COMMERCIAL CRIME International

January 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

CCS underscores benefits of anti-counterfeiting project

COMMERCIAL Crime Services (CCS) has welcomed the move by three leading companies to sign up to the Declaration of Intent to Prevent the Maritime Transport of Counterfeit Goods (DOI).

A year on from when the original declaration was signed in November 2016, it has been announced that ocean carrier APL, global automotive giant Honda and French luxury leather goods company Longchamp, have added their signatures to the Declaration. *(see January 2017 issue of CCI)*

CCS is one of several organisations, which include the International Federation of Freight Forwarders Associations (FIATA) and the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy (BASCAP), who are part of this worldwide initiative.

The Principles of the Declaration include a zero-tolerance policy towards counterfeiting, as well as strict supply chain controls, risk profiling and due diligence checks to ensure maritime operators are not co-operating with those involved with counterfeiting.

APL, Honda and Longchamp join other big names such as Maersk, MSC and CMA CGM; freight forwarders – Kuehne and Nagel and Expeditors; and major multinational brand owners – Unilever, Bayer, Procter & Gamble, Chanel, Pfizer, Richemont, Lacoste, Dupont, Philip Morris International and CropLife.

CCS said one of the factors which will help in the fight against counterfeits shipped around the world is for carriers and brand owners to have a resource of data which highlights recent cases of counterfeit shipments.

Such a database will offer a number of benefits.

- It enables statistics to be developed which, can then be used to generate interest and call for governments to allocate resources to tackle counterfeiting
- Provides intelligence to shipping intermediaries so they can avoid getting involved in suspect shipments. This will create further barriers for counterfeiters to use the supply chain to move fake goods.
- In the long term it can help identify trends that will help Customs, shipping companies and manufacturers, allowing risk profiling and targeting of counterfeit shipments in advance.

Members are reminded that CCS is able to help via its role and systems developed over the last 36 years, in collecting, analysing and promulgating industry relevant information which could aid in the prevention of counterfeiting as well.

This would simply be another application of a time-tested service to the industry provided by CCS.

It is also a good example of public-private partnership in dealing with organised crime.

The DOI is a result of a major report done by BASCAP on *'The Roles and Responsibilities of Intermediaries – Fighting Counterfeiting and Piracy in the Supply Chain'* which identified global shippers as one of the key intermediaries being infiltrated by large amounts of counterfeit goods.

"The DOI is a joint effort between the global shipping industry and brand owners to work together to stop the transport of counterfeit goods on shipping vessels," said Sophie Peresson, director of BASCAP.

"It responds to growing concerns of BASCAP members about criminals exploiting shipping vessels as a

Continued on page 2/

In This Issue of CCI

Supply Chain Security

Transport supply chain players 'must address cyber risks'

TT Club has added its voice to growing concerns over the frailty of the global supply chain when faced with cyber attacks.

Alexis Cahalan, formerly of the TT Club, now with Thomas Miller Law based in Sydney, emphasised the logistics and freight forwarding community's particular vulnerability to disruptive cyber activity.

Her conference paper at the Trans-Pacific Asia Conference held in China referenced the recent "not Petya" incident as evidence that the risk of cyber attack is now a reality which needs to be seriously addressed by all participants in the transport supply chain. "There is a case for employing a corporate culture of risk management to assess these vulnerabilities within individual companies and to develop a response framework with this in mind," advised Cahalan.

Risks are increasing rapidly not just in terms of greater hacking and malware activity. The desire for supply chain visibility and efficiencies is driving technologies, such as Internet of Things and access through smartphones and the like. There is a danger that rapid adoption of such technology means many companies have yet to consider thoroughly the cyber security implications of 'bring your own device' procedures. Defensive action cannot be whittled down to just one area of operation.

However, human behaviour, both a successful supply chain's greatest strength and weakness, can be usefully targeted.

"Employee awareness of the potential dangers of day-to-day activities will help. Trust in email communication, auto-connect Wi-Fi settings and password protocols, peripheral equipment and flash drives, computers in general, should all be monitored and reviewed," she said.

from page 1 - maritime anti-counterfeiting declaration

channel for transporting large quantities of counterfeit products. We have been very impressed by the response and cooperation from the maritime shipping industry to DOI initiative."

Geraldina Mattsson, Department Manager of the Intellectual Property Department for Honda Motor Europe said container loads of counterfeit automobile parts are shipped around the world, without detection, by criminal networks using a variety of techniques to hide their unlawful activity.

"We see this Declaration as an important step in bringing together the brand owners, vessel companies and the service industry that supports maritime trade to find solutions. We are delighted to add Honda's name to the list of signatories," she said.

Marilyne Serafin, Head of the Intellectual Property Department for Longchamp said, "Like others in the luxury and fashion goods industry, Longchamp products are counterfeited on a large scale and vast amounts of fakes are shipped by sea to ports around the world.

"We are pleased to add our name to the Declaration to show our support for this critically important joint effort with the maritime industry. This type of voluntary collaboration among all of the parties that deal with this transport issue will be the key to stopping these illegal fake goods from getting on the world's vessels."

The UN Office on Drugs and Crime has reported that containerised transport of goods accounts for around 90% of total international trade; however, less than 2 percent of these containers are ever inspected to verify their contents.

According to a report by Organization for Economic Co-operation and Development and European Union Intellectual Property Office, trade in counterfeit goods amounted to US$461 billion in 2013, an 80 percent increase on the figures from 2008.

This means that counterfeits account for 2.5 percent of total global trade value. Another report by Frontier Economics, commissioned by BASCAP and the International Trademark Association, predicts the total annual cost of counterfeiting and digital piracy at between US$923 billion and $1.13 trillion, and predicts this could double by 2022 if current trends continue.

Meena Sayal, Unilever global brand protection director, said since the original signing, signatories have formed five working groups and have started to develop best practices on issues such as Know Your Customer – all targeted at stopping the maritime transportation of counterfeit goods.

CCS - via Counterfeiting Intelligence Bureau (CIB) - provides specialised intelligence to members to tackle counterfeiting. CIB operates the Hologram Image Register for the International Hologram Manufacturers Association.

* *EC announces IP protection measures - page 6*

The case for outsourcing your KYC

Outsourcing KYC is a good way for banks to safeguard their continued regulatory compliance and control spiralling costs, explains Toby Tiala*, Programme Director, Equiniti KYC Solutions.*

IN a bid to combat money laundering, market manipulation and even terror funding, the rising tide of conduct-based regulations continues to challenge banks globally. The cost of compliance - and non-compliance - is steep. The average bank spends over £40m a year on Know Your Customer (KYC) processes yet, in 2016 alone, bank fines worldwide rose by 68%, to a staggering $42bn.

A double squeeze

Resource stretched mid-sized banks, in particular, are having a tough time. As regulators up the ante they are creating an operating environment increasingly conducive to fines. To cope, banks are expanding their compliance resources to mitigate their risk of transgression. Those with resource limitations are, therefore, the most vulnerable.

They are right to be worried. Since 2008, banks globally have paid a staggering $321bn in fines. Earlier in the decade, high profile money laundering and market manipulation cases caused the level of overall fines to skyrocket. After a brief period of respite (when governments and the Financial Conduct Authority backed off fearing industry suffocation), the fines have been steadily creeping back up. This time, however, big ticket fines have been replaced by a far higher number of smaller penalties. Put another way, the regulators are now tightening a much finer net than before.

A bank's ability to profile and identify risky customers and conduct enhanced due diligence (EDD) is critical to ensuring compliance with anti-money laundering (AML) law. This is no trivial task. Major banks are ploughing expertise into their KYC and creating proprietary systems dedicated to meeting the new requirements. Mid-sized banks, however, don't have this luxury and are challenged by the need to beef up their resources. Applying regulations like AML4, PSD2 and MiFID II to complex legal entities like corporates and trusts is a convoluted business.

New focus

A large proportion of regulatory fines result from high risk customers slipping through the cracks, usually stemming from ineffective beneficial ownership analysis, customer risk rating or EDD. This is especially common in complex entities with numerous 'beneficial owners' - something that has brought these individuals into sharp focus. A beneficial owner in respect of a company is the person or persons who ultimately own or control the corporate entity, directly or indirectly. Conducting KYC to effectively identify high-risk beneficial owners of complex entities is skilled and complicated work, to say the least.

Nowhere can the new focus on beneficial ownership be seen more clearly than in the EU AML4 Directive, which recently came into force, in June 2017. This directive is designed to expose companies with connections to money laundering or terrorism, and decrees that EU member states create and maintain a national register of beneficial owners.

Big impact

The growing focus on beneficial ownership is having a clear impact on banks' relationships with their trade customers. According to research from the International Chamber of Commerce, 40% of banks globally are actively terminating customer relationships due to the increasing cost or complexity of compliance. What's more, over 60% report that their trade customers are voluntarily terminating their bank relationships for the same reason. That this could be evidence of the regulations working will be of little comfort to banks that are haemorrhaging revenue as a result.

The UK has already formed its beneficial owners register but caution is advised. The data quality still has room for improvement and the regulations make it clear that sole reliance on any single register may not translate into effective AML controls. Mistakes - genuine or otherwise – may still occur but automatically checking these new beneficial ownership registers is a clear step forward.

The key for mid-size banks is to zero in on what will both enhance their KYC procedures and deliver clear and rapid visibility of high risk entities. Once established, this will enable them to manage their own risk profile, together with their customer relationships, and minimise the negative impact on their revenues.

Highly complex KYC and EDD activity can severely inhibit the onboarding process for new customers, often causing them to look elsewhere. The deepening of these procedures is making matters worse – it can now take up to two-months to onboard a new client according to Thompson Reuters, with complex entities usually taking the most time. Large banks have proprietary systems to accelerate this process but, for mid-sized banks, this is a serious headache; not only does it extend their time-to-revenue from corporate clients, it can also turn them away entirely, and lead them straight into the hands of their larger competitors.

Continued on page 4/

Money Laundering

EU Parliament proposes new AML measures

THE EU's Civil Liberties Committee has agreed new measures to step up the fight against money laundering.

Members of European Parliament (MEPs) are seeking to introduce EU-wide definitions of money laundering related crimes, including practices that are not currently deemed a crime in all EU countries, such as self-laundering (i.e. where a person who has committed a crime tries to hide the illicit origin of those proceeds).

They also want an EU-wide minimum term of imprisonment of at least two years in cases with aggravating factors, such as organised crime.

Where a judge passes the national maximum jail sentence, it would have to be of at least five years.

The MEPs said the lack of uniform definitions and penalties currently allows criminals to exploit differences and commit crimes where penalties are lowest.

MEPs want a range of new EU-wide penalties for those convicted of money laundering, that goes further than the existing EU Commission's proposal.

These include:

- barring those convicted from running for public office or holding a position of public servant,
- banning businesses and other legal persons from signing contracts with public authorities, and
- confiscating property and other assets.

The EU Parliament's rapporteur on the file, Ignazio Corrao, said: "This directive will deprive criminals of their most important asset, money, and it will make it more difficult for criminal organisations to launder the profits of their criminal activities in the legal economy of the EU.

"Parliament also clearly stated that imprisonment cannot be the only penalty and provided for new additional measures such as confiscation or the ban on entering into contracts with public authorities or running for elected offices."

According to the Commission, the proceeds from criminal activity in the EU are estimated to be €110 billion per year, corresponding to 1 percent of the EU's total GDP.

from page 3 - outsourcing your KYC

Combine and conquer

For these banks, outsourcing their KYC to a dedicated specialist partner is a compelling solution. These partners have agile, tried and tested KYC systems already in place, are perpetually responsive to the changing regulatory requirements and have highly skilled personnel dedicated to navigating the KYC and EDD challenge in the shortest time possible.

Plugging into a KYC-as-a-Service partner enables mid-size banks to seriously punch above their weight, by accelerating their onboarding of new clients to match (and often beat) the capabilities of large banks, dramatically reducing their overall compliance costs and helping them get ahead – and stay ahead - of the constantly shifting regulatory landscape. This, in turn, releases internal resources that can be redirected in support of the bank's core revenue drivers and day-to-day business management.

It is clear that the regulatory squeeze is set to continue for the foreseeable future. Banks that have the vision and wherewithal to accept this notion and take positive steps to reorganise internally will not only be able to defend their ground against larger competitors, they may even turn KYC into a competitive differentiator.

Specialist outsourcing is fast becoming the norm for a wide variety of core banking processes. Few, however, are able to demonstrate as rapid and tangible benefit as the outsourcing of KYC.

**This article is copyright Equiniti KYC Solutions and appeared in November 2017. https://equiniti-kyc.com/news/2017/11/the-case-for-outsourcing-your-kyc/*

A BARCLAYS bank employee in London has been jailed for six years and four months for his role in a conspiracy to launder over £2.5 million, which had been stolen using Dridex malware.

The 29-year-old man acted as 'personal bank manager' to two money launderers, setting up 105 bogus bank accounts for them using false ID documents. He managed the accounts to ensure that receipt of the stolen funds was not blocked by the bank's security processes and that the pair could transfer money between them freely. The money launderers were jailed for the conspiracy in October 2016 after an investigation by the National Crime Agency.

During a search of the man's home, NCA officers recovered over £4,000 in cash, seven luxury watches and three mobile phones.

Organisations urged to protect against impersonation attacks

ONE in five email messages sent today come from unauthorised senders, indicating massive amounts of fraudulent activity, research has suggested.

ValiMail's 2017 Email Fraud Landscape Report shows that the overwhelming majority of company domains are vulnerable to rampant email impersonation attacks.

Even more worryingly, the research says that most companies have not attempted to implement fraud protection through the latest and most complete form of protection, DMARC (Domain-based Message Authentication, Reporting & Conformance).

DMARC is a widely used standard that ensures only authorised senders can use an organisation's domain name in their emails.
Key findings from the report, which analysed the most popular one million global domains, include:

- **Email fraud is a pervasive threat.** One in five messages sent today come from unauthorised senders, indicating massive amounts of fraudulent activity.
- **Virtually all domains lack adequate protection**. Just 0.5 percent of the top million domains have protected themselves from impersonation by email authentication, leaving 99.5 percent vulnerable.
- **Incorrect DMARC deployments prevent email protection**. Over three-fourths (77 percent) of domains that have deployed DMARC records remain unprotected from fraud, either through misconfiguration or by setting a permissive DMARC policy.
- **The difficulty of fully implementing and maintaining DMARC leads to inadequate protection**. Only 15 to 25 percent of companies that attempt DMARC succeed at achieving protection from fraud, depending on category.

DMARC is accessible to most domains. Over three-fourths (76 percent) of the world's email inboxes support DMARC and will enforce domain owners' authentication policies, if those policies exist.

ValiMail says implementing email authentication would save the average company $8.1 million per year in cybercrime costs — $16.2 billion annually across the Fortune 2000.

Alexander García-Tobar, CEO and co-founder of ValiMail said email has been weaponised by hackers as the leading way to infiltrate networks, and the vast majority of businesses are leaving themselves vulnerable by either incorrectly configuring their authentication systems or forgoing protection entirely.

"Businesses are asking their employees to complete an impossible task: identifying who is real and who is an impersonator, by closely examining every message in their inboxes," he said.

He added, "The only sustainable solution is for companies to take control of their email security at the technology level and stop placing the onus on employees to prevent phishing attacks."

Shehzad Mirza, the Director of Operations for the Global Cyber Alliance said the research demonstrates the volume of email fraud threats faced by companies today and highlights the alarming lack of understanding of how to combat these threats.

He said, "In order to truly protect our inboxes, we must drive greater adoption of cybersecurity technologies and protocols such as DMARC."

Mimecast tests show surge in impersonation attacks

THE latest Email Security Risk Assessment (ESRA) test results carried out by Mimecast indicates a sharp rise in impersonation attacks.

While most organisations are concerned about malware being the main risk to their email related security posture, the test results reveal an increased risk of impersonation attacks as compared to attacks leveraging malware.

Mimecast's survey showed that impersonation attacks rose almost 50 percent in the third quarter, compared to the second. Emails with malware attachments or dangerous files types, combined, only increased about 15 percent. Missed impersonation attacks were seen to occur more than seven times as often as missed email-borne malware.

Ed Jennings, chief operating officer at Mimecast said, "This latest report reveals that many email security providers are leaving organisations very vulnerable to these often hard to detect impersonation attacks. Cybercriminals know that many traditional email security services are improving their ability to stop email-borne malware, but remain ineffective against impersonation attacks."

The test inspected actual inbound emails of almost 100,000 users over 631 days. The organisations used a variety of common email security systems.

EC announces intellectual property protection measures

THE European Commission has adopted measures it says will ensure intellectual property rights are well protected.

It says the initiatives will make it easier to act efficiently against breaches of IP rights, facilitate cross-border litigation, and tackle the fact that 5 percent of goods imported into the EU (worth €85 billion) are counterfeited or pirated.

The main measures include:

1. Stepping up the fight against counterfeiting and piracy.

The Commission seeks to deprive commercial-scale IP infringers of the revenue flows that make their criminal activity lucrative – this is the so-called 'follow the money' approach which focuses on the 'big fish' rather than individuals. It also ensures that enforcement actions are adapted to the requirements of today's digital age.

With these initiatives, the Commission aims to:

- **Ensure an equally high level of legal protection and a predictable judicial framework across the EU**. New guidance provides clarification on how to apply the 2004 Directive on the enforcement of intellectual property rights (IPRED). The Directive has proved a relevant tool in fighting IP rights (IPR) abuse, but there have been differing interpretations among Member States of some of its provisions over the years. The guidance clarifies these interpretation issues, which will increase legal certainty for all stakeholders and facilitate civil enforcement across the EU straight away, without the need for new legislation. In addition, the Commission calls on Member States to step up their efforts by boosting judicial training, systematically publishing judgements on IP cases and encouraging alternative dispute resolution tools

- **Encourage industry to fight IP infringements.** Building on the positive experiences under the Memorandum of Understanding on the sale of counterfeit goods via the internet, the Commission continues to support industry-led initiatives to combat IP infringements, including voluntary agreements on advertising on websites, on payment services and on transport and shipping. Such agreements can lead to faster action against counterfeiting and piracy than court actions. They complement recent Commission guidelines for online platforms to tackle illegal content.

Image: Pixabay/iriusman

- **Reduce the volume of counterfeited products reaching the EU market.** The Commission proposes to reinforce cooperation programmes with third countries (China, South-East Asia, Latin America) and create a watchlist of markets that are reported to engage in, or facilitate, substantial IPR infringement. The Commission will publish an updated report on IPR enforcement in third countries. The Commission will step up co-operation between EU customs authorities, notably by assessing the implementation of the EU Customs Action Plan on IP infringements for 2013-2017 and proposing more targeted assistance to national customs authorities.

2. Creating a fair and balanced system for Standard Essential Patents.

Many key technologies that are part of global industry standards (such as WiFi or 4G) are protected by Standard Essential Patents (SEPs). Now, the Commission offers guidance and recommendations for a balanced and efficient SEPs system where two objectives are reconciled: product manufacturers can access technologies under transparent and predictable licensing rules; and at the same time patent-holders are rewarded for their investments in R&D and standardisation activities so that they are incentivised to offer their best technologies for inclusion in standards.

More transparency and predictability should give the EU – including its many start-ups – a headstart in the global technological innovation race and fully grasp the potential of 5G and the Internet of Things.

Measures 'far from enough'

Despite this, the 'Together Against Counterfeiting' alliance, which brings together over 80 companies across all industrial sectors, along with 16 European and national and international trade associations, said the initiatives do not include binding legislative measures to help right-holders in the fight against counterfeiting.

"While the package clarifies several issues relating to the application of IPRED, including the calculation of damages, the scope of injunctions, and a clarification on the concept of "intermediary", it fails to properly address the issue of counterfeiting," the Alliance said.

Continued on page 7/

Working group explores use of behavioural science to tackle fraud

AN industry working group of the Insurance Fraud Bureau (IFB) has appointed behavioural experts to carry out experimental research into the impact different approaches could have on fraud levels.

The work will target opportunistic fraud in personal general insurance lines and the research will explore how changes to various parts of the customer journey could positively change customer behaviour.

It will also assess the potential impact of a public attitude campaign.

Opportunistic fraud includes the provision of false information at application stage and exaggeration of genuine claims.

It is believed to account for a significant majority of the total value of undetected fraud which could cost the industry as much as £2 billion.

Tackling this type of fraud has been a long-standing challenge to the industry, said IFB.

One of the many complex challenges faced by the industry is identifying ways of interrupting dishonest behaviour, or inadvertent mistakes, while reassuring honest customers and avoiding any barriers to the timely payment of legitimate claims.

Decision Technology has been appointed for their innovative approach to running trials within a simulated environment which provides a safe space for testing multiple interventions without disrupting live insurer processes or customers.

IFB said the insurance industry has never done this type of research before. Test results should enable the relative commercial impacts of each intervention to be measured across different insurance products and lifecycle stages.

Recommendations for the long-term approach to addressing the problem will be drawn from the results and presented to the industry in the first half of 2018.

David Hertzell, Chair of the Insurance Fraud Taskforce said, "Tackling opportunistic fraud requires significant and sustained behaviour change which presents immense challenges.

"It is impossible to accurately measure whether or not an opportunistic activity has been prevented; finding ways to measure how effective individual techniques can be is therefore vitally important.

"I am looking forward to seeing the results and how they may be put into practice."

Amanda Blanc, Chair of the IFB and Group CEO AXA UK and Ireland said, "Introducing interventions into the customer journey is an area where we need to tread very carefully. Consumer trust is fragile and we know that the vast majority of insurance customers are honest.

"However, it is important that we find a way to reduce the cost of fraud which ultimately impacts the premiums that those honest customers pay."

She added, "This piece of work is an exciting step forward in helping to identify and measure where we can have the greatest impact."

from page 6 - EC announces measures to protect IP rights

It added, "In its current shape, the package will not strengthen the existing framework and will not prevent counterfeiting on online and offline markets. This could be solved by establishing legally binding provisions applicable to all actors in the value chain and ensuring the implementation of proactive measures against counterfeiting. These measures should be proportionate and appropriate for each type of infringement."

Its members now want the EC to support its measures with strong legislative action before the end of the current mandate, in particular in the framework of the ongoing assessment on tackling illegal content online.

Speaking on behalf of the European Brands Association (AIM) an organisation representing many of the alliance's signatories Michelle Gibbons, AIM's Director General, commented: "The publication of the IP Package is a first step in the right direction, but it is far from enough. Unless the legislative framework to protect European innovation and creativity is modernised and strengthened, counterfeiting will continue to expand dramatically, as will negative impacts for the health and safety of European consumers and the European economy".

The Alliance said the growing proliferation of counterfeiting has clearly shown the limits of the current voluntary approach and the publication of the IP Package constitutes a missed opportunity to create a binding incentive for all actors to join forces in the fight against counterfeiting.

Former investment bank director jailed

A FORMER associate director of a foreign investment bank in Hong Kong (Bank A), has been sentenced to three and a half years' imprisonment at the District Court for accepting bribes of about $1.46 million for managing the investment portfolio of a client with the bank.

The defendant was an associate director of Global Wealth Management and Business Banking of Bank A and responsible for managing clients' investment portfolios. In May 2007, the defendant convinced a client to invest in Hong Kong stocks. The client relied entirely on the defendant to manage his investments.

At a meeting the defendant told the client that it was a trade practice for the latter to pay him 20 percent of the realised profits from investments. The client understood that the 20 percent was "handling and intelligence fees", and acceded to the defendant's request.

Between June and July 2007, the defendant sent the client two emails together with trading summaries detailing a profit of over $3,090,000 earned from trading in stocks. At the end of the trading summaries, there was a remark indicating "20 percent" or over $618,000.

After the defendant reminded the client of the "handling and intelligence fees", the client signed a blank cheque for over $610,000 and gave it to him. The cheque was deposited into the bank account of the defendant's younger brother.

In September 2007, the defendant further sent the client two other emails together with trading summaries detailing another profit of about $4.25 million earned from trading in stocks.

Although the defendant did not make a remark of "20 percent" on the trade summaries, the client understood that he had to pay about $850,000 to the defendant.

One month later, the client gave a signed blank cheque for that amount to the defendant when they met at the hotel. The cheque was deposited into the bank account of the defendant's younger brother.

In December 2007, two sums of money, namely $1 million and $400,000, were transferred from the bank account of the defendant's younger brother to that of the defendant.

The defendant was charged by Hong Kong's Independent Commission Against Corruption which also conducted the investigation.

Ireland to introduce new corruption laws

IRELAND has introduced a new Criminal Justice (Corruption Offences) Bill which is aimed at completely modernising Irish anti-corruption laws.

It will repeal and replace seven existing Acts that deal with corruption and bribery and has been described as a robust and innovative piece of legislation that provides for a number of new offences as well as stronger penalties for those convicted of corruption.

Included in the new legislation is a new strict liability offence where a corporation can be liable for the actions of directors, managers, employees or agents who commit a corruption offence for the benefit of the corporation. Companies will have to prove that they took all reasonable measures and exercised due diligence to avoid the commission of the offence.

This white-collar crime measure is designed to prevent crime in companies and businesses corporate bodies. It shall be a defence for a company to prove that it took all reasonable measures and exercised due diligence to avoid the commission of the offence.

The Bill, expected to come into force in the fourth quarter of 2018, also includes a new offence of 'trading in influence' to criminalise bribing a person who may exert an improper influence over the decision-making of a public or foreign official.

Under the Bill, it is an offence for a public official to make use of confidential information acquired in the course of their duties to obtain an advantage.

It also prohibits a person giving a gift where the person knows or reasonably ought to know that it will be used to facilitate corruption.

Minister for Justice and Equality, Charlie Flanagan who introduced the Bill said, when enacted, it will significantly strengthen Ireland's capacity to tackle corruption, both in public office and in commercial enterprises.

Sentences of up to 10 years are provided for as well as unlimited fines for conviction on indictment of the main corruption offences in the Bill. The Bill gives discretion to a court to order that a public official found guilty of a corruption offence be removed from their public office or position. Those convicted of corruption could also be barred from seeking certain public appointments for up to 10 years.

US seeks better cooperation over MLAT requests

THE United States Department for Justice (DoJ) has said more needs to be done by authorities worldwide to expedite mutual legal assistance (MLAT) requests.

These requests ensure that prosecutors have the evidence that they need to bring criminals to justice, US Attorney General Jeff Sessions said in his keynote remarks at a Global Forum on Asset Recovery held in Washington DC.

He stressed if such evidence is not properly shared between nations, then, in many cases, justice cannot be done.

"It is essential that we continue to improve that kind of sharing. As a prosecutor for 14 years, I know first-hand that the best evidence is often simple things like bank records, airplane records, and telephone records," he said.

In response to the increasing volume and complexity of legal assistance requests, the Department of Justice has taken two actions that are critically important, Mr Sessions said.

"First, we have increased staffing levels at the Department's Office of International Affairs, or OIA. Second, OIA has created two new units dedicated to reviewing and executing foreign requests. As a result, OIA has significantly reduced its backlog by thousands of cases, despite receiving 16 percent more requests in fiscal 2016 than in fiscal 2015.

"These are important steps. But we can and must do more to help one another. I challenge all of you to devote more resources to quickly and effectively reducing your backlog too. You know how serious these cases can be. There is no time to waste."

Mr Sessions said The Department is also working towards the implementation of a framework with some of our closest allies that would supplement the MLAT process and reduce potential conflicts of law regarding the disclosure of electronic evidence. That kind of framework would enhance public safety efforts in the US and around the world.

"In order for this type of framework to function, however, we need to ensure that our warrants continue to be effective even when an American company chooses to store customer data outside of the United States. When we have access to the right evidence, we get results."

Since 2004, the United States has returned millions in corruption proceeds to compensate victims. It has seized or restrained $3.5 billion worth of corruption proceeds involved in money laundering offences, said Mr Sessions. That includes approximately $119 million to the people of Italy, $115 million to the people of Kazakhstan, more than $20 million to the people of Peru, and millions more to the people of Nicaragua, South Korea, and Taiwan.

"That recovery has only been possible because of cooperation with our foreign law enforcement partners," he said.

Mr Sessions said nearly half of the $3.5 billion in corruption proceeds restrained by the Department is related to just one enforcement action. That action was related to a Malaysian sovereign wealth fund known as 1MDB. 1MDB was created by the Malaysian government to promote long-term economic development for the benefit of the Malaysian people.

He added, "In total, 1MDB officials allegedly laundered more than $4.5 billion in funds through a complex web of opaque transactions and fraudulent shell companies with bank accounts in countries ranging from Switzerland and Singapore to Luxembourg and the United States. This is kleptocracy at its worst."

* *Companies more vulnerable to data grabs by law enforcers - See page 10*

NEARLY six in ten Americans believe the United States became more corrupt in 2017, according to a snapshot poll done by Transparency International.

The levels of perceived corruption in government institutions were already high in 2016. US citizens are now more critical of their government's performance in tackling corruption, and expressed concern in a number of areas. The results of the US Corruption Barometer 2017 show:

- 44 percent of Americans believe that corruption is pervasive in the White House, up from 36 percent in 2016.
- 58 percent of people say the level of corruption has risen in the past twelve months, up from 34 percent who said the same in January 2016.
- Almost 7 out of 10 people believe the government is failing to fight corruption, up from half in 2016.
- 55 percent gave fear of retaliation as the main reason not to report corruption, up from 31 percent in 2016.
- 74 percent said ordinary people can make a difference in the fight against corruption, up 4 percentage points from 2016.
- 32 percent believed business executive were corrupt.

Cybercrime

Firms more susceptible to data grabs by law enforcers

Major multinational corporations holding large volumes of client data and those offering cloud computing services are facing the risk of increased demands that they share records with regulators and law enforcers. Countries are preparing to ease and expedite data sharing for criminal investigations with foreign law enforcement authorities, and this can affect emerging markets as much as developed economies. Raghavendra Verma *reports from New Delhi.*

MUTUAL legal assistance treaties (MLAT) provide the standard international mechanism though which countries grant access to the data stored in their jurisdiction to foreign law enforcement authorities.

With major communication service providers such as Facebook, Google, Microsoft and Yahoo located in the US, and the digital economy spreading, the fact is that American law enforcers have great leverage to demand that data on overseas companies and citizens maybe released to their investigators.

But it also offers a treasure trove of data, in a reliable jurisdiction, for law enforcers of other countries. So, corporations are keeping a close eye on moves to make the growing number of requests for international data exchange – to and from the US, more efficient.

Time consuming and laborious

As it stands, MLAT procedures are often very long-winded, time consuming and laborious – a report '*Hitting Refresh – Making India-US Data sharing work',* released by the New Delhi-based Observer Research Foundation (ORF) in August, quoted Indian law enforcement officers as saying that the MLAT system was not built to handle the volume of current requests and is not only broken but is "beyond repair".

Although the number of pending requests under the India-USA MLAT is only in its hundreds, it does not indicate the real demand for electronic data during criminal investigations as officers are discouraged from making these requests owing to the procedural delays and complexities involved, said the ORF report, which is largely based on interviews with law enforcement agencies, communication service providers and policymakers.

The report further said that US recognises the problems with the MLAT process and is therefore negotiating a bilateral data-sharing agreement with the UK that would allow law enforcement agencies of the two counties to request content data directly from firms located in each other's jurisdiction.

To enable such data sharing, the US Department of Justice in 2016 introduced amendments to the Electronic Communications Privacy Act (ECPA) removing the federal warrant requirement for foreign requests, it said.

"Once the US and UK reach an agreement, the Indian government is likely to seek a similar agreement signed with the US," Bedavyasa Mohanty, co-author of the ORF report told *Commercial Crime International*.

Even at 26 percent internet penetration, India's internet user base is already a critical market for many US companies, said the ORF report. As the number of internet users in India increases, Indian law enforcement will become more dependent on American web companies to secure data, it said.

But will privacy protections be respected in emerging market countries such as India if more effective data exchange regimes are created? The UK is certainly looking to create such protections as it talks to the US about a potential new data swap system.

The concern has already been acknowledged in July 2016 by Peter J Kazdik, an assistant attorney general at the US Department of Justice, in a letter to the United States Senate, where he said that the proposed ECPA amendment "would establish a framework and standards that could be used to reach similar agreements with other countries whose laws provide robust protection of human rights, privacy, and other fundamental freedoms."

Data residency

If this succeeds, then governments might be more relaxed about allowing their own data and financial records of local companies and citizens to be stored on clouds, whose servers are in another country. One consequence of current inflexibilities of the existing MLAT process is that many governments force commercial entities to keep data on local servers, just in case regulators and law enforcers need to check it.

India is a case in point. Currently most Indian government organisations and banks require that data is stored on India-based servers and most big Indian companies operate their data centres within the country, said an India-based executive working for a top US-based IT company, who requested anonymity.

"Data residency is a very narrow way of looking at things and could harm Indian businesses," said the executive, adding, "India has the opportunity to become the service centre and data and cloud factory of the world provided it does not insist on strict data localisation."

Continued on page 11/

Fraudster raised $15m from initial coin offering scam

A FRAUDSTER who convinced people to invest in an initial coin offering (ICO) scheme which he claimed would yield a 13-fold profit in less than a month, has been stopped after the United States' Securities and Exchange Commission (SEC) filed charges against the man and his company, PlexCorps.

SEC's complaint, filed in federal court in New York, alleges that the man and PlexCorps marketed and sold securities called PlexCoin on the internet to investors in the US and elsewhere.

He claimed that investments in PlexCoin would yield a 1,354 percent profit in less than 29 days. The SEC also charged his partner in connection with the scheme, which raised up to $15 million from thousands of investors since last August.

The charges are the first filed by the SEC's new Cyber Unit. The unit was created in September to focus the Enforcement Division's cyber-related expertise on misconduct involving distributed ledger technology and ICOs, the spread of false information through electronic and social media, hacking and threats to trading platforms.

Robert Cohen, Chief of the Cyber Unit at SEC said, This first Cyber Unit case hits all of the characteristics of a full-fledged cyber scam and is exactly the kind of misconduct the unit will be pursuing."

The SEC obtained an emergency court order to freeze the assets of PlexCorps, and both the accused.

The SEC charged them both and PlexCorps with violating the anti-fraud provisions, and the man and PlexCorps with violating the registration provision of US federal securities laws.

from page 10 - data grabs by law enforcers

According to the executive, the issues currently under discussion between the government and the Indian IT industry that could relax controls on data localisation include encryption, data access controls and speed of access.

Mr Mohanty said that, as and when a proposed data swap agreement between India and the US comes into place, American companies would be required to set up local mechanisms for data sharing in India to effectively respond to law enforcement requests.

It will also become more important for companies to voluntarily disclose instances of data theft and hacking attacks, which until now they have been reluctant to do to avoid revealing vulnerabilities and to protect their market value and trust, said Mr Mohanty. "Governments may also require reporting of every cyber incident," he said.
"In preparation for that time companies could have to bolster disclosure mechanisms, including liaison officers for law enforcement authorities," he added.

Large and sensitive data handling in itself could become highly complex and problematic. Citing a 2015 case of hacking into the computer networks of the US democratic party national committee, Troy J. Wilkinson, executive vice president of International Consultants & Investigations Inc, in New York told *Commercial Crime International* that anyone who processed that data, whether an outsourced company, third party or even employees at their home, could all potentially come under investigation.

Client confidentiality breaches

Given such a broad dragnet, the handover of data log and computer systems to the authorities during a data breach investigation could be very painful for any company, Navneet Rajan Wasan, a legal consultant and former director general of India's National Investigation Agency told *Commercial Crime International*.

In addition to the disruption caused by such investigations to the normal functioning of businesses, there will be increasing concern among banks and other financial institutions about breaches of client confidentiality as the details of unrelated customer accounts could also be taken away by the investigators, said a senior police office in New Delhi, who requested anonymity.

Under existing Indian law, investigators are only required to seek a certified true copy of the data so that entire business in not brought to a halt, said Mr Wasan.

But what if that changed and actual business operations could be disrupted? "The only thing that you can do is to build your own defence against data breach," he said.

According to Mr Wilkinson, companies need to have an accurate inventory of where their data is stored, and how they are accessing and protecting it.

"It is a major challenge which we need to address though hardware, software and approaches such as policies, procedures and training," he said, "but awareness is key."

Security vulnerabilities in finance sector soars 400%

THE number of security vulnerabilities detected in the financial services sector has increased by over 418 percent in the last four years, according to research from global cyber security and risk mitigation firm NCC Group.

The company analysed vulnerabilities found in 168 financial services organisations using a number of different scanning methods.

The results revealed that the number of security vulnerabilities detected within the sector has increased dramatically in recent years, rising from an average per organisation of 217 in 2013 to 910 in 2016.

Of the issues marked as high and medium risk, 24.7 percent were web application framework vulnerabilities within the software designed to support the development of web applications including web Application Programming Interfaces, services and resources. This number increased almost five-fold since 2013.

David Morgan, NCC Group Executive Principal said, "Although the type of scan used can impact the detection of vulnerabilities in certain categories, the sheer size of the increase in web application framework issues means that the rise can't be entirely attributed to this.

"The sector is increasingly taking a digital-first approach to better engage with customers, and a consequence of this is organisations will be exposed to an increased number of security vulnerabilities, so it's important that they are aware of the risks."

It was found that all of the high and medium risk web application framework vulnerabilities could be fixed by updating the affected platforms or tools. 98.2 percent of these vulnerabilities were mitigated by updating PHP, as the newest versions of the scripting language can mitigate a number of security bugs. Other fixes included updating ASP.net and Apache Tomcat, which are both used to power mission-critical web applications.

Morgan added, "Since they are a frequent target for cyber criminals, financial services companies should be continuously monitoring for vulnerabilities and regularly updating their software, particularly when these tools form the building blocks of what are often business-critical web applications."

Navigation chart now includes cyber risk

THE United Kingdom Hydrographic Office has published a revised edition of the Admiralty Electronic Navigational Charts and Electronic Chart Display and Information System (ECDIS) Maintenance Record (NP133C) that contains new sections to support on board cyber risk management and ECDIS familiarisation.

NP133C now provides guidance to help bridge crews record and manage cyber risks on board.

This update has been developed by UKHO experts in line with guidance published by the International Maritime Organization (IMO), stating that approved safety management systems should consider cyber risk management in line with the ISM code before January 2021.

NP133C has been revised to help mariners achieve this through the documentation of threats and procedures to mitigate risk to ships.

First published in 2014, this publication is designed to help seafarers demonstrate compliance with IMO regulations during Port State Control inspections, with easy to use checklists and templates to record ECDIS annual performance checks and software maintenance.

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