COMMERCIAL CRIME
International
September 2015

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Alerting business to the threat from fraud and corporate crime, and its prevention

Warning as invoice fraud using spoofed email grows

Invoice fraud is growing and hitting already hard-pressed companies, the ICC Financial Investigation Bureau (FIB) said last month. The problem is now worldwide and all business organisations need to be on their guard and understand what to look out for and what to do, it added.

The FIB is particularly concerned about the growth in invoice fraud involving spoofed email addresses, whilst also acknowledging that many other forms of similarly problematic vendor fraud exist. In such cases, it is usual for hackers to intercept email traffic between a buyer and seller, and to then 'enter' the conversation pretending to be the seller and asking that invoice payments be directed to a different bank account they control. A number of plausible reasons may be given for the request and, as a result, the change is often authorised without more than a cursory check, especially in a mature business relationship. The diversion only comes to light when the (real) seller queries non-payment of its invoice after the due date, by which time the money has long since been moved out of reach.

It is important that companies realise the contact email address the fraudsters substitute may only include a minor amendment, giving the impression it is correct, said the FIB. It may thus look almost identical to the previous (and accepted) email address, but may read .org instead of .com or .co.uk for example. Such tiny changes are not hard to detect if account staff are aware of the potential problem and know what to look out for. But in many cases the FIB has investigated it is clear that this simple fraud prevention step is not being taken.

Geographical shift

Previous warnings in CCI about this particular type of invoice fraud found that most requests from hackers asked that money be sent to bank accounts located in the Far East, and this in itself could be deemed a warning sign, especially if there was no obvious reason why a company would bank in the region; say if it were an SME based elsewhere. However, there is evidence this may be changing and that fraudsters are setting up bank accounts in multiple locations to disguise their actions. In a recent report to the FIB, for example, a US-based cheese seller whose client's email was hacked, described how the Taiwanese buyer was led to believe that it wanted a payment of over USD$90,000 sent to a Scottish Bank and then a Polish Bank, to where the funds were ultimately sent. The US exporter said that the Taiwanese government didn't have much interest in the case and insufficient authority to investigate it. The FBI was asked to look into what was alleged to be an elaborate scheme involving spoofed emails and forged documents. The US exporter said the matter had been reported to the Polish bank that received the funds, but clearly it still needed more assistance.

Self protection

As national authorities and banks continue to appear reluctant to get involved in such crimes, the FIB urges companies to take their own proactive steps to detect and prevent them wherever possible. Among the basic measures it recommends are informing and educating staff about the problem, highlighting what they should be looking out for, and providing a mechanism through which to report any suspicions. Within this, it suggests:

- ✦ know your supplier and their invoice/payment patterns to help identify exceptions and anomalies.
- ✦ be vigilant for any change of email ID and verify that the change is legitimate.
- ✦ set up single points of contact within companies that regular payments are made to.

continued on page 3/

In This Issue of CCI

ICC INTERNATIONAL CHAMBER OF COMMERCE BRIEFING

The world business organization

Updating members on ICC's ongoing activities to support international business.

ICC/Chinese strengthen business ties

As part of objectives to enhance the geographical reach and influence of ICC as the world business organization, Chairman Terry McGraw led an ICC delegation to Beijing in late July with a view to strengthening its ties with leading Chinese businesses and policymakers. Terry met with Chinese Vice-Premier Wang Yang, who called on ICC to play "an active role in China's reform" and "to create more opportunities for foreign cooperation with Chinese companies."

Post-2015 Sustainable Development Agenda

July saw an important step forward in the United Nations' post-2015 development agenda, with the culmination of negotiations to overhaul the international community's development financing framework. The final agreement - known as the Addis Ababa Action Agenda - provides a foundation to support the implementation of the UN Sustainable Development Goals (SDGs), which will be formally adopted by world leaders at a major international summit in New York later this month.

Trade policy

ICC's representations in the lead up to the Addis conference resulted in a strong focus on international trade within the final development financing agreement. But it's vital that these good words galvanise real world action. Writing in the Financial Times last month, ICC Secretary General John Danilovich called on governments to use the Addis Agenda as a springboard to deliver on three longstanding commitments to: (i) implement the WTO's Trade Facilitation Agreement; (ii) enhance the availability of trade finance; and (iii) conclude the Doha Round of world trade talks before the end of the year.

ICC welcomed the announcement at the end of July that an agreement has been struck to revise the WTO Information Technology Agreement - a longstanding priority for ICC. Estimates suggest that the new deal to remove tariffs on ICT products - from smartphones through to copiers - could boost global GDP by some $190 billion.

India Economic Convention

ICC co-hosting the 2015 India Economic Convention in New Delhi on 17 September. The Convention, which will be chaired by a number of senior Indian Ministers, will review the progress of reforms spearheaded by Prime Minister Narendra Modi to make India a leading centre for global business.

Trade Fraud

World Bank reports fraud in Tunisian trade practices

COMPANIES and individuals connected to former Tunisian president Zine El Abidine Ben Ali avoided paying $1.2 billion in import duties between 2002 and 2009, the World Bank said in a recent report. Ben Ali fled to Saudi Arabia with family members and a reported $50 million in gold after a bloodless coup in 2011.

The World Bank study on Tunisian trade practices identified tariff gaps by comparing data on exports from its trade partners with the value of imports reported by the country's Customs authority. The declared value of imports by Ben Ali-connected firms was found to be 18% higher than average firms, with declared quantities of imports 21% higher, but reported unit prices were found to be on average 4.8% lower. For imported goods subject to high tariffs, the reported prices were even lower at 8.1%. The Bank says this type of underreporting allowed regime-connected companies and individuals to evade $217 million in taxes in 2009 alone.

The World Bank's country manager for Tunisia said the avoidance of import duties by business associates of Ben Ali undermined competition and allowed wealthier, politically connected elites to amass greater profits by paying lower import duties.

Fake shipping agency cheques

HAITI's National Port Authority (APN) has reported finding that 143 cheques worth $10 million issued by the shipping agency Seabord Marine of Haiti SA to the order of APN between 2008 and 2011 were falsified and misappropriated.

Following a two-year investigation, the Unit for Combating Corruption (ULCC) found that to conduct the fraud, the fraudsters created a company called "APNI/Import-Export". With the help of accomplices, the 143 cheques, written manually, included a space after the beneficiary "APN" which allowed them to add "I-Import-Export." The cheques then became payable to "APNI-Import-Export", which held an account at the Banque Nationale de Credit under the name of Ulrick Duplessy.

Based on its findings, ULCC recommended that Duplessy and Joseph Bernard Jean, the Accounting Controller for Seaboard Marine, and several others be prosecuted for theft, forgery and use of forgery and money laundering for their part in the fraud. But seven months later, press reports say that no action against them has yet been initiated.

FMC fines UASC and NVOCCs to protect international shipping

THE US Federal Maritime Commission (FMC) recently reported reaching a compromise agreement with Dubai-based and Qatar-owned United Arab Shipping Company (UASC) for alleged violations of the US Shipping Act and FMC's regulations.

UASC, along with six non-vessel-operating common carriers (NVOCCs) had been charged with US$1,227,500 in civil penalties. Although all seven shipping lines settled and agreed to penalties, none admitted to any violations.

The FMC charged UASC with unlawfully rebating to its NVOCC customer, Falcon Maritime and Aviation Inc, a portion of the applicable service contract rate in the form of an administrative fee not identified in the service contract, and for which no services were provided.

UASC also allegedly provided transportation not in accordance with the rates and charges in its published tariff. Under the terms of the compromise, UASC paid US $537,500 to FMC.

FMC, which is responsible for protecting the American shipping public from entities who may be in breach of the Shipping Act, said "The compromise agreements demonstrate how serious we are about protecting the international shipping marketplace from fraud and threats to cargo security, and in our commitment to shield the many lawful participants in international trade from commercial deception and other unlawful trading practices."

UK plans corruption plea deals

THE UK could soon adopt US-style plea deals for corporate corruption, according to recent reports. The Serious Fraud Office (SFO) has said it expects to sign its first deals by the end of the year under a new scheme in which a company would admit wrongdoing for economic crimes including fraud and bribery, but avoid drawn-out and potentially damaging corporate criminal cases.

The deals, known as deferred prosecution agreements (DPAs), became available to prosecutors last year. They were brought in by the Ministry of Justice. Any agreement would have to be approved by a judge at a public hearing and could result in substantial fines, the overhauling of a company's procedures and an acceptance of its failures. But it would mean that any criminal charges were put on hold. Agreeing a DPA to avoid a criminal prosecution would also lessen a firm's reputational damage, and allow it to continue bidding for government contracts.

DPAs will be used only where the "public interest is not best served" by mounting a criminal prosecution, according to the SFO, which investigates the most difficult fraud cases. Individual corrupt workers could still be taken to court and the companies would be told to help in bringing cases against them, it added.

Email invoice fraud - continued from page 1

✦ always confirm a change of bank account request with the company, preferably by means different to that by which it was received. If you simply return an email, for example, it will simply go back to the fraudster. Better to phone or email using the address held on file.
✦ once a payment has been made, immediately check with the recipient they have received it, again using the information about them held on file.

In many cases, when these frauds are detected it is still possible to prevent the funds from being dissipated if the recipient bank is made aware of the scam and is prepared to hold the funds until legal action is taken to freeze them. This is key to frustrating the fraudsters. It has been the FIB experience that increasingly banks are prepared to assist the victims of fraud if they are given comprehensive and timely information. The FIB and IMB can assist in such cases.

Lukoil m/l charges

ROMANIAN authorities recently charged Russian oil producer Lukoil with complicity in money laundering worth 1.77 billion euros ($1.95 billion). Prosecutors at the Court of Appeal in Ploiesti, where Lukoil's refinery is based, alleged that Romanian and Russian company managers misued the company's credit and capital. Their statement said from 2011 to 2014 "the suspects knowingly used company goods and credit granted to the company to benefit other companies in which they had a direct or indirect interest." In July, prosecutors froze Lukoil's assets and bank accounts worth about 2 billion euros ($2.22 billion).

Corruption

Brazil's Operation Car Wash may sink political donation corruption

Brazil's Federal Police's Operation Car Wash has led to arrests of top businessmen, politicians and lobbyists. The success of these cases will depend on whether political donations can be legally regarded as bribes. **Mauricio Savarese** *reports from Brasília.*

It all began at a simple petrol station in Brasília, two miles away from the country's Congress. On 17 March 2014, Federal Police entered a currency exchange booth at the forecourt to investigate its small money trade business. They bumped into a network of political and corporate corruption that has cost state oil giant Petrobras at least $2 billion. Overpriced financial operations, consulting jobs that never existed and kickbacks masquerading as legal donations have been used to divert funds from Brazil's most iconic company.

The leader of the investigations is a young judge who seems inspired by Italy's anti-mafia Clean Hands Operation, which reduced that country's old political system to rubble. Judge Sergio Moro, 43, is a highly-skilled specialist on white collar crime based in Curitiba, Brazil's 8th most populated city. That is a shock in itself in a nation where all the scandals that hit the news come from major cities like São Paulo and Rio de Janeiro. But there is more that separates him from his colleagues in Brazil. Firstly, technicalities did not stop his investigation, unlike in many previous cases – in Brazil, like Italy, judges have a hand in pushing criminal investigations forward, as well as adjudicating on cases. Secondly, this tenacious expert learned from the Italian case that political parties do use apparently legal donations to launder money.

This is now the crux of his case, with recent high profile arrests leading to a likely referral to Brazil's Supreme Court. It will now consider whether political donations can be reviewed as bribes – a critically important question for clean government and business in Brazil.

Investigations should take two more years to complete - much to the regret of a government that is being hamstrung by the drip-feed of bad news from the inquiry.

The name Operation Car Wash is actually a reference to the US TV series Breaking Bad. That is because the petrol station in the programme was actually a front for a lucrative black-market operation.

In real Brazilian life, it was the station's owner, Carlos Habib Chater, who led investigators to money dealer Alberto Youssef, a key figure in the scandal. Youssef's scheme was fed by Paulo Roberto Costa, Petrobras' former director, and several executives from Brazil's multinational construction firms. Costa and other state-oil executives used Youssef's money changing networks to channel funds to politicians - some in opposition parties, who could have started congressional inquiries into the scheme long ago, should they have been honest.

Successful strategy

Moro's strategy was clear from the start. Priority number one was to arrest as many of those involved for as long as possible, so they were more easily convinced to sign plea bargain deals - up to six months in many cases.

Although many judicial experts consider that to be an illegal approach, Moro's decisions always stood without legal challenge. By striking agreements, he avoided deep investigations into political figures, ensuring the case - until now - remained in Curitiba courts, avoiding early referrals to the Supreme Court, whose members are appointed by politicians, and who may have blocked progress.

That method has allowed him to untangle a key part of Brazil's institutional corruption since the year 2000. Since the beginning of 2014, he has persuaded five top businessmen to strike plea bargain deals and confess that they paid bribes to politicians through donations to their parties. It was information that was unlikely to have been raised in a Brazilian court. According to the country's electoral law, political parties do not have to reveal their sponsors - only candidates have to. "There is evidence of some of the kickbacks being passed on as electoral donations registered by the [ruling] Worker's Party, which would have been made by their request," Judge Moro has written in a ruling.

The grounds of that decision led to the arrests of Petrobras executive Renato Duque and the ruling party's treasurer, João Vaccari Neto. And that has made Moro's investigations highly political. If his 'donations as kickbacks' theory is accepted by the Supreme Court, that may threaten the political future of President Dilma Rousseff, who was re-elected less than a year ago. She has not been directly implicated, but suffers pressure to resign from hundreds of thousands of demonstrating pot-bangers. If her presidential campaign is found to have received bribes, her candidacy could be invalidated by Brazil's Superior Electoral Court.

Prosecutor Deltan Dallagnol, who has worked with Moro, thinks his donations-kickback theory holds water and should be regarded as a crime. "There were 24 electoral donations to the Worker's Party over 18 months paid by companies of one of these corrupted groups. And it is clear that those were discounted from the kickbacks to be

paid to a Petrobras executive," he told Commercial Crime International. "They just masqueraded the nature of the transaction. That is typical money laundering." But when it comes to the Supreme Court agreeing… "Let's wait to see if they accept it," Dallagnol warned.

That said, defence lawyer Alberto Toron, who has worked in big scandals over the last two decades, argues Moro is not treating all suspects equally. "These arrests are arbitrary, unnecessary. He has let some of these businessmen go, the Supreme Court has let some others." He believes the judge from Curitiba has gathered a lot of popularity because of the investigations, but that does not mean that the Supreme Court will embrace his theory. "There needs to be more than plea bargain signatories to state that case to our Justices," he said.

Economic fallout

Moro has already said that the investigations will take another two years, which surely will have an effect on Brazil's sluggish economy, dissuading constructors and Petrobras who fear his inquiries from making investments. Indeed, at least 23 big companies have been stopped from signing deals for the next 10 years with the state oil company because of the scandal. But it is undeniable that the probes are going to have a positive effect in tempering Brazilian corruption: more than 50 politicians are now under federal investigation, including former ministers, Congressmen, and the speaker of the lower house of Congress Eduardo Cunha. He was in August accused by federal authorities of using evangelical churches to launder money.

More than a dozen businessmen have been arrested since last May, including the CEO of multinational constructor Odebrecht. Another big constructor that was a key player in the Petrobras scheme, Camargo Correa, struck a leniency deal with Brazilian authorities to give back about $30 million in bribes. That is the corporate version of the plea bargains that some of their executives are signing with Judge Moro.

Looking ahead, Brazil's future may be brighter given its law enforcement and judicial institutions have proved to be robust in the fight against corruption - there is no cover-up nowadays. But there is a huge cloud of doubt on the country's political make-up for the next elections. Nobody seems to want friends in politics for now: who will take advantage of that in the ballot box remains to be seen.

FATA: how gold is used to launder money

INTERNATIONAL bodies are studying how and why gold remains a means to launder money.

The Financial Action Task Force, an international body that sets standards for anti-money laundering and combating terrorist financing, recently released a report with more than a dozen case studies on how gold can be used to launder money.

Gold "is an extremely attractive vehicle" for laundering money, the report said. It provides a mechanism for illicit funds to be made anonymous, transformable and easily exchangeable. Those are attractive selling points to money launderers as regulators increasingly target money flows in the formal system.

"Internationally enforced anti-money laundering measures are influencing a shift in criminal behaviours towards methodologies with lower law enforcement visibility, which makes gold very attractive," the report said. Among the vulnerabilities attracting money launderers to gold, the report added, are the fact that the market for scrap gold is cash intensive, it can be traded anonymously, it's a form of global currency, it provides reliable returns and it's easily smuggled from place to place.

According to a new book: "Trade Based Money Laundering : The Next Frontier in International Money Laundering Enforcement," gold's "unique characteristics" also make it popular across the trade-based money laundering landscape. "Gold is used in all three stages of money laundering; placement, layering and integration," the book's author says. "It is attractive to both criminal and terrorist organisations - there is nothing else like it out there."

Bank closes to settle US m/l probes

BANAMEX USA, a unit of Citigroup Inc that served customers doing business in Mexico and the US, has reportedly agreed to shut down and pay $140 million in penalties to settle state and federal money-laundering probes. Banamex is an arm of Banco Nacional de Mexico, Mexico's second-largest bank, which is owned by Citigroup.

Citigroup has since confirmed that it would "wind down" Banamex USA. Its offices in Houston and San Antonio also will be closed. The operation had $1 billion in assets, $700 million in deposits and 394 employees as of March 31, 2015.

Explaining the move, a spokesperson for the regulator said that Banamex agreed three years ago to correct numerous weaknesses in its anti-money laundering program. "But it failed to do so and moreover, had committed more violations of regulators' anti-money laundering mandates since," he said.

Euro Forex linked to alleged $2bn organised crime fraud

ALLEGATIONS of a huge international fraud perpetrated by a company called Euro Forex Investment Ltd (EFIL) - aka FX Capital International Corporation or FXCAP - were recently made by a Chinese website and independently supported by an alleged investor victim. Other firms said to be linked to the fraud were named on the website as PFS Pacific Finance Services Ltd, London Capital NZ Ltd and Asia Finance Corporation Ltd. It is claimed that Euro Forex was a scam set up in the UK that was administered from New Zealand (Wellington), and which sold foreign exchange products, mainly into China.

The investor told a New Zealand website that the scheme claimed to have more than 50,000 investors around the world from more than 100 countries. So far, the confirmed victims have exceeded 3,000 people from nearly 10 countries including the UK, US, Australia, Canada, Japan, Singapore and China. In China there are victims from nearly 100 different cities including Hong Kong, Taiwan and Macau.

The investor claimed potentially as many as 10,000 people have been "defrauded" of US$2 billion, with a "professional criminal group" ultimately behind the scheme that takes advantage of complex international law and the constraints of legal jurisdictions in different countries. Investors allegedly believed Euro Forex was helping them do online forex trading, but now believe most of their money has found its way to Singapore and "some key criminals."

In February 2013, Britain's Financial Conduct Authority (FCA) said Euro Forex Investment Ltd was not authorised to carry on regulated activities in the UK, but may be targeting UK consumers. However, Euro Forex said its "New Zealand license" enabled it to offer "investment expertise to global clients." But it never had any New Zealand licence.

Unique trading approach

The investor told reporters the earliest known date Euro Forex Investment Ltd started promoting itself in China was June 2012. It claimed to have 13 years history of forex trading and managing money for investors. Euro Forex used the reputations of the UK and NZ to make itself look trustworthy. It claimed to have trading offices in Paris, Switzerland and Greece and more than 200 employees.

According to the investor, the company claimed to use a "unique" trading approach that enabled it to deliver monthly returns of 9% to 16% with very low risk. It offered silver accounts paying 9%, golden accounts paying 12%, and premium accounts paying 16%. Each investor had to stump up at least US$100,000.

Early warning

Over time the name on brochures "quietly changed" to EFIL-Euro Forex Investment Ltd. Then on July 20, 2013, all accounts were frozen and trading halted. The explanation given was that this was due to the implementation of NZ's Anti-Money Laundering and Countering Financing of Terrorism Act, which took effect on June 30, 2013.

The company apparently told investors that accounts would be frozen for three months to clear out "bad" accounts. Investors were allegedly told if they opened a hedging account, trading would continue during this three month period. Investors were also allegedly told they would be able to withdraw their money from October 18, 2013. Just prior to that, on October 13, Euro Forex became FXCAP, with its website redirecting users to www.fxci.com.

Euro Forex/FXCAP also allegedly offered payments cards issued by British company Prepaid Financial Services Ltd, known as PFS, with documents that came with the card allegedly coming from Pacific Finance Services Corporation Ltd, known as PFS NZ, which was to be contacted if there were any problems. These cards apparently didn't meet investors' expectations, turning out to be prepaid cards not connected to their trading accounts and with no money on them, plus a load limit of US$2,500 per year.

Another update on the website, dated September 1, 2014, allegedly said management had decided to stop clients from trading their accounts from this date. Clients would be allowed weekly withdrawals of between 3% and 5% of their current account balance from January 2015, the update said, and new clients would then be able to open accounts. An apology was made for "inconvenience" caused during 2014. In reality, it is alleged that no investor has been able to withdraw any money for two years. Police in China, Singapore and the UK are investigating.

Fake l/c fraud

INDIAN police recently arrested a 37-year-old law graduate accused of allegedly duping a Korea-based bank of Rs5.52 crore by presenting a forged document to get a loan. Last December, it is alleged, the man gave a fake letter of credit to an Indian branch of Shinhan Bank. It was purportedly issued by UCO Bank in Kolkata and assured the Korean bank that it would repay the loan if the man were to default. The fraud came to light in June when he failed to repay the loan and the Korean bank contacted the bank in Kolkata to invoke the letter of credit. Police said the fraudster had received help from an insider at the Korean bank who verified the authenticity of the document.

Pension liberation fraud rising

PENSIONS fraudsters are stepping up their efforts in wake of the new UK pension freedoms that came into force in April, the City of London Police said recently. The CoL Police said the total amount lost to 'pensions liberation fraud' - a type of fraud where scammers convince investors they can get better returns from riskier, often fictional investments - skyrocketed to £4.7 million in May 2015, more than treble the £1.4 million lost the month before.

The May fraud total is the largest single month since May 2013 - which is as far back as the released figures go. The average amount lost per reported case over the 25-month period recorded by police was £6,979 - but the May 2015 average was more than £60,000.

The fraudsters are fully aware that many pensioners now have ready access to large capital sums and are potentially a soft target for the many and various scams that currently exist, said one pensions consultant quoted. These usually start with a cold call, a text message, or an email offering a free review with the prospect of substantially increasing the value of their savings by, for example, taking advantage of the "amazing" investment opportunities that they can provide, he added. The results are invariably negative for the saver, with some of the victims losing the whole of their savings as a consequence.

Investment in company a fraud

US citizen Terina K Carney, also known as Terina Humphrey, 49, has admitted defrauding numerous investors in her fraud scheme between December 2012 and January 2015. Although not registered as an investment adviser Carney, the owner of Riverside Lease LLC, told investors their money would be used as an advance payment on behalf of a third-party business. It would allow the business to continue operating while it secured long-term funding from a bank.

Carney promised to obtain a high rate of return for investors, from 10% to 30% on top of their original investment. Investors were told that, once the business received its long-term funding from the bank, they would receive their original investment plus interest from those funds. Investors were also told that Riverside Lease held their money and there was little to no risk of the investor losing their principal investment because the third-party business never had direct access to their money.

After reviewing bank account information, agents determined that once the investor's money was received, it was never used to provide short-term financing for any other business.

US-based exec led $1.5bn Ponzi targeting Japan

THE US recently indicted the chief executive of a Las Vegas investment company - MRI International Inc - and two of his former Asia-based executives alleging they headed a $1.5 billion Ponzi-style fraud scheme.

The indictment alleges that Edwin Fujinaga of Las Vegas, and Junzo Suzuki and Paul Suzuki, both of Tokyo, victimised thousands of unsuspecting Japanese investors in their scheme, which operated for at least four years until it was exposed in April 3013. Prosecutors said the three men told thousands of overseas victims that their investments would be safely held and managed by an independent, third-party escrow agent in Nevada.

Investments were primarily sold through the company service center in Tokyo, promising high returns and low risk through a technique dubbed "factoring." The company promised high returns buying accounts receivable from medical providers at a discount, then attempting to recover more than the discounted amount from the debtor. The government alleges the Ponzi scheme defrauded victims by using money from new investors to pay early-stage investors and persuade others to take part.

US-based Brazilian took $12m

A Brazilian national based in the US was recently charged with defrauding investors out of more than $12 million.

Court documents allege that Daniel Fernandes Rojo Filho owns a company called DFRF Enterprises LLC, which is incorporated in Massachusetts and Florida. Beginning in 2014, Filho and others acting at his direction allegedly began offering people the chance to invest in, and therefore become "members" of DFRF. In solicitations posted in internet videos, as well as pitches made in person, Filho is alleged to have falsely told potential investors that DFRF was engaged in a lucrative, international gold-mining business. Additionally, it is alleged that he misrepresented DFRF's ties to a consulting company in Brazil and a private bank in Switzerland.

It is further alleged he told potential investors that their principal investments would be 100% insured against losses by a company based in the United Kingdom and Barbados, all of which was untrue. Relying on Filho's alleged misrepresentations, investors gave Filho and DFRF more than $12 million. Instead of investing the money as promised, however, Filho allegedly took more than $3.5 million himself.

Change of tactics blurs 'boiler room' culpability

Boiler room operations have been under the spotlight recently in the UK, following a police push and successful prosecution of those that rent their offices to such fraudsters (see box). However, following changes in tactics, today's boiler room scams are far more sophisticated and harder to prosecute than when the fraud first emerged in the 1990s. In a recent article, criminal fraud specialist **Gillian Bradbury** *from Byrne and Partners, looked at the changing face of so-called 'boiler rooms'.*

When interest rates are low, as they have been for several years now, investors will always be tempted to seek out novel and innovative ways to make more money from their savings. Bright, driven and ambitious individuals are always on hand to help them to do so, but some of the schemes they propose are not always legitimate.

Boiler room scams have been carried out in a particular fashion for a number of years. Openers make hundreds of initial cold-calls, working through lists of potential targets. They are tasked with getting as much information about the personal and financial circumstances of any person they manage to speak to as possible. Their primary role is always to secure a target's interest through repeated introductory calls, which they usually follow up with professional-looking marketing information.

The high-pressure sales tactics start with the introduction of the 'closer'. This is the name ascribed to the salesperson who takes over the relationship once interest had been established. They build a rapport with a target, often by lying. They sell the idea of the investment and secure the payments, which may initially be deposited in a legitimate account but are soon moved elsewhere out of reach. There is usually evidence that they have (among other things) made false claims and misleading promises that would never be fulfilled; lied to and deceived investors; manipulated investors by, for example, emphasising the brevity of an investment opportunity and/or creating fake background excitement designed to entice; continued to seek payments from investors for as long as the investor had money to spend and had not become suspicious; falsified documents; and made legal threats and/or turned up at investors' houses uninvited, demanding money.

Moving with the times

The 'traditional' boiler room format began to change at the turn of the millennium however, almost entirely driven by the property boom around that time and the subsequent evolution of land banking fraud that followed. Since land is not a regulated investment there was no longer a need for boiler rooms to be based overseas, as was often the case to date, and the fraudsters relocated to smart London addresses, lending an air of authenticity and legitimacy. The new fraud saw land, often in greenbelt zones around the UK, bought and split up into house-sized plots, then sold as land with the potential to obtain planning permission and, therefore, an investment.

What made this type of fraud different from the boiler room operations typical of the early part of the decade were the victims. No longer were the elderly or vulnerable targeted (using re-circulated victim lists) but the fraudsters started to purchase databases from legitimate data collection companies. Investors could be anyone of any age, from any background, who had shown an interest in investing, and particularly an interest in land. These were still fraudulent transactions however: the investment was never going to be worth the price paid for it, nor were the returns promised ever going to materialise.

As the tactics used by salespeople on the phones became less objectionable though, the subjective dishonesty of the individuals involved became a real issue for prosecutors. In many cases, investors themselves were saying that they were willing to take the risk and knew that what they were paying for plots was well in excess of the actual value of the land. As a result, prosecutors found themselves having to go further to show that investors were being duped or deceived. And whilst this change was initially driven by the property boom and with it, the opportunity to invest in land, the fraudsters soon realised the same tactics could be employed successfully with other direct act assets or passion investments, particularly gems, containers and metals. As a result, boiler room fraud has not only boomed in recent years, but detecting it early has become significantly more difficult, as has bringing a successful prosecution against those held responsible.

Game changer

From a legal point of view, everything changed following Operation Pemberton, the UK's first successful prosecution for land banking fraud, which involved proving three things:

1. In order to recoup their investments, investors' land would need to be made the subject of a planning permission application or, at the very least, an application for change of use, which was itself a lengthy, costly process to which the fraudsters had given no thought.

2. Since this was not (on the defendants' admission) a 'collective investment scheme', this process would involve the combined will of all the investors in the subplots, meaning that any individual owner could hold all the others to ransom.
3. If the land itself had any prospect of benefitting from a change of use or planning permission application, it would have been snapped up by a professional developer or land banking company and would therefore not be available to be sold on to individual investors in the way that it had been.
As part of this prosecution, a significant number of employees of the various companies involved were arrested and/or interviewed. Eventually, just four were charged who were all, at one time or another, directors of the companies and of those, only two were successfully convicted.

A police crackdown on the use of City of London addresses for boiler-room investment fraud yielded its first successful prosecution recently when Servcorp UK, a company offering serviced offices and mail forwarding pleaded guilty to seven offences relating to failures to provide client records for inspection, and paid £32,500 in fines and costs.

Police said a "significant number" of Servcorp's clients were under investigation for "fraudulent activity involving the sale of worthless or non-existent commodities like diamonds and wine to vulnerable consumers."

The prosecution formed part of Operation Broadway, a multi-agency push against investment fraudsters operating in and near London's financial districts. Police visited 25 offices in the Square Mile, Canary Wharf and Westminster in March as part of the operation. Each boiler-room operation makes about £1.25m on average, the police said. Boiler-room scammers tend to make upfront cash payments, choose short-term leases, work at unusual hours and opt not to display the company name. The police said they are seeking to work with virtual and serviced office companies and mail-forwarding services to ensure that they are not used for criminal activity.

Operation Cotton, which concluded in June, involved a similar fraud with one key difference: this was a collective investment scheme. The dishonest misrepresentations and promises centred on whether or not the companies involved would really apply for a change of use or planning permission on behalf of investors, and, as such, the extent to which the individuals involved were aware of this.

Prosecution proceedings were brought on the basis of two main charges. Count one alleged a conspiracy to defraud. The second count contained a more technical offence of operating a regulated activity (the collective investment scheme) without authorisation. At trial, the prosecution was unable to prove the more serious fraud count against only two of the defendants.

Similarly, in Operation Wasabi (which also concluded in June) the prosecution of several people alleged to be involved in a conspiracy to defraud investors by selling coloured diamonds achieved mixed results. It was the directors and controlling minds behind the operation who were successfully prosecuted, but those only involved in the day to day selling of the commodities were not proven to be part of the conspiracy. In this case, what was being sold were, on the whole, genuine, certified, coloured diamonds. These commodities were tangible and had a real value. In fact, had the fraudsters been mounting them on rings and selling them in a shop window for the same prices, the principle of caveat emptor (buyer beware) would apply. It was the promise of substantial and/or short-term returns that rendered the representations made in this case fraudulent. It appears that the jury did not accept the prosecution's case that the salespeople were aware of this.

Seismic shift

These later frauds represent a seismic shift away from the boiler rooms of the past. Boiler rooms today, although still telesales environments, are often selling tangible commodities, with a value.

There is less need for deception and lies by salespeople, particularly closers. The margins, although still significant, are decreasing. The style of selling is becoming less high-pressure and the lines between honesty and dishonesty, once absent, are starting to be redrawn.

The term 'boiler room' may still be bandied about when describing telesales operations, but it can no longer be automatically thought synonymous with dishonest behaviour by all those involved. Whilst those behind actual frauds are still getting caught, as police and prosecutors continue to 'follow the money', the nature of boiler room operations is changing, and merely being involved in a high-pressure sales environment does, it seems, no longer make you a fraudster.

Fake film investment warning

THE UK's National Fraud Intelligence Bureau says crimes involving fraudulent investments into film productions have been rising steadily this year, with victims across the country being targeted by cold callers selling Unregulated Collective Investment Schemes (UCIS). This is a fund into which several people can contribute, in order that it can then be invested into other assets.

Victims have been offered investments, usually by way of buying shares, in film productions, often said to star famous actors, with various companies that have been cloned or are fraudulent.

The ripple effect of Identity Theft and tools to detect it

We hear about data breaches all the time, but less about what happens to the stolen data afterwards. Each piece of data doesn't just disappear, it gets collected and combined into the tool of choice for today's fraudsters. As **Ryan Wilk**, *Director at NuData Security explains, the problem is so difficult to overcome that society is having to rebuild how it does internet security using behavioural analytics.*

Since 2005, more than 675 million data records have been involved in data breaches in the US alone, according to the Identity Theft Resource Center. These records include incredibly personal data such as a person's Social Security number, name, address, phone number, credit card number, name of local bank branch and so on. Data thieves sell this information to aggregators, who cross-reference and compile full identities – called "fullz" on the data black market. This increases the value and usefulness of the stolen data, which may have been gathered from multiple data breaches.

With this level of information, fraudsters can create new bank accounts or take out loans under an actual person's name. These actions cannot be traced back to the fraudster and can cause problems for the fraud victim for years down the road.

Bad news travels fast

A recent report found that it took just 12 days for the account information of 1,500 "employees" to travel from California to 22 countries and five continents. In that time, it was viewed over 200 times and clicked on over 1,100 times. Fortunately, in this case, these accounts were fake; set up for fake employees and then intentionally "breached" in order to determine the speed at which compromised data travels. This is especially disturbing when you consider it takes an average of 200 days for most corporations to detect a breach has taken place.

The experiment didn't just show how quickly stolen information gets circulated. It determined that the false information was being tested for validity too. Had the fake data been real accounts, fraud attempts would already be underway.

It's the ripple effect. Small data breaches look on the surface to be minor losses of data but they expand out across the digital waters faster than ever before, converging into a wave of personal information so detailed that undoing the damage is next to impossible.

The rise of Account Takeover

What can you do with all of this stolen information? It depends on how much of it is amassed. There is a hierarchy of value on the dark web for stolen data. Stolen credit cards can cost mere cents and are labour-intensive and low return for fraudsters. It takes many attempts for a fraud scheme to work, as cards are tested and cycled through. With so many data breaches last year, credit card numbers flooded the black market, lowering their value.

Fullz sell for $5 a piece, but require a more in-depth and risky scam to be fully utilised. Working user accounts with a payment method attached, an easy-grab scam with lucrative results, go for a mere $27 each and can translate into hundreds to thousands of dollars in stolen money and merchandise.

As a result, account takeover is growing quickly in the fraud world. NuData Security monitors more than 18 billion user interactions across the internet annually, and is seeing 112% year-over-year increases in account takeover attacks.

In account takeovers (ATOs), fraudsters attempt to hijack valid user accounts, instead of creating new accounts with stolen credit cards. ATOs can be automated, including scripted attacks, or can be done with small teams of human operators posing as account holders. Helping out the scammers are middlemen who play a key role in testing the login credentials before they are used again to commit actual fraud.

Based on behavioural analysis, NuData has found that there are, on average, three high-risk logins for every high-risk checkout. The first login is to verify if the account works. The second time is to gain intelligence and the third time is when the fraudster attempts to commit actual fraud. The transaction is no longer the point of focus for fraud – it is the login. This shift creates an imperative to look at the login and account creation - rather than the transaction - in order to stop fraud before it happens.

In a sea of available data, account takeover pirates have their pick of digital credentials. Thus organisations must not only secure their own data, but also be ever vigilant against people using stolen data on their websites as well. By protecting the login pages of your sites, you cut fraudsters off at the source. You stop them from being able to take control of the account in the first place.

Behavioural Analytics

How can you protect login pages from data thieves? This is where behavioural analytics shines. Let's take a look at what user behavioural analytics means. Most merchants look for a username and password match. Some use device ID or check for password resets.

But the newer, more sophisticated criminals are skilled at bypassing these mechanisms.

Full packages of user information - full identities - are prevalent and cheap. If you are not confident that you can separate account testers and fraudsters from legitimate users, then the real question to ask is, "Do I understand my user in enough detail?"

Rather than a simple checklist, behavioural analytics focuses on observed characteristics of who the user is, not just who they tell you they are. User behaviour analytics are aimed at observing and understanding how the user behaves, in an effort to answer bigger questions, such as:

How did the user behave previously when they logged in?
Are they behaving the same now?
When the user is inputting data, is it similar to how they've interacted on the same device before, or is it completely different?
Is their behaviour repeated?

Repeated behaviour can tell a lot. If the behaviour is the same every time they visit, perhaps it's a good user, acting the same as always. But if it's the same behaviour that 1,000 users are all repeating, it could indicate that this behaviour is part of a crime ring that could be a distributed, low velocity attack – the kind of attack that exposes you to massive amounts of loss.

Observing user behaviour in detail enables the best chance of beating fraud.

A new era in fraud detection

A recent research note from Gartner indicates that perimeter-focused security isn't keeping malicious actors out when it comes to enterprise security controls.

Merchants are beginning to realise they can no longer rely on basic data validation measures anymore, because when it comes to account takeover, all of the data may be compromised and will be correct regardless of who logs in – legitimate user or imposter.

Instead, the key is to look at the behaviour at login and connect it to checkout. Behavioural analytics digs under the surface of matching usernames and passwords to truly understand user behaviour. These behaviour patterns reveal details that fraudsters can't hide despite their best efforts. As account takeover schemes gain prominence, fraud detection and prevention efforts need to be focused on behaviour. Behavioural analytics provide the intelligence needed to stop fraud before it starts.

Rise in account takeover/email fraud

CYBERCRIMINALS are exploiting publicly available information and weaknesses in corporate email systems to trick small businesses into transferring large sums of money into fraudulent bank accounts, in schemes known as "corporate account takeover" or "business email fraud."

Companies across the globe lost more than $1 billion from October 2013 through June 2015 as a result of such schemes, according to the Federal Bureau of Investigation (FBI). The estimates include complaints from businesses in 64 countries, though most come from US firms. Both "organised crime groups from overseas and domestic-based actors" are typical perpetrators, said the FBI.

Their targets included businesses such as Mega Metals Inc, a 30-year-old scrap processor. In April, the company wired $100,000 to a German vendor to pay for a 40,000-pound container load of titanium shavings. Mega Metals typically buys three to four loads of titanium a week from suppliers in Europe and Asia. But following the recent transaction, the vendor complained that it hadn't received payment. A third party had infected the email account used by a broker working for Mega Metals.

A cybersecurity firm that investigated the loss, said it appeared that malicious software implanted on the broker's computer allowed the crooks to collect passwords that provided access to the broker's email system, and then to falsify wire-transfer instructions for a legitimate purchase. The money has since been moved out several times, so there is no chance of getting it back.

ATM cash theft mastermind extradited

A Turkish man accused of masterminding a string of ATM cash-out attacks dating back to 2008 - and stealing almost $55 million - was recently extradited from Germany to face trial in the United States. Ercan Findikoglu, 33, had been wanted by the US Secret Service for five years. He faces 18 charges, including hacking into the computer networks of at least three US payment processors: Fidelity National Information Services, ElectraCard Service and enStage. Findikoglu allegedly coordinated - and received "a significant portion of revenues" from - an attack campaign predicated on fraudulently increasing the credit limit of prepaid debit cards to make unauthorised withdrawals.

He has also been charged with masterminding a group that made 15,000 such transactions across 18 countries in February 2011, stealing $14 million; 5,700 transactions in December 2012 across 20 countries, stealing $5 million; and February 2013 attacks that resulted in the theft of $40 million.

Theft using hacked accounts thwarted

DIXONS Carphone, a leading European electrical retailer with more than 3,000 stores, has been explaining how iovation helped it to stop an organised crime ring that was targeting iPhone 6's from its online store using hacked accounts.

iovation (iovation.com) protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, device-based authentication and real-time risk evaluation. The company's device reputation database is the world's largest, used to protect 12 million transactions and stop an average of 200,000 fraudulent activities every day. iovation identifies more than 45 specific fraud types, such as identity theft, credit card fraud, account takeover and shipping fraud.

During one of its most recent attempted fraud attacks, Carphone Warehouse explained how the organised fraud ring tried to specifically target iPhone 6s from its online storefronts using hacked accounts and how, by using iovation's device and transactional intelligence, it was able to identify commonalities and patterns between fraudsters and prevent fraudulent purchases from hacked accounts.

iovation's global fraud network contains the behaviour of more than 2.5 billion internet-enabled devices such as laptops, mobile phones and tablets, and 23 million client-reported fraud and abuse reports to determine the fraud risk in a transaction. "iovation helps us correlate locations, devices, accounts and fraud indicators, giving us a powerful weapon to stop large-scale fraud," said the company. "By optimising iovation's fraud prevention policies through identifying devices that have been used to commit fraud with iovation's other clients, and weigh that heavily in our review process, we get insights into fraudulent behaviour that we couldn't get anywhere else."

Carphone customer data stolen

HACKERS have gained access to the personal details of 2.4 million people after getting into Carphone Warehouse's systems, the company admitted last month. The IT systems of one of its UK divisions were found to have been breached after having been subjected to a "sophisticated cyber-attack," it said.

The division operates the the websites OneStopPhoneShop.com, e2save.com and Mobiles.co.uk. The same division also provides services to its recently launched iD mobile network, as well as to TalkTalk Mobile and Talk Mobile, around 480,000 customers of which may also be affected.The hackers may now be in possession of customer names, addresses, date of birth and bank details.

New hacked email property fraud

UK solicitors have become embroiled in a new form of email hacking fraud in which the proceeds of property transactions are sent to accounts under fraudster control.

The hackers intercept emails between buyers/sellers to/from their solicitor, and shortly before completion on the property is due notify them of a change in bank details, usually because the previously specified account is said to be 'being audited'. Believing the email from the solicitor is genuine, and even double checking with their solicitor first in some cases - by email - buyers instruct their banks to make the transfer to the new account. The fraud is only discovered when the solicitor calls to say the money has not arrived in its account, and by the time the matter is reported to the police it has been moved elsewhere out of reach. As well as losing the money - sometime several hundred thousand pounds - buyers face the prospect of the sale falling through and, in some cases, being homeless if the sale of their existing property has completed as planned.

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