 crore due to cheating and forgery in the last three years, a recent RTI (right to information) request reported in the press has revealed. (1 crore = 10 million rupees = US$160,000)

The report said that Indian Overseas Bank was the worst hit with a loss of Rs 3,200 cores - more than it made in profit - while State Bank of India (SBI) lost Rs.2,712 crore, and that between April 2010 and September 2013, the number of bank fraud cases showed a slight decrease yearly but that the amount of money lost has been increasing year on year. This is despite the Reserve Bank of India (RBI) issuing detailed instructions to banks in July 2012 containing details on how they should examine fraud cases and report them to CBI, the police and the special fraud investigation office (SFIO).

According to reports based on the documents examined, more than 6000 employees of different banks

Sim fraud warning to Indian banks

IN India, the government has asked a mobile service provider and a private bank to pay Rs 12 lakh and Rs 6 lakh respectively to the victim of an online fraud, after finding that both Vodafone and ICICI Bank were lax and had let the customer down. It is hoped this landmark case will change banks' outlook on how they deal with client data.

The case arose when a fraudster obtained a SIM card from Vodafone with a forged passport photocopy. He used the SIM to siphon over Rs19 lakh from the ICICI Bank account of a company called Sango Consultants, run by a man and his wife. The fraudster gained access to bank data, blocked the wife's mobile and approached a Vodafone franchisee for a new SIM card. Using the SIM card, he acquired details and passwords to transfer money from the account. The one-time password issued by the bank as a safety measure was sent to the fraudster's mobile number. Vodafone replaced the SIM card but initially calls were diverted to another number.

are under suspicion of involvement in these cases. They are not just lower or mid-level employees, but in some cases, CMDs and directors of different banks. At the same time, analysis of cases investigated by the CBI revealed that bankers sometimes exceed their discretionary powers and give loans to unscrupulous borrowers on fake or forged documents.

While loans on forged documents were found to be the main component of the banks' losses, there are other reasons too: the increase in alternate channels including internet banking and even the use of ATMs, which has reduced the human interface between the customer and banks has led to an increase in fraudulent activities.

No complacency as UK fraud falls

AN analysis of fraud trends during 2013 by CIFAS, the UK's Fraud Prevention Service, has revealed a mix of apparently good and equally alarming news about fraud.

According to the CIFAS analysis, overall fraud levels decreased in 2013 by 11% from the levels recorded in 2012 – the first year-on-year drop since 2010 – but fraud remains at a much higher rate than in pre- (2008) recessionary times. The decrease, however, is proof of the positive preventative impact of counter fraud measures such as data sharing. While there are some alarming fluctuations within the fraud figures, the most notable findings are:

- Over 221,000 confirmed frauds were identified during 2013.
- Identity crimes – where fraudsters use a person's identity data to impersonate them (identity fraud) or hijack an individual's existing account (facility takeover fraud) – accounted for over 60% of all frauds.
- Over 125,000 individual instances of an identifiable person becoming victim to fraud.
- Some startling variations from 2012 have occurred in terms of the products targeted by fraudsters: frauds against mail order and bank accounts have experienced sizeable decreases, while loan and plastic card (e.g. store and credit cards) accounts have seen notable surges. Plastic cards are now the product most commonly targeted by fraudsters (up by 24% from the levels of 2012 and accounting for 30% of all confirmed fraud in 2013).

The 11% decrease in fraud levels recorded during 2013 is good news for all those who participate in the collective effort to prevent fraud, said CIFAS. It demonstrates how increased investments in fraud prevention systems such as data sharing have meant that participating organisations have lost less to fraud. However, the figures also show that fraudsters have turned their attention to targets that they deem to be more vulnerable: namely those who are not making best use of existing systems: meaning that public and private money is effectively being left unguarded for criminals to take.

And, while identity crimes such as identity fraud or the hijacking of an existing account (where both rely on the criminal having the right data to circumvent security and identity processes) fell during 2013, they still represented over 60% of all fraud recorded during 2013, with well over 125,000 individual victims of fraud identified. This is the third year that identity crimes have accounted for such a huge chunk of fraud in the UK, said CIFAS. Sadly, it also confirms that still not enough is being done by individuals and organisations. Consumers have the right to demand that organisations handle their data securely, and increase their anti fraud efforts and stop fraud before someone financially loses out.

2013 was also notable in terms of the changes in annual patterns of fraud said CIFAS. While bank accounts are still one of the most commonly targeted products, levels of fraud have reduced when compared with 2012. Similarly, mail order account providers have reaped the benefit of enhancing their security procedures by seeing much less fraud in 2013. Fraud targeting credit or store cards (up 24%) and loan accounts (up 55% – this included secured, unsecured and payday loans) both increased: demonstrating that beneath the apparent overall decrease, it is far from being all good news as fraudsters ramped up their efforts against different targets.

$36m investment club fraud

A sixth man was found guilty of involvement in a $36 million investment fraud scheme last month. Christopher Jackson, 46, was the last of six defendants convicted for their participation in the scheme known as Diversified Management Consultants, or DMC.

According to court documents, between 2003 and 2009, DMC purported to help people invest money in real estate development and save their homes from foreclosure. In reality, authorities said, DMC was an investment fraud scheme that defrauded at least 180 people out of approximately $36.9 million.

DMC was an umbrella for the various defendants' investment clubs, the court was told. They induced people to invest their ordinary savings, tax-deferred retirement savings and proceeds of cash-out residential loan refinancing. They told investors that their money would be used to purchase property and buildings for a real estate venture. Instead, the victims' money went to pay other investors' bogus returns on investment and to pay for the defendants' personal expenses.

Jackson was know as a "closer" among the DMC participants. His investment club, known as Genesis Innovations, recruited approximately 80 investors and took in more than $10 million. Many of Jackson's victims invested all of their retirement savings with him based on his promise of a high interest rate and very little risk. Out of the $10 million, Jackson invested no more than $2.5 million in developing real estate, authorities said.

Generosity costs fraudster her liberty

A female finance manager who successfully embezzled nearly £600,000 from her employer and was only caught when an offer to help a work colleague backfired, has been jailed for three years.

When the workmate was refused a pay rise, the court heard that Sharon Porter, 41, took it on herself to fund her colleague's salary increase personally by paying her out of the money she was stealing from her firm Escape Recruitment Ltd. Unfortunately for her, however, the workmate went to bosses to find out why she was being paid the same salary from the company's account, but getting the increase in cash from Porter.

A subsequent investigation found that Porter had set up a monthly standing order for herself, and had been siphoning off huge amounts of money in the period from 2006 to 2011, which she used to pay off credit card debts. She had also given herself a salary increase unbeknown to her employer. And yet the company only reluctantly called in the police when it became clear that Porter would be unable to repay the money. She was dismissed but went on the get a top job with another company who was told nothing about the earlier fraud.

Investment charade

A man has been jailed for seven years after defrauding 300 investors through a trading scam in a prosecution brought by the FCA in the UK, who described it as one of the most elaborate scams ever seen. Some £17.5m is owed to investors, of which the FCA has recovered £5.4m, leaving estimated losses of £12.2m.

Benjamin Wilson ran the scam under the name SureInvestment, an unauthorised firm based in Dorset which claimed to carry out futures trading for the benefit of investors. Between 2003 and 2010, Wilson took £21.8m in deposits from investors, many of whom were his personal friends. He claimed to be trading the money and generating monthly returns of up to 9%. But in fact the money was spent on extravagant business and lifestyle expenses.

The FCA said that the whole of SureInvestment was a charade. Almost nothing about the company was as it appeared. Wilson used his charm and the trappings of apparent success to lure investors. He claimed to be a genius. He forged numerous documents, including company accounts. The FCA said the huge amount of effort that went into creating a legitimate façade for the company was much greater than in most cases of this kind.

Three arrested in Dutch Ponzi scheme

THREE people were arrested in the Netherlands in connection with a €43m investment fraud last month. The two men and one woman are suspected of conning hundreds of people out of their cash by promising high returns on property and mortgage investments.

Searches were conducted at homes in Amstelveen and Soest and business premises in Amersfoort, Baarn, Amsterdam and Amstelveen after an investigation began following a complaint to the Dutch financial regulator.

Investigators also sequestered around 70 bank accounts used for the scam, where it is alleged that investors were told their money was being placed in German property. The rest of the money is thought to have been spent privately by the suspects and used to make interest payments to other investors in a pyramid/Ponzi-style operation.

Beware boiler rooms selling diamonds

FRAUDSTERS operating from boiler rooms are targeting the vulnerable in a new form of investment scam involving diamonds, according to recent press reports. And because diamonds are an unregulated form of investment, diamond brokers do not have to be registered with the regulator, making it harder to check their bona-fides.

In the UK, reports allege that people are being cold called and offered an opportunity to realise high returns by investing in diamonds. But the gems may be marked up to 17 times their actual value. The elderly are popular targets and the reports allege that one victim with Alzheimer's handed over £90,000 in three months after being called by a company selling diamond investments. On each occasion he was told to keep it secret.

Apparently, in 2013, around 250 reports of diamond fraud were made to Action Fraud with more than 90 being sent on to forces by the UK's National Fraud Intelligence Bureau (NFIB) for investigation. Reports suggest several live investigations into diamond frauds are ongoing.

Police said that diamonds were just another commodity being sold by boiler rooms that use the same mix of technical jargon, impressive job titles and mock websites to appear credible to naive investors.

'Complicated' hedge fund fraudster guilty

RANDAL Kent Hansen, 65, was found guilty of fraud in South Dakota recently in connection with his role in a multi-million dollar fraud that was described in court as very complicated.

Hansen was indicted in May 2013 for conspiracy to commit wire fraud and mail fraud The case involved the investigation of a hedge fund known as RAHFCO Funds Limited Partnership and RAHFCO Growth Fund. As president of the fund, Randy Hansen collected money from over a hundred investors that totalled over $20 million dollars. Investors were told that only a small portion of the money was supposed to be used to make trades on the futures market for the S&P 500, that the rest was securely invested in government securities, and that they could withdraw funds.

The fund operated from 2007 until April 2011 when one of Hansen's co-conspirators turned himself into authorities. The investigation revealed that the fund was operating in a Ponzi-like fashion with new investor money being used to pay off older investors seeking to withdraw funds. Ultimately, investor losses exceeded $10 million.

New UK sentencing for corporate fraud

THE Sentencing Council for England and Wales recently published a new sentencing guideline for corporate fraud, which can be used as a reference for judges as they begin to use deferred prosecution agreements (DPAs) for the first time. The guideline applies to organisations convicted of fraud, money laundering, and bribery, on or after 1 October 2014. The UK's use of DPAs was set to begin last month. The corporate fraud guideline is part of a broader look at sentencing guidelines for individuals convicted of fraud, with guidelines applying to individuals expected to be released this summer.

The Sentencing Council said because DPAs are not criminal convictions, its guidelines would not apply in the same manner. Rather, the council hopes judges can look to the new guideline to help them arrive at appropriate financial penalties to be included in DPAs. Those penalties should be similar to a fine imposed after a guilty plea, the council said.

"The guideline aims to ensure consistent and appropriate sentencing for these crimes, removing any profit made from the offence, and having a real economic impact on the offending organisation, including its shareholders," the Sentencing Council said in a statement accompanying the guideline.

Indentity thief jailed

AN American man was recently jailed for six years after pleading guilty to stealing the identities of terminally ill patients and using that information to defraud insurance companies.

Government prosecutors claimed that Joseph Caramadre and his partner defrauded insurance companies up to $46 million in the 15-year scheme.

Managers arrested in kickback probe

NEWS reports last month said that managers at Foxconn had been arrested on charges that they demanded kickbacks from iPhone component makers.

The reports said that around a dozen managers have been taken into custody. Allegedly they include Deng Zhixian, director general for Foxconn's committee of surface mount technology, and retired senior vice president Liao Wancheng, who was the alleged mastermind behind the purported scheme.

Foxconn officials have said since that they are working to make sure such illegal behaviour does not happen again.

Crime may thrive after Turkish crackdown on police

Law enforcement and the judiciary are under threat in Turkey amid political wrangling and corruption probes. Thousands of police officers have been reassigned, the deputy of a financial crime unit has been dismissed, and the independence of the judiciary has been brought into question. Crime, smuggling and corruption are all likely to increase unless the political situation improves. ***Paul Cochrane*** *reports.*

Turkey, like much of the Middle East, is experiencing political turbulence and uncertainty. In early 2013, massive demonstrations erupted in Istanbul, ostensibly over the redevelopment of Taksim Gezi Park into a shopping mall, but expanded into protests against the government of the ruling Justice & Development (AKP) Party, which has been headed by Prime Minister Recep Erdoğan for 11 years.

Following the Istanbul protests, the political temperature rose further in December, 2013, when police financial crime units arrested some 50 people for graft, including the sons of three cabinet ministers, the mayor of Istanbul's Fatih district, a construction mogul, the general manager of partly state-owned Halkbank, and Iranian-Turkish businessman Reza Zerrab.

All those arrested had links to the ruling party. Erdoğan claimed the crackdown was a "dirty operation" to smear his administration, and dismissed members of the police force, the head of Istanbul police, and the chiefs of the financial crimes, anti-smuggling, cybercrime and organised crime units. "Nearly 5,000 police officers of different ranks were assigned different duties, and police chiefs of big cities were replaced," said a Turkish criminologist who wanted anonymity.

Critics accuse Erdoğan of taking advantage of legitimate investigations to install pro-AKP supporters in the police and judiciary. "The rule of law is under threat, and the separation of powers is under threat as the government wants to keep legislative power, especially, under its control," added the source.

In January however, the Speaker of Parliament Cemil Çiçek claimed there was no independent judicial review of Turkish legislation, while the government passed a law restructuring the Supreme Board of Judges and Prosecutors (HSYK) in February. "Everything is on ice right now due to the current (fraud) controversy. Erdoğan is decimating the judiciary, and there is a lot of collateral damage, with many careers and businesses up-ended if they are suspected of being an ally [of the US-based opposition movement led by cleric Fethullah Gülen]. It's all about power and who runs the AKP and subsequently Turkey," said Atilla Yesilada, an Istanbul-based analyst at Global Source Partners Inc.

Three elections are to take place over the next two years, starting with local elections in March, but the outcome for judicial independence does not look optimistic given the tensions on both sides of the political divide. "If the Gülen movement wins, many innocents will be put in prison because of corruption accusations, and if the AKP wins, the corruption cases will be dropped," added Yesilada.

Crime on the rise

With an undermined police force and judiciary, crime looks set to increase. "It is difficult to estimate crime and the sources of new crime that we will come across in Turkey, but definitely it will increase, as will white collar crime and corruption," said the criminologist.

Of particular concern is that the deputy of the Financial Crimes Investigation Board (Mali Suçları Araştırma Kurulu or MASAK) was replaced in December. "Normally people can inform MASAK of financial crimes but as the root of these financial corruption probes goes back to information provided to MASAK, which is supposed to be independent, this is now under threat with the government interfering in bureaucratic operations. Confidence within the police and public confidence in the police is decreasing," said the criminologist.

Smuggling concerns

Such enforcement concerns could play into the hands of smugglers, with Turkey a major crossroads between Europe and Asia in the narcotics and human trafficking trades, as well as counterfeit goods, while the country has porous borders with conflict-riven Syria, a turbulent Iraq, and Iran, which remains under heavy international sanctions. Indeed, the Office of the US Trade Representative (USTR) in its 2013 annual review placed Turkey on its 'watch list' for ineffective and inadequate protection of intellectual property rights. "US rights holders continue to raise serious concerns regarding the export from, and trans-shipment through, Turkey of counterfeit and pirated products," the report stated.

Turkey has also regressed in Transparency International's Corruption Perceptions Index 2013, dropping from 49th position in 2012, to 53rd out of 177 jurisdictions. "The commercial crime that is most frequently investigated and therefore that occurs most frequently is bribery, followed by bid rigging, malversation and malfeasance," said Ms Olgu Kama, a Partner at law firm ELIG in Istanbul.

To address such concerns, in July 2012, Turkey criminalised private-

Police chief outlines Nigerian oil subsidy fraud problem

NIGERIA's Commissioner of Police Special Fraud Unit (SFU), Tunde Ogunsakin, said recently that the unit succeeded in recovering N6.5 billion ($40m) from suspected fraudsters last year. He said the money was recovered from a total of 1,142 cases including fuel subsidy, bank frauds and other fraud-related incidents, which were reported to the unit from in 2013. He noted that a substantial part of the recovered money was from fuel subsidy fraud cases.

Ogunsakin said the unit tackled a variety of subsidy fraud cases. The cases of criminal diversion of subsidy funds against 11 major oil marketers were referred to the unit by the federal government for investigation and subsequent prosecution. He noted that from the findings and investigations conducted so far, substantial evidence of criminal infractions was adduced against some of the oil marketers.

"Our challenge is that most cases related to oil subsidy are crimes committed outside the shores of Nigeria, hence, it requires international contact and investigation to conclude most of the cases," he said. But worthy of mention was the fraud allegedly carried out by the management of companies like Stonebridge Oil Ltd, Eurafric Oil and Coastal Services Ltd, Geacan Energy Ltd, Capital Oil and Gas Industry Ltd and Gulf bank.

Stonebridge Oil Limited received the sum of N1,784,715,258.14 as subsidy under the guise that it discharged 20,187,353.00 litres of petrol on July 29, 2011, which it claimed to have imported into the country via the vessels MT Brave Ex, MT Starling Ex and MT Pyxis Delta. But investigation by the unit revealed that the Pyxis Delta did not carry petrol on the date claimed and never discharged any product into MT Brave through MT Starling as claimed by the marketer. Also, investigations revealed that MT Brave was in Port Harcourt waters during the period and was never anywhere near offshore Cotonou where the marketer alleged the ship to ship transfer took place.

On another occasion, Eurafric Oil and Coastal Service received the sum of N1, 306,170,995.88 as subsidy money from the federal government under the guise that it discharged 17,836,556 litres of petrol on December 21, 2011, which it claimed to have imported via the vessels MT Dani Ex and MT Hellenic Blue. However, investigations by the unit revealed that MT Dani was nowhere near offshore Lome and did not have any ship to ship transfer from MT Hellenic Blue on the alleged date.

Ogunshakin said the most intriguing of all the cases so far is that of now defunct Gulf bank, where about N15 billion was fraudulently diverted by some senior management staff at the bank. He said: "Our experience on bank fraud cases reveals the insider factor. 80% of frauds are conceived and perpetrated by top bank executives in collaboration with outsiders.

Turkish crime crackdown - cont/

to-private bribery and broadened the scope of both domestic and foreign bribery offences in its legislation to abide by the OECD's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. However, the OECD's Phase 3 anti-bribery review of Turkey, which is to occur this month, may be affected by the ongoing corruption scandal. "The implications of these allegations may be reflected in the report, as Turkey is currently undergoing Phase 3 examinations," added Kama.

Corporates take care

Away from the current fraud scandal, Kama said that multinational companies (MNCs) are "extremely careful" about their actions in Turkey, primarily due to the need to be compliant with multinational treaties such as the UK Bribery Act.

Assuming the independence of the judiciary and law enforcement survives the current political crisis, Kama said a key reform that would help legitimate businesses work in Turkey is protection for whistleblowers. And companies can take steps themselves. "MNCs merely using global corporate compliance policy is not enough. Adaptation to the local context should be made. To that end, we advise companies to retain local counsels who are familiar with the Turkish culture," she argued. Notably, any whistleblower protection system lacking anonymity "may not work in Turkey, simply because other employees may regard the employee who blew the whistle as a snitch." As a result, setting up anonymous telephone hotlines for whistleblowers "would be good idea," said Kama.

However, whistleblowing and journalists investigating commercial crime could be thwarted by government interference in the media. Some 100 journalists have been fired or reassigned since December, while Erdoğan admitted in January that he had made a call to a media outlet to change headlines.

Furthermore, a draft internet bill has been proposed that critics say will censor journalism and social media. "This bill is all the more disturbing for seeming to be an integral component of a series of draconian statements and initiatives by the authorities in recent months," said Reporters Without Borders in a January statement, while ranking Turkey 154 out of 179 jurisdictions in its Press Freedom Index 2013.

Bank Secrecy Act used against companies

TWO companies that sell bulk orders of fake hair products recently agreed to pay $15 million to resolve claims they could have been conduits for dirty money, after an unusual case that was based on an anti-money laundering law used more often to target big banks.

The US Bank Secrecy Act requires banks to monitor transactions for questionable activities and report any suspicious activity to federal authorities. However, in a sign of how widely US anti-money-laundering efforts have spread, federal prosecutors in New Jersey filed a case in January that used the same law to penalise two wholesale companies for allegedly allowing customers to structure payments in a way to avoid triggering federal reporting requirements.

Shake-N-Go Fashion and Model Model Hair Fashion, which distribute hair extensions, wigs and other hair accessories and share the same owners, allowed customers to deposit payments directly into the companies' bank accounts, prosecutors said. They also allowed customers to break up the payments so that each deposit was under $10,000, even if the total order was larger, they alleged. Businesses that receive more than $10,000 in cash in one or related transactions are required to report that information to the IRS. Some of the companies' employees knew about the structured deposits, it was also alleged, but did not correct the problem and failed to file appropriate reports.

In a civil settlement, the two companies did not dispute the allegations. In order to resolve the matter they agreed to forfeit $15 million and improve their anti-money laundering compliance programs. Afterwards, New Jersey US Attorney Paul Fishman said in a statement, "It doesn't matter what your business is; you are required to follow the financial reporting requirements of the United States."

M/l monitoring not effective say execs

WHILE banks claim their focus on money laundering is at an all-time high, a new report has revealed that a third of executives think their transaction monitoring systems are neither efficient nor effective.

According to the survey carried out by KPMG, 88% of 317 AML and compliance professionals across 48 countries quizzed by the firm said that money laundering is now back at the top of their firms' agenda, up from 62% in 2011.

Yet satisfaction with transaction monitoring systems is apparently poor, as one in three respondents said their tech is neither efficient nor effective. Worse still, only just over half said their systems are able to provide the complete picture by monitoring transactions across businesses and jurisdictions.

And despite concerns about oversight, control and data confidentiality, outsourcing and offshoring are becoming more common. To date, 31% of respondents have outsourced and 46% have off-shored some of their anti-money laundering functions, the report found.

Moreover, while KPMG says that accurate cost forecasting is vital for informed decision making, it remains a key area of weakness due in part to the number of regulatory change announcements and the speed in which they are expected to be implemented.

The suggestion emerging from the data is that senior management is likely to continue to underestimate anti-money laundering expenditure, unless lessons are learnt from past mistakes. And more than three quarters of respondents said that the pace and impact of regulatory changes are significant challenges to their operations.

Financial industry needs to get on top of m/l says FINRA

FINRA, the US Financial Industry Regulatory Authority, said recently that money laundering should be a top concern for the financial industry this year. The agency said it plans to focus on anti-money laundering tactics with institutional business in 2014.

FINRA also identified a misconception among some executing brokers that the Customer Identification Program (CIP) requirements - which require banks to form a reasonable belief that they know the true identity of each customer - do not apply to delivery versus payment/receipt versus payment (DVP/RVP) customers. FINRA said that the CIP requirements do apply and that the executing broker is responsible for implementing the requirements for these customers, who were identified as responsible for a new trend in money laundering in the past year.

“Depending on the nature of the account and the risks associated with it, firms may conduct additional due diligence on this type of account [DVP/RVP] and obtain information on the individuals with authority or control over the account,” FINRA said. It also recommended that all firms develop a risk-based anti-money laundering program to address the risk of money laundering specific to their firm. “Firms that have high-risk customer bases should tailor their programs around the specific risks of those customers, including the types of customers, where its customers are located, and the types of services they offer to those customers,” it added.

Securities firm fined for failure to monitor/prevent potential m/l

AN Omaha-based securities clearing firm will pay a $1 million civil fine for not complying with securities industry requirements to prevent money laundering and other "extensive" failures, FINRA said recently.

Wall Street's industry-funded watchdog said that COR Clearing LLC, formerly Legent Clearing LLC, did not have an adequate program in place for monitoring potential money laundering by clients of the brokerage firms for which it clears securities and provides other functions. COR, as part of the settlement, must also retain an independent consultant to conduct a comprehensive review of its policies, systems and employee training.

Clearing firms act as middlemen between securities brokerages and exchanges. They typically handle back-office tasks for brokerages, including order processing, settling trades, and record keeping. FINRA rules require clearing firms and brokerages to have policies and procedures in place to comply with a federal law aimed at detecting and curbing money laundering.

But the anti-money laundering program at COR was lacking, especially given the clearing firm's business model, FINRA said. Many of the 86 securities brokerages that cleared through COR buy and sell thinly-traded, low-priced securities, it added. Low-priced securities are often subject to efforts to falsely inflate trading volume and share prices, a securities fraud violation that is a precursor to money-laundering. What's more, many of the brokerages had been already disciplined by FINRA for their own violations of anti-money laundering rules, FINRA confirmed.

FINRA identified the multiple violations between 2009 to 2013, it said, adding that COR's anti-money laundering surveillance program suffered a "near-complete collapse" for several months in 2012, during which it failed to conduct any reviews to identify and investigate suspicious activity.

The $1 million fine underscores the responsibility that clearing firms have to monitor cash flow of their brokerage firm clients.

Australian police crack global m/l ring

AUSTRALIAN police said late January that they had cracked a major global money-laundering ring with operatives in more than 20 countries and funds syphoned off to groups reported to include Hezbollah.

The Australian Crime Commission (ACC) said more than Aus$580 million ($512 million) of drugs and assets had been seized, including Aus$26 million in cash, in a year-long sting operation codenamed Eligo targeting the offshore laundering of funds generated by outlaw motorcycle gangs, people-smugglers and others.

According to the ACC, the operation had disrupted 18 serious and organised crime groups and singled out 128 individuals of interest in more than 20 countries. Eligo saw 105 people arrested on 190 separate charges and resulted in the closure of three major clandestine methamphetamine labs and Australia's largest-ever urban hydroponic cannabis hothouse in Sydney last November.

Legitimate international cash wiring services were a major focus of the operation, with the government's anti-laundering agency AUSTRAC saying they had been identified as at "high risk of being exploited by serious and organised crime groups". Allegedly, criminals targeted foreign nationals and students in Australia awaiting remittances from overseas, hijacking the transaction by depositing dirty money to the payee and then taking the cash wired from offshore. At least one of the exchange houses used in the Middle East and Asia delivered a cut from every dollar it laundered to Lebanon's Shiite movement and Hezbollah.

Organised crime is estimated to cost Australia Aus$10-15 billion per year by the ACC, with drugs, money-laundering, fraud, firearms and high-tech cyber offences the major issues. Profits from transnational organised crime were estimated at $870 billion in 2009 - the latest available data - representing about 1.5% of global GDP at the time.

Bahrain m/l ring

TWELVE men have been accused of being part of a money laundering ring that illegally transferred SR400 million ($106.6 million) overseas. The suspects are all Indians working in one of Bahrain's leading money exchange companies, including six branch managers, a press report alleged, adding that the men would transfer up to SR1 million a day to the UAE.

It is claimed they sent the cash using forged documents purporting to be from 80 commercially registered companies with the help of an employee at the Commercial Registration Bureau. Almost half of the 80 companies used to send the money abroad were fake and the rest had done business with the exchange company before, but had no idea the funds were being sent in their name. It is also alleged the money was brought into Bahrain in bags via the King Fahad Causeway, but not known where it came from. It was then taken directly to the exchange company so it could be laundered and transferred abroad.

Ivory Coast battles cybercrime

IVORY Coast's rise to become Africa's cyber criminal capital has prompted the government to take measures to crack down on cybercrime. But it's an uphill battle in a country where cyber criminals are treated like celebrities and the best have songs written about their exploits. The police say these 'celebrities' conned more than $15 million out of people all over the world in the past two years, and that's just the money they have managed to trace.

The average age of a cyber criminal in Ivory Coast is now between 16 and 17, and they each make around $13,000 a month by taking taking advantage of Ivory Coast's cheap and fast internet - cyber cafe's cost less than $1 for four hours online.

In response, Abidjan now has its own 'Web mayor', who teaches young people how they can legitimately make money online, for instance through blogging or web design. And two years ago the government set up a dedicated taskforce to fight cybercrime, the Plateforme de Lutte Contre la Cybercriminalite (PLCC). It is made up of the country's law and security forces and is the first of its kind in Africa. It has a new forensic laboratory, which works on providing digital evidence. "First of all we identify, without any doubt, who was behind the screen when the victim was scammed," the head of the PLCC told reporters recently. "Secondly, we link that person to the crime with digital evidence." Last year alone the PLCC made nearly 100 arrests, naming and shaming the convicted criminals on the government website, while the cyber crime law, passed last May, has introduced prison sentences of up to 20 years.

The data gleaned investigating these cases has also given the PLCC a better idea about how the Ivorian cyber criminal works and who they target. They now know the "love" (romance advance fee fraud) method is by far the most common way of conning people out of their money, and more than half their cases come from complainants in France, followed by Ivory Coast, then Belgium and Canada.

Data breaches lead to fraud

ONE in three data breach victims in 2013 later experienced fraud, according to a survey released by Javelin Research last month. That's up from one in four in 2012, according to the company, which polled 5,634 US adults over three weeks last October about financial fraud incidents. "The correlation between a fraud victim and a breach victim gets stronger every year," said Al Pascual, who co-authored the report. He added the theft of personal records is less likely to result in fraud these days because cyber criminals are more focussed on payment card details, of which there is a dearth for sale online after a spate of data breaches. He said these are easier to monetize.

Kazak online bank thieves arrested

CYBER thieves were arrested for hacking Kazakhstan's online banking system and stealing over 300 million tenge ($1.9 million) last month.

The thieves mainly targeted the accountants of different companies who transacted online.

To withdraw the money stolen from the accounts, the hackers forged IDs and used frontmen to open bank accounts in various banks in Kazakhstan. Then they made money transfers to these accounts using hacked passwords and cashed them out.

Emails not from financial company

IN the UK, Aberdeen Asset Management - which manages £193 billion worth of institutional and private investors' money - is warning people to look out for emails from fraudsters purporting to be from the company.

Its alert warns that it has become aware of an individual offering "false lease agreements" through email using the name and old logo of Aberdeen Asset Management. The individual is also using a profile on Linkedin, which suggests he is an Aberdeen Asset Management member of staff to lend credibility to his approach. But Aberdeen does not offer such agreements and will never contact the public in this way.

Data skimmed at pumps

REPORTS say that thirteen men were arrested in January for using Bluetooth-enabled data skimmers planted on petrol station pumps to steal more than $2 million from petrol station customers throughout Texas, Georgia, and South Carolina. The Bluetooth-enabled skimmers were invisible to people who paid at the pumps, and the thieves were able to download the skimmed data without physically removing the devices.

Payment system hacking predicted

EXPERTS are predicting that a string of recent retail data breaches could be the prelude to a major wave of hacks against US payments systems that antivirus software and account monitoring tools cannot deter.

The experts stressed that companies should install systems that spot and block intrusions swiftly, before massive volumes of personal data can be stolen.

Experiment highlights power of social media employment scams

FOLLOWING on from the recent story on employment scams in the January issue (page 12), recent reports say that a US government agency has been duped in a similar way. Fortunately though, this was an experimental scam created by security experts. But it provides a valuable lesson about the dangers of social media - and man's weakness for a pretty face.

The "scam" involved Emily Williams, a fictitious attractive woman with a credible online identity (including a real photo that was allowed by a real woman), posing as a new hire at the targeted agency. Within 15 hours, the fake Emily had 55 LinkedIn connections and 60 for Facebook with the targeted agency's employees and contractors. Job offers came, along with offers from men at the agency to assist her with her new job.

Around Christmas time the security experts placed a link on Emily's social media profiles linking to a Christmas card site they created. Visits to this site apparently led to a chain of events that culminated in the security team stealing highly sensitive information from the agency. Partner companies with the agency were also compromised. Having got what they wanted within a week, the penetration scam was then extended to credit card companies, banks and healthcare organisations with very similar results.

The security experts noted that an authentic attacker could have easily compromised any of the partner companies, then attacked the agency through them, making the assault more difficult to detect. They pointed out that the scam began from the ground up, inflating Emily's social network till it enabled the attack team to suck in security personnel and executives. But most of the people who assisted Emily were men. Interestingly, a similar experiment using a fake male profile had no success.

'Insider' allegation prompts new investigation into bank card processing company

ALLEGATIONS of insider fraud are being investigated by Indian police in the state of Karnataka nearly a year after fraudsters broke into two payment processing companies (the other was in the US) that handled the prepaid cards for two Middle Eastern banks, Bank Muscat and National Bank of Ras Al-Khaimah in the UAE, and stole $45 million. The fraudsters were later caught by authorities in the US and Europe and most of the money was recovered.

One of the payment processing companies hacked into was enStage Software, situated in Halasuru, which managed payments processing for Muscat Bank of the Sultanate of Oman. The bank, which lost $39 million to the fraudsters, has since complained that someone in enStage Software may have been involved in hacking its data centre - that was maintained by the provider - prompting the new investigation into the possible link between the international ring of hackers and staff of enStage.

The modus operandi of the fraudsters involved targeting the prepaid cards issued by the banks. They broke into the software of the payment processing companies of the two banks and increased the available balance and withdrawal limits on their cards. The fraudsters then prepared 12 fraudulent prepaid travel cards from 8 to 10 countries, which were used to withdraw millions of dollars in numerous cities within a few hours.

Commenting on the investigation, a police spokesperson said that an inquiry had found that no one could have transferred the money unless they had ATM cards or e-banking facilities. Therefore, without the involvement of someone at enStage, it would have been highly impossible to steal the money.

SpyEye inventor pleads guilty

THE primary developer and distributor of SpyEye malware, which is designed to steal online banking credentials and credit card information, pleaded guilty to conspiracy to commit wire and bank fraud last month. Russian national Aleksandr Andreevich Panin, also known as "Gribodemon" and "Harderman," will be sentenced in April.

The US Justice Department claims that SpyEye has infected more than 1.4 million computers in the United States, and was the dominant malware toolkit used from 2009 to 2011. The financial services industry says more than 10,000 bank accounts were compromised by SpyEye infections in 2013. However, although it is still used by some cyber criminals, the effectiveness of the malware has now been limited after software makers added its detection to their malware removal programs.

SpyEye malware is designed to automate the theft of confidential personal and financial information, including online banking credentials, credit card information, usernames, passwords, PINs and other personally identifying information. It secretly infects victims' computers, enabling cyber criminals to remotely control the infected computers through command-and-control servers. Once infected, cyber criminals remotely access the computers and steal personal and financial information through a variety of techniques.

Beware stolen information in emails

AS data breaches at major firms become more common, security experts have highlighted the use of this stolen information in a growing number of spear phishing attacks, and are warning recipients to beware of being caught out by emails that are more believable because they contain, say, a correct name and address. To avoid getting speared and fooled into revealing even more vital data such as a credit card number, for example, they point out that vigilance is the key to staying safe.

Don't let the presence of familiar personal information in a message lull you into a false sense of security. Just because a message includes a home address doesn't mean it's valid. In fact, legitimate mail from a bank or vendor generally shouldn't include this information, unless it's a notification of shipping to that address. Similarly, the presence of a home phone number in a message means nothing, and a legitimate vendor would never send your password in email. An email message containing your national insurance number (or the last four digits) should be scrutinised carefully too, as once again a legitimate sender wouldn't expose it in an email.

There are some fundamental rules that apply even to email messages that look legitimate because they already have some of your personal information. Readers should already be aware of them but it doesn't hurt to recap:

- Don't click links in email purportedly from your bank. If the message warns of an account problem that needs your attention, launch your browser and go directly to the bank's site.
- If you're at all suspicious of a link in an email message, hover the mouse over the link, and check the destination URL. A link URL that doesn't match the link's stated destination is a big red flag.
- Pay attention to the URL in the browser's address bar. Many phishing sites don't even try to use believable URLs. Others use warped versions of the true URL, perhaps paypla.com or ebay.something.com. If the URL looks wrong, leave the site and enter the real URL by hand.
- Don't register your details in vendor websites. It may save time in the future but it puts your data at the mercy of any hacker who breaches the vendor's security. And there have been plenty of such incidents recently.
- Use a password management tool. Such apps store all your login credentials and will automatically fill in your credentials at the correct website, but not at a fraudulent copy of the site.
- Install a security suite that includes effective phishing protection, such as Kaspersky or Bitdefender.

Always bear in mind that data breaches give the bad guys ammunition for phishing attacks, and phishing attacks in turn can cause new data breaches.

It's a vicious cycle.

Cybersecurity a priority says FINRA

FINRA, the US Financial Industry Regulatory Authority, said recently that the hacking of sensitive customer information is a top threat facing the financial industry in 2014. In its “2014 Regulatory and Examination Priorities” letter to financial firms FINRA highlighted increased cybersecurity, along with anti-money laundering programs, additional disclosure practices, and several other activities, as the primary defences to protect the financial industry in 2014.

Cybersecurity was identified as a top priority because of ongoing cybersecurity issues across the financial services industry, such as the recent Target security breach which compromised 40 million customers credit and debit card information. “Many of the nation’s largest financial institutions were targeted for disruptions through a range of different types of attacks,” which appear to be increasing, said the letter. Additionally, FINRA said it is concerned about the integrity of financial firms’ infrastructure and the safety and security of sensitive customer data that is vulnerable to hackers.

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: andyholder2@gmail.com

ISSN 1012-2710