# COMMERCIAL CRIME International

October 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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


## IMB sees new trend in bills of lading manipulation

MEMBERS should take note of a new trend in bills of lading (B/L) manipulation in trade finance after several cases were detected by CCS' International Maritime Bureau (IMB) in the last six months.

Whilst B/L forgery is not new, the latest variation sees fraudsters making subtle changes to the back page of the document. These modifications are not easy to spot, making verification difficult if one is not aware of the potential red flags to look out for.

### How previous forgeries worked

According to the IMB, up till recently, forged B/Ls are verified by inspecting them for possible errors on the face or the front page of the document.

Typically, the perpetrators modus operandi would be to tamper with data on the front page of a B/L. This could include; mis-declaring the contents of cargo, mis-representing of the date of a B/L, changing the vessel's name, and sometimes forging a signature on the face of the B/L.

All these the IMB has been able to verify for members and the documents have subsequently found to be false.

### Disturbing new trend

In an alarming new development uncovered by IMB, all the information on the front page of a forged B/L appear exactly as in the genuine document; so checks carried out to verify the B/L become very difficult if one only looks at the front page of the document.

In these cases, the B/Ls are all consigned to order, and the shipments are bulk cargoes.

"What we have found in these cases is that the endorsement on the back of the B/L is false. All the details on the front page of document is absolutely correct, however when we looked at the back page, we found anomalies, and upon checking, confirmed with the shipper that it is not their signature or stamp on the back. It is quite a clever forgery," said an IMB spokesman.

### Common factors of this B/L scam

- All these cases involve carriers and ship owners own B/Ls (not non-vessel operating common carriers or NVOCC B/Ls)
- The shipments were all bound for China, coming usually but not necessarily from South America.
- The exporters are large companies, very reputable, and commodities typically are all bulk cargoes, so far these have included copper and soya.

IMB says it is of great concern that these documents are being produced with the false endorsement purportedly from genuine parties and going through a different banking chain.

"The dangers of this practice are firstly, that it is a fraud against the banking system as the perpetrators don't have rightful ownership of the cargo and the bill of lading does not represent the cargo," the IMB spokesman said.

"Also for the carriers and traders at the discharge port there potentially could be two or more claimants for the cargo, all claiming to be the genuine holders of the negotiable B/L," the IMB spokesman added.

That is a matter that could be resolved ultimately by the shipowners, but the process will take time and cause delays to ships.

IMB says as B/Ls are negotiable documents, the danger is that if someone claims to have a B/L endorsed to them, they have entitlement to that cargo.

The risks are high as the cargoes

*Continued on page 5/*

## In This Issue of CCI

# FIB warns of cases of advanced fee fraud

CCS' Financial Investigation Bureau (FIB) has received a number of reports of cases where following sale purchase agreements, the buyers were asked to pay an advanced fee.

This fee was related to either an advance on the purchase price or payment for shipping or warehousing/storage costs.

In a couple of cases, there had been expressed instructions that if the transaction failed, the advanced payment would be returned to the buyers.

However, after evidence emerged that the shipment would not take place, the buyers have been unable to obtain reimbursement of the monies paid upfront.

FIB said in all these cases, the suppliers had not been properly checked out, they had no track record regarding their performance in the past and no history of having supplied to the victim buyers.

FIB says the purpose of these frauds is not to obtain the purchase price of the cargoes (which are very substantial) but to defraud the buyers of the advanced payment.

The latest case investigated by FIB involves a shipment of aviation jet fuel oil from St. Petersburg, Russia bound for delivery in Rotterdam.

When FIB looked at the documentation generated in this transaction, the information looked to be genuine on the surface. But on close examination, FIB found that unnecessary terminology, clauses and phrases were used.

These irregularities are normally are good indicators that the transaction is suspect and should be enough to raise alarm bells among members.

FIB advises that at the end of the day, it comes down to the principle of Knowing Your Customer and Knowing the Transaction.

"If buyers in these cases had made checks about the reputation and track record of the sellers and whether the cargo existed and was ready to be shipped, they would have avoided the problem before making the advanced payment," FIB said.

In these cases, the legal option for recovering the advanced payment will be through the local courts of the country of the seller, which can in some cases take an inordinate amount of time and with no guarantee that the courts will fully understand the nature of the transactions.

FIB says that this leaves the buyer in a position where they could be unable to recover their losses, in addition to the fact that the amount of money at stake will be disproportionate to the costs of legal action and recovery.

www.icc-ccs.org/icc/fib

# FraudNet holds inaugural meeting in Italy

MEMBERS of ICC FraudNet will discuss a range of issues, including tackling anti-corruption in Italy at its 29 Conference on Cross Border Fraud and Asset Recovery to be held on October 5 in Milan, Italy.

The session *Tackling Anti-Corruption in Italy - An Italian Perspective* will be moderated by Roberta Guaineri from law firm De Castiglione Guaineri e Associati (Italy). Panelists for the session are Professor Nicoletta Parisi from the Italian Anti-Corruption National Authority, Marco Reggiani General Counsel of Snam Group and Nicola Bonucci, Director Legal Affairs OECD.

Another session titled *Private Prosecution in the UK: An Underutilised Weapon for Asset Recovery* will involve deliberations by panelists Kate McMahon from Edmonds Marshall McMahon (England), Ian Casewell from Mintz Group and Kevin Hellard from Grant Thornton. The session will be moderated by Michele Caratsch, from Baldi & Caratsch (Switzerland). Moderator, Glen Glynn from Arthur Cox (Ireland) will lead a topical discussion on *Asset Recovery and Crypto Currencies,* with panelists Stefan Kühn from BDO, James Pomeroy from PwC and Professor Daniele Marazzina from Politecnico di Milano.

Paolo Valerio Barbantini, Deputy DG of Italian Revenue Agency will speak on *Italian Fiscal Investigations: An Overview of Recent Developments in an International Context (OECD Common Reporting Standards, Mutual Assistance in Administrative Matters; Panama Papers).*

ICC FraudNet
COMMERCIAL CRIME SERVICES
est. 2004

Executive Director of ICC FraudNet, Ed Davis from Sequor Law (USA) will chair a session looking at FraudNet's history and major developments ahead.

This is the first time that FraudNet have met in Italy in its 14 year history and a record turnout of more than 100 delegates are expected including representatives from its four Strategic Partners, BDO, Grant Thornton, PwC and Mintz Group.

# One insurance fraud detected every minute says ABI

A total of 562,000 insurance frauds were detected by insurers in the United Kingdom (UK), according to the latest analysis by the Association of British Insurers (ABI), with one insurance fraud detected every minute.

Of the total number, 113,000 were fraudulent claims, while 449,000 were dishonest insurance applications. The number of dishonest insurance claims, at 113,000, were valued at £1.3 billion.

The number was down 8 percent on 2016, while their value rose slightly by 1 percent. The fall in number reflects the industry's collaborative work in detecting and deterring fraud, ABI said.

The number of organised frauds, such as staged motor accidents, fell 22 percent on 2016, with frauds worth £158 million detected.

This reflected the work of the Insurance Fraud Bureau, who are currently investigating a rising number of suspected frauds, and the Insurance Fraud Enforcement Department (IFED). IFED is the specialist police fraud unit investigating insurance fraud, such as staged motor accidents and illegal insurance advisers (so-called ghost brokers). Since its formation in 2006, IFED has secured over 400 court convictions for insurance fraud.

The value of fraudulent detected motor insurance claims, at £775 million, rose by 4 percent on 2016. The number of these frauds, at 67,000, showed a small rise.

Fraudulent property insurance claims fell. The number detected dropped by 11 percent on 2016 to 22,000, with a value of £100 million.

For the first time, the ABI's annual detected fraud figures include data on application fraud - where details such as age, address, or claims history are deliberately misstated.

Insurers detected 449,000 cases of confirmed or suspected application fraud, where people lied or withheld information to try and get cheaper cover.

Motor insurance made up the bulk of dishonest applications, with typical lies including the nature of the applicant's occupation, and driving record, where previous claims and motoring convictions were not disclosed.

ABI gives examples of some of the more interesting insurance scams uncovered including:

1. Pothole claim full of holes

A cyclist claimed £135,000 compensation from a council for injuries he said he sustained when he fell off his cycle after hitting a pothole. However, evidence showed that the accident happened when he fell off on a slippery road at another location. He was jailed for three-and-a-half years.

2. Bodybuilder pumps up his claim

A bodybuilder, who claimed £150,000 for a back injury, was exposed when he was filmed doing a press-up challenge. He was ordered to pay £35,000 in legal costs.

3. Bus cheats busted

The ring leader of a gang who staged a bus crash to try to get £500,000 in insurance pay-outs for fake injuries was jailed and banned from driving for two years. Using a rental car, he staged the crash, following which eight of his fellow fraudsters on the bus claimed for fake injuries to necks and hips.

4. The fraudster of Venice

A student was convicted after attempting to claim £14,000 through six invented claims following a trip to Venice, including the alleged loss of an iPod, laptop and designer watch.

5. Huge car insurance scam sees over 150 convictions

A four- and half-year police investigation into a huge crash for cash staged accident operation in South Wales, which netted the ringleaders £2 million, led to the convictions of 150 people. Selling fake insurance leads to a genuine prison sentence. A man was jailed for three years and eight months for selling fake motor insurance policies to unsuspecting motorists.

6. Not injured, until the ambulance arrives

After staging a road collision, two fraudsters appeared uninjured until the ambulance arrived, when they then started feigning injury. Each received a jail sentence.

* *Source: ABI*

A former direct sales representative of a Hong Kong bank and a former chief financial analysis manager of a financial intermediary have been charged with defrauding the bank of loans of over HK$1.7 million in total for nine applicants and commissions amounting to more than HK$64,000 by fraudulent means.

The former sales representative was responsible for sourcing potential loan customers by operating street booths and distributing promotional items such as handbills. The financial analysis manager was tasked with arranging for potential loan applicants to apply for loans from financial institutions.

# Lloyds Bank and London Police team up to fight financial crime

LLOYDS Banking Group and the City of London Police have signed a partnership agreement which will see the bank invest £1.5 million in unique policing initiatives to tackle economic crime.

The money will be allocated to several projects over a three-year period, with the goal being to strengthen UK financial capabilities to detect criminals and to protect the public and businesses.

For example, the partnership will deliver cross-training of financial investigators with the intention of sharing best practices and expertise across both organisations.

This will enhance capability in the detection, prevention and awareness of economic crime.

In addition, a programme of secondments and exchanges between the City of London Police and Lloyds Banking Group will take place, helping investigators and analysts to better understand criminal methodologies and banking practices and how this affects law enforcement.

During the three-year period, an economic crime panel of experts will be established, which will allow for a group of volunteer specialist economic crime advisors to come together and share expertise and best practice.

# Australian banks boost fraud protection systems

FIVE banks in Australia have agreed to improve their fraud protection systems following a review by Australian Securities and Investment Commission (ASIC).

They will improve their compliance measures and controls for deposit accounts that can be operated by a third party, such as a financial adviser.

The banks involved in the review have agreed to make improvements to their current practices based on ASIC's findings, including:

- Ensuring account application forms adequately explain to customers that they will be giving the adviser authority to operate on their account, and sending follow up communications to customers after the account is opened with details of the authority that has been given;
- Better monitoring of the advisers' use of such accounts and their transaction requests, and investigating any suspicious requests; and
- Considering the circumstances of any fraud that occurs using these accounts and, where appropriate, remediating a customer who has lost funds due to unauthorised transactions by their adviser.

ASIC's industry-wide review was prompted by concerns raised through an investigation of the conduct of persons involved in Sherwin Financial Planners Pty Ltd (in liquidation) and Wickham Securities Pty Ltd (in liquidation).

By the time the Sherwin group of companies collapsed in January 2013 they owed nearly AUS$60 million to approximately 400 clients.

ASIC's review looked at the policies, procedures and controls that banks have in place to prevent fraud and unauthorised transactions for consumers who have deposit accounts that can be operated by their adviser.

ASIC's review did not identify concerning levels of fraud but found that banks could do more to manage the risks to customers associated with third party access to money in customers' accounts.

At the time of review, there were around 455,000 of these accounts open across the five banks ASIC reviewed, held by approximately 530,000 customers with balances totalling around AUS$28.6 billion.

These accounts are often marketed as 'cash management accounts'.

The findings of the review include:

- The amount of control that advisers are provided with over a consumer's deposit account varies between different banks – from 'view only' access to complete control.
- Banks should do more to explain the level of access that customers are providing to their financial adviser, and the potential risk of unauthorised transactions.
- Control measures for protecting customers' accounts from unauthorised activity should be strengthened, and banks should do more to reduce the risks to customers.

The five banks that were reviewed were Bendigo and Adelaide Bank Limited, Commonwealth Bank of Australia, Macquarie Bank Limited, National Australia Bank Limited and Westpac Banking Corporation.

ASIC's review found that adviser-operated deposit accounts are most popular with older Australians. Of the 497,000 individuals identified through ASIC's report, 73 percent were aged 50 years or older.

# Groups used smurfing, crypto exchanges to launder €2m

TWO criminal groups who laundered an estimated €2.5 million using different methods, such as smurfing and cryptocurrency exchanges, have been dismantled following action taken by Spain's Guardia Civil and the National Police of Colombia with support from Europol.

Twenty-three members of the group were arrested – mainly from Spain, Colombia and Venezuela - and another nine investigated.

Twelve house searches were carried out - 10 in Spain and 2 in Colombia - and two vehicles seized, alongside mobile phones, computers and banking and financial documents.


Also, numerous virtual wallets used by the criminal organisation to launder the cash were frozen by law enforcement authorities.

Europol supported the operation by facilitating information exchange and by deploying four experts to Spain equipped with a mobile office and a Universal Forensic Extraction Devices (UFED).

The investigation began in January 2017 when Colombian authorities warned about a Colombian family with

links to drug trafficking that was operating in the Spanish city of Zaragoza.

The Spanish Guardia Civil verified the existence of a criminal organisation operating in Spain and dedicated to laundering the money earned by other criminal groups who were operating in various locations in Spain and France.

The criminal network picked up the illicit proceeds, split them and sent them in small remittances – a criminal method known as smurfing.

Among the criminal groups they collected the money from, investigators also identified a second network operating in Madrid in Spain.

This second network was also involved in collecting large sums of cash from other criminal groups linked to illicit activities such as drug trafficking or crimes against the heritage in Spain.

The group used cryptocurrency exchanges to convert large amounts of money from cash into cryptocurrencies, like Bitcoins and Altcoins, and later transferred them to other virtual wallets controlled by the Colombian organisation, which allowed the return of the illicit proceeds to South America, thus hiding the origin of the money.

# from page 1 - bills of lading manipulation

represented by the bill of lading could be worth substantial sums of money.

Hence, IMB says it is vital that banks and shipowners are aware of this trend.

If this trend continues, it may become necessary for banks when they do their compliance checks for B/Ls with IMB, to provide both the front and the back pages of the B/L (in the case of documents where there is an endorsement on the back) so that that endorsement can be inspected thoroughly, IMB says.

These checks may take longer than normal.

These abuses of B/Ls undermine the integrity of this document which is relied upon by so many stakeholders in the trading chain including banks, shipping companies and genuine buyers and sellers.

And for this reason, when these documents are identified, there is a case for the stakeholders who have information regarding the parties who are submitting these documents to reveal it to the IMB.

This will enable the IMB to record this intelligence on its database and pass relevant information without identifying the source to other potential victims of this type of fraud, IMB says.

# Proposals will give European Banking Authority more power

THE European Banking Authority (EBA) could soon have additional powers to regulate financial institu–tions to better address money laundering and terrorist financing threats.

Last month, the European Commission (EC) announced it would strengthen the EBA's role and give it the necessary tools and resources to ensure effective cooperation and convergence of supervisory standards.

The Commission said this would consist of legislative and non-legislative measures to make anti-money laundering (AML) supervision more effective and improve the cooperation between prudential and AML supervisors.

"These measures will contribute to promoting the integrity of the EU's financial system, ensuring financial stability and protection from financial crime," the Commission said.

It proposes to give the EBA a more explicit and comprehensive mandate to ensure that risks of money laundering and terrorist financing in the European Union's financial system are effectively and consistently incorporated into the supervisory strategies and practices of all relevant authorities.

If adopted, the EBA will have new powers, among others, to be able to request national AML supervisors to investigate potential material breaches and to request them to consider targeted actions such as sanctions.

Also, the EBA's existing powers will be reinforced so that, as a last resort if national authorities do not act, the EBA will be able to address decisions directly to individual financial sector operators.

The Commission has set out some FAQs about the proposed changes.

**What are today's AML rules and how do supervisory authorities manage associated risks?**

The EU has a strong legal framework for preventing and fighting money laundering and terrorist financing in place. Financial institutions as well as other entities are required to put in place internal systems to identify, assess and manage money-laundering risks related to their business.

The supervisory framework for combating money laundering is based on the Anti-Money Laundering Directive (AMLD), which also applies to a number of actors outside the financial services sector.

While the rules are set at European level, their enforcement is carried out by national authorities.

*"Recent cases of money laundering in European banks have given rise to concerns about weaknesses and gaps in the implementation of the legislative framework"*

The fifth revision of the AMLD (5AMLD) is an important step forward towards a stronger supervision of money-laundering issues in the EU. The Directive sets up a system for better cooperation and exchange of information between money-laundering and prudential supervisors. It also provides for the conclusion of a Memorandum of Understanding between the money laundering supervisors and the European Central Bank for the exchange of information.

**Why is additional action on supervision required?**

Despite this strengthened legislative framework, several recent cases of money laundering in European banks have given rise to concerns about weaknesses and gaps in the implementation of the legislative framework by the EU's network of different supervisors, in relation to three issues in particular:

- Delayed and insufficient supervisory actions to tackle weaknesses in financial institutions' AML risk management;
- shortcomings with respect to cooperation and information sharing both at domestic level, between prudential and AML authorities, and between authorities in different Member States;
- lack of common arrangements for the cooperation with third countries in relation to the AML supervision of financial institution.

In the EU, the supervision of comliance with AML legislation is carried out at national level.

In the Banking Union, the Single Supervisory Mechanism (SSM) is tasked with the direct supervision of significant banks. At the same time, for the prudential aspects relevant to money laundering supervision, it has to apply and rely on national legislation transposing EU Directives in the relevant Member State.

At EU level, the European Supervisory Authorities [the EBA, the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)] have the mandate to ensure that the Union's prudential and AML rules are applied consistently, efficiently and effectively.

However, this is just one of the many tasks these authorities have to carry out. In addition, supervisors are subject to differently transposed national

Continued on page 7/

# from page 6 - new powers for EU banking regulator

rules, as prudential requirements in legislation have not been supplemented with harmonised guidance.

**What changes to the current anti-money laundering framework does the Commission propose?**
In order to address the shortcomings identified and further reduce risks in the EU financial system, the Commission proposes, updating its previous proposals on the European Supervisory Authorities, to introduce a set of targeted amendments to the existing legislation on prudential supervision and the regulatory framework of the European Supervisory Authorities.

To ensure high quality AML supervision and effective coordination among different authorities across all Member States, AML responsibilities in the financial sector will be entrusted specifically to one of the three European Supervisory Authorities (ESAs), namely the EBA, as it is in the banking sector that money-laundering and terrorist financing risks are the most likely to have a systemic impact.

The Commission proposes to clarify the EBA's mandate in the context of anti-money laundering in order to make it more explicit and more comprehensive, accompanied by a clear set of tasks, corresponding powers and adequate resources.

**What is the role of the European Banking Authority under the new rules?**
On the basis of existing tools and powers of the Authorities, as amended by the pending proposal to review the European Supervisory Authorities, the Commission proposes to give the EBA a more explicit and comprehensive mandate to ensure that risks of money laundering and terrorist financing in the Union's financial system are effectively and consistently incorporated into the supervisory strategies and practices of all relevant authorities.

The amended Regulation will:

- ensure that breaches of AML rules are consistently investigated: the EBA will be able to request national AML supervisors to investigate potential material breaches and to request them to consider targeted actions - such as sanctions;
- provide that the national AML supervisors comply with EU rules and cooperate properly with prudential supervisors. The EBA's existing powers will be reinforced so that, as a last resort if national authorities do not act, the EBA will be able to address decisions directly to individual financial sector operators;
- enhance the quality of supervision through common standards, periodic reviews of national supervisory authorities and risk-assessments;
- enable the collection of information on AML risks and trends and fostering exchange of such information between national supervisory authorities (so-called data hubs);
- facilitate cooperation with non-EU countries on cross-border cases;
- establish a new permanent committee that brings together national AML supervisory authorities.

The Commission says these amendments will bring major improvements to the supervisory framework of AML risks and contribute to risk reduction in the financial sector.

**How will the three European Supervisory Authorities cooperate on the fight against AML and terrorist financing?**
A dedicated committee will be established within the EBA to prepare decisions relating to money laundering and terrorist financing measures (comparable to the existing EBA bank resolution committee). It will be composed of heads of national supervisory authorities responsible for ensuring compliance with laws against money laundering and terrorist financing. The EBA will also cooperate closely with the ESMA and the EIOPA in the framework of the existing Joint Committee of the ESAs.

**How did the Commission prepare this proposal?**
In May 2018, the Commission invited the Chairpersons of the ESAs, the Chairperson of the Anti-Money Laundering Committee of the European Supervisory Authorities and the Chairperson of the Supervisory Board of the European Central Bank, to establish a Joint Working Group to initiate a collective reflection on ways of improving the current framework for cooperation between AML and prudential supervisors.

**How does this link work on completing the Banking Union?**
Money laundering issues create risks for the integrity and reputation of the European financial sector and may have financial stability implications for specific banks. The European Parliament and the Council have therefore indicated that this is a matter for further work as the EU is completing its Banking Union by risk reduction and risk sharing and developing the Capital Markets Union.

AML issues are part of the work on Banking Union mandated by the European Council until December, and the European Parliament has proposed relevant amendments in the context of the pending relevant legislative proposals, in particular the Banking Package, proposed by the Commission in November 2016.

The Commission has encouraged the European Parliament and the Council to reach agreement on these proposals swiftly.

# Egypt attempts to curb corruption being undermined

*Egypt's attempts to crack down on corruption, commercial crime and money laundering are real. But they are being undermined by low existing standards, government authoritarianism and blind-eyes turned to military wrong-doing, anti-crime experts argue.* Pavlos Boulos *reports*.

THE Egyptian government talks a good game when it comes to fighting financial crime. At the behest of the International Monetary Fund (IMF) it is imposing a slew of reforms to improve its capacity to suppress graft, fraud and dirty money flows.

Cairo amended the regulations governing the Administrative Control Authority (ACA) in October 2017 to bolster anti-corruption efforts among the state's six million employees.

"Egypt is trying to present itself as following the IMF reform programme, which includes measures on transparency and corruption. The Central Bank has been making concerted efforts in this field," said Chloe Teevan, programme coordinator for the European Council on Foreign Relations' Middle East and North Africa Programme.

The government of strongman President Abdel-Fattah Al Sisi, a former field marshal, last year passed five amendments granting the body full technical, financial and administrative independence to investigate corruption.

These changes also require an annual report to be submitted to the President and the Egyptian parliament, as well as coordination with other watchdog institutions such as the Central Auditing Agency.

Also, to try and improve the ACA's investigative capabilities, a memorandum of understanding (MoU) was signed with the USA's Federal Bureau of Investigation (FBI) in December 2017.

According to the FBI, two ACA officers have graduated from the FBI's National Academy, and the two agencies have conducted joint training exercises.

According to a Lebanese financial consultant that is working with the Egyptian government on regulatory reform, who wanted anonymity, there is also a significant amount of training underway in AML issues of state employees.

"There is a willingness at the top level to implement reforms and train up staff," he said.

## Low base

All this is positive. But the fact is that Egypt's attempts to fight corruption and other financial crime is starting from a low base.

The consultant said, "Many of the middle and lower level state employees lack appropriate knowledge and training, be it for anti-money laundering or understanding global regulatory requirements and why they need to be abided by. So, there is progress, but Egypt is way behind international norms, and enforcement is another key problem," he said.

This is because, to put it politely, Egypt's judiciary is not up to scratch – especially when it comes to judging and assessing complex international financial crime. As the USA State Department's 2017 International Narcotics Control Strategy Report (INCSR) observed, "Egypt should improve its capacity to successfully investigate and prosecute money laundering offences. In particular, the judicial system should continue to increase the number of judges trained in financial analysis related to money laundering activity."

Such a shortcoming is noted on the ground. "You can tell from the judiciary's line of questioning that they don't have basic knowledge of simple things like what a tax haven is, or where the British Virgin Islands are. There is definitely a lack of understanding…" said Osama Diab, a non-resident fellow at the Tahrir Institute for Middle East Policy in Washington DC.

That said, if a weak status quo was the only problem Egypt's anti-crime reforms had to contend with, there would at least be light at the end of the tunnel – a good chance that north Africa's most populous country (95 million souls and rising) would become a cleaner place to do business in future.

## Regime concerns

But it is not. Egypt has also been sliding into authoritarianism under President Sisi, sparking concerns that anyone with good contacts with the current military-backed government are likely to get a free ride if they break the law. And political opponents may get hit, even if they are clean.

Terror finance rules are a case in point. Egypt has been waging a campaign against domestic terrorism, issuing an Anti-Terrorism Law in 2015, which includes a life-sentence for financing terrorist groups.

Critics however say that the law has been used for political purposes, with over 60,000 imprisoned, the majority members of the Muslim Brotherhood, which was officially banned in 2013.

"The terror list that the regime creates is artificial, including obvious political opponents, for example the ex-footballer Abu Treika, who was placed on the list with no evidence," said Maged Mandour, an Egyptian researcher at the Carnegie Endowment for International Peace.

*Continued on page 9/*

# Foreign bribery 'still a problem in over half of global trade'

TRANSPARENCY International's (TI) new report, Exporting Corruption, finds that only 11 major exporting countries - accounting for about a third of world exports - have active or moderate law enforcement against companies bribing abroad in order to gain mining rights, contracts for major construction projects, purchases of planes and other deals.

Country by country, the report names the top offenders as well as the flaws in national legal systems that allow this crime to continue unchecked. TI says one of the most shocking examples exposed in recent years is the massive foreign bribery scheme carried out by the Brazilian construction conglomerate Odebrecht involving about US$788 million in bribes to government officials and political parties in at least 12 countries.

"Foreign bribery has huge negative consequences for the economies of the nations targeted. Money gets wasted on deals that are overpriced or do not yield real benefits. Limited resources are diverted to benefit a few individuals while citizens are denied vital public services, such as access to clean water, safe roads or basic health services," said TI.

Around the world, competitors that offer better products lose out in an unfair marketplace and this triggers a race to the bottom, with some companies choosing to engage in bribery because others are doing it.

# from page 8 - Egypt corruption

Football star Abu Treika, who currently resides in Qatar, was put on a terrorism list along with 1,529 others for alleged ties to the Muslim Brotherhood in January 2017.

"They are arresting anybody criticising the regime, often for allegedly supporting the Brotherhood: liberals, secular bloggers, legalists, and political bodies," says Mandour.

Egyptian banks are nonetheless required to screen accounts for black-listed individuals, with the government regularly issuing updated lists.

While Sisi has publicly stated that 1.5 percent of the economy is in the military's hands, independent estimates range 5 percent to even 40 percent of GDP: "What Sisi said is hard to believe, the lowest possible estimate, but even that is a lot of money, 1.5 percent of US$332 billion," said Mandour.

"The private sector is being squeezed out by the military," he adds.

Crucially, the ACA, does not have the mandate to probe the military, which is handled by military courts.

"Whatever initiatives they create are pointless if an agency can't investigate financial crimes by the military," said Mandour.

### Military immunity

Under a 1966 law, amended in 2012, the military is immune from being investigated for financial crimes and corruption, while military personnel are exempt from investigation or prosecution until retirement.

So, it was not for nothing that earlier this year, President Sisi issued a law that allows senior officers to serve for life: "That means such officers will never be investigated for any financial wrong doing," said Mandour.

The military's re-seizure of power in 2013 after a year of a Muslim Brotherhood government, which followed the 2011 ejection by revolution of another military-backed ruler, President Hosni Mubarak, has led the armed forces to reinvigorate their political and economic position in the state, further cemented by the election of Sisi as President in 2014.

This led to the amending of laws to give the President widespread power, including the ability to appoint or remove heads of supervisory authorities.

"Right across the board regulatory bodies have been subordinated to military control, whether customs or the ACA, or the Central Auditing Organisation. These bodies always had army officers [in senior positions], but now there's more and more officers being put into them," said Robert Springborg, an expert on Egypt and Fellow of the Italian Institute of International Affairs.

"How can we speak of any appropriate or independent regulation?" he asks.

The Sisi government has also placed regime insiders in key official roles. The governor of the Central Bank of Egypt (CBE), Tarek Amer, is the nephew of Abdel Hakim Amer, a former defence minister, while Sahar Nasr, minister of investment and international cooperation, is the daughter of Salah Nasr, the former head of intelligence, and the head of the FIU at the central bank is a relative of President Sisi.

"Under Amer the central bank follows the diktats of government and doesn't release information," said Springborg, notably on the number of suspicious transaction reports flagged by banks, or money laundering cases investigated by the bank's financial intelligence unit which affects the CBE's ability to investigate financial crime.

# Solicitors and law firms report 52% rise in cybercrime

THE Solicitors Regulation Authority (SRA) received a 52 percent increase in the number of cybercrime reports from solicitors and law firms in 2017, with 157 reports compared last year compared to 103 in 2016.

SRA said solicitors and law firms are being targeted by cyber criminals because of the money and information they hold. It says attacks can also threaten a firm's own operations or its reputation.

In its recently published Risk Outlook 2018/19, SRA said cybercrimes and scams that firms were vulnerable to include:

- email modification fraud – the most common type of cybercrime against solicitors, where criminals intercept and falsify emails between a client and the firm, leading to bank details being changed and money being lost.
- phishing and vishing – where criminals email or phone to obtain confidential information, such as a password, through gaining the trust of a solicitor or other member of staff.
- malware – harmful software that includes viruses and ransomware programs, which encrypt files and demand a ransom in return for decrypting the files.
- CEO fraud – where criminals impersonate a senior figure at a firm through hacking, or having a very similar email address, to impose authority and order money transfers.
- identity theft – where bogus firms copy the identity and brand of a firm.

In the first quarter of 2018, email modification fraud accounted for more than 70 percent of all cybercrime reports.

Almost all other cybercrime reports also involve some form of forgery to deceive targets into responding, rather than explicit hacking of the firm's systems.

In 2016, £9.4m of client money was reported as lost to cybercrime, increasing to £10.7m in 2017.

However, SRA says it suspects there is some underreporting, particularly where money is replaced promptly by the firm or their insurer.

This is because SRA is seeing fewer reports than we would expect given media reporting of the frequency of these attacks.

In one example in March 2018, a firm was attacked with ransomware. The criminals left a ransom note on the firm's system, saying that they had obtained sensitive information and would publish it unless the firm paid £3m.

The firm declined to do this and the criminals began publishing the firm's data through Twitter.

The firm worked with computer forensics specialists to deal with the breach and find out how their system was accessed.

And they obtained an injunction from the High Court to bar anyone from further sharing the information that the hackers had published, as well as successfully securing the removal of information from websites. They reported the breach to the National Crime Agency and to the SRA.

It is not yet clear how the firm's systems were infected with ransomware, but many of these attacks rely on fake links or attachments in emails.

### Spotlight on email modification fraud

This fraud happens when criminals impersonate someone going through a process involving the transfer of money, such as a property transaction. They do this by breaking into that individual's email system or forging emails from it.

The criminals contact the solicitor through the stolen or falsified address to tell them the bank account details have changed.

They usually do this at short notice and when there is time pressure, for example, on the afternoon of a property completion.

The solicitor sends money to the new bank account and this is quickly moved on by the criminals. When used to steal conveyancing money, it is also known as 'Friday afternoon fraud', as many of these transactions take place on Friday afternoons.

SRA has also seen cases where the criminal impersonates the firm and tells the client that the firm has new bank details.

In these cases, the client sends the deposit and other money directly to the fraudster's account.

This fraud is relatively common in firms and often accounts for at least half of all cybercrimes.

During 2017, email fraud reported to SRA fell to an average of 46 percent of all cybercrimes but in the first quarter of 2018 had risen to 71 percent.

### Spotlight on remote working

Firms are increasingly using systems to help their employees work on the move. This includes 'bring your own device', which allows people to work from home or anywhere on their own devices while connected to a cloud-based server.

This can offer security if updates to the system are made automatically and data is backed-up.

*Continued on page 11/*

# Financial organisations too confident about cyber security

FINANCIAL services firms in the United Kingdom are too confident about their cyber security protection, a survey by FICO and Ovum has shown.

The survey says 55 percent of the executives from the sector who were interviewed believed their firm was a 'top performer', while 41 percent said their firm was 'above average'.

But FICO says this is not realistic.

Despite this confidence, only 36 percent of organisations are carrying out more than a point-in-time assessment of what their cybersecurity risk is.

"The grave risk posed to our privacy and security demands that firms take an honest view of their protection," said Steve Hadaway, FICO general manager for Europe, the Middle East and Africa.

He added, "These numbers suggest that many firms just don't understand how they compare to their competitors, and that could lead to a lack of investment. When we review firms' cyber security risk with our FICO Enterprise Security Score, I can tell you that most firms are not above average."

Telecommunications providers were second, with 42 percent calling their firm a top performer. The least confident - or most realistic - respondents were in retail and ecommerce, where 38 percent said their firm is a top performer, and just 19 percent said they were above average.

The survey showed three out of four executives from UK firms said their firm was better prepared than their competitors, and 43 percent said their firm was a top performer.

While this overconfidence was seen across the eight regions surveyed, Canada was the only country where more respondents (44 percent) said they were a top performer for cybersecurity protection.

Maxine Holt, research director at Ovum said, "IT leaders have greater funding than ever to protect organisations from the continuously evolving threat landscape and meet complex compliance demands.

"These same IT leaders are undoubtedly keen to believe that the money being spent provides their organisation with a better security posture than any other – but the rapid pace of investment, often in point solutions, rarely takes an organisation-wide view of security."

Ovum conducted the survey for FICO through telephone interviews with 500 senior executives, mostly from the IT function, in businesses from the UK, the US, Canada, Brazil, Mexico, Germany, India, Finland, Norway, Sweden and South Africa. Respondents represented firms in financial services, telecommunications, retail and ecommerce, and power and utilities.

from page 10 - law firms see rise in cybercrime

### What solicitors and firms can do

SRA says it wants firms to benefit from the advantages IT can bring.

However, they need to take care that their system keeps client information and money safe. The best defences against many cyberattacks are to:

- keep systems updated.
- use antivirus software on desktops and laptops.
- backup important information frequently and securely, and learn how to restore the system from a backup.
- encrypt mobile devices and install a system to track and delete the data if they are lost.
- make sure everyone in the firm knows how to create secure passwords.
- avoid using administrator accounts (those with the privilege to access other users' accounts and install software) for regular work that does not involve maintaining the IT system.
- make sure everyone in the firm knows how to recognise the signs of email modification fraud and common phishing scams.
- plan how to respond to an attack or other incident.

SRA says it is working with the National Cyber Security Centre (NCSC) and the IT security sector to regularly update the information it provides to firms.

No defence is perfect, and some organised cybercrime activity can be hard for even technology companies to stop. As such, SRA says it takes a proportionate approach to breaches reported to them.

When SRA has taken regulatory or disciplinary action against firms, it has been where the firms did not:

- take reasonable steps to protect themselves or check their client's instructions.
- follow basic security guidance.
- report the incident, where appropriate.
- act to remedy the losses.

**Cybercrime**

# Firms face real threat of denial of service attacks

FINANCIAL institutions still face a very real threat from denial of service attacks that could disrupt their operations, Verizon Enterprise has warned in its 2018 Data Breach Investigations Report.

They still need to be alert to payment card skimmers installed on ATMs by organised criminal groups, and now there is ATM jackpotting too, where software or hardware is installed to make the ATM spit out money.

Verizon's analysis found there were 146 breaches and 598 incidents in the financial sector so far this year.

The majority of breaches (79 percent) were perpetrated by outsiders with 19 percent reportedly coming from sources within organisations.

Hacking was responsible for 34 percent of cyber breaches.

Overall Verizon's study revealed there were over 53,000 cyber attack incidents this year, including 2,216 confirmed data breaches.

There were 53,308 security incidents and 2,216 data breaches across 65 countries.

"This year we saw, yet again, that cybercriminals are still finding success with the same tried and tested techniques, and their victims are still making the same mistakes," Verizon says.

It adds, "Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will. That could mean stealing payment card data, personally identifiable information or your intellectual property.

"And they don't care who they take it from. Ignore the stereotype of sophisticated cybercriminals targeting billion-dollar businesses."

Verizon said most attacks are opportunistic and target not the wealthy or famous, but the unprepared. Seventy-six percent of breaches were financially motivated, with almost three-quarters (73 percent) of cyberattacks being perpetrated by outsiders.

"Members of organised criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12 percent," Verizon said.

"Not all the baddies are outsiders though. Over a quarter (28 percent) of attacks involved insiders. The insider threat can be particularly difficult to guard against - it's hard to spot the signs if someone is using their legitimate access to your data for nefarious purposes."

# Singapore wants financial firms to beef up cyber resilience

THE Monetary Authority of Singapore (MAS) is proposing that financial institutions (FIs) in Singapore implement essential cyber security measures to protect their IT systems.

These requirements will help FIs strengthen their cyber resilience and guard against cyber attacks.

FIs will be required to implement six cyber security measures:
1. Address system security flaws in a timely manner; establish and implement robust security for systems.
2. Deploy security devices to secure system connections.
3. Install anti-virus software to mitigate the risk of malware infection.
4. Restrict the use of system administrator accounts that can modify system configurations; and,
5. Strengthen user authentication for system administrator accounts on critical systems.

These measures, which are already part of the existing MAS Technology Risk Management Guidelines, are aimed at enhancing the security of FIs' systems and networks as well as mitigating the risk of unauthorised use of system accounts with extensive access privileges.

**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: Nathaniel Xavier Email: nathx73@yahoo.co.uk
**ISSN 1012-2710**