COMMERCIAL CRIME International

May 2020

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

Piracy continues to pose threat amid coronavirus

IN recent weeks there has been much emphasis on the vital role that shipping, and seafarers play in the battle against the deadly Covid-19 pandemic in terms of keeping trade moving.

Quite rightly, seafarers are being recognised as key workers in a key sector, bringing us essential items such as food, medicines and fuel.

However it has also become evidently clear that travel controls imposed due to coronavirus – such as restrictions on crew changes – could start to have a negative impact not only on seafarers financial circumstances and wellbeing, but on the entire shipping supply chain, resulting in import shortages.

ICC International Maritime Bureau (IMB) joins other global shipping organisations in calling for all countries to allow the free movement of seafarers. But it is also reminding the industry not to neglect the problem of piracy which seemingly carries on regardless of the ongoing epidemic.

News agency *AFP* reports that eight crew members of a Singapore-owned container ship are missing and thought to have been kidnapped after it was stormed by pirates off Benin in late April. The incident has been confirmed by the ship's German management firm.

Separately, the US Maritime Administration issued an Alert on 17 April warning that a maritime threat had been reported in the Gulf of Mexico, saying that four piracy incidents had taken place between 4 April and 14 April, involving attacks on offshore support vessels, some of which left crew injured.

IMB's recently released first quarter piracy report further highlights that piracy and armed robbery remains a very real danger to ships' crews as seafarers face continuing threats.

IMB's 24-hour Piracy Reporting Centre (PRC) received a total of 47 attacks in the first three months of 2020, up from 38 in the same period last year. Pirates boarded 37 ships during that period.

Gulf of Guinea hotspot

The Gulf of Guinea remains the world's piracy hotspot. Seventeen crew were kidnapped in three incidents in these waters, at distances of between 45 and 75 nautical miles from the coast.
PRC recorded 21 attacks in the Gulf of Guinea in the first quarter of 2020. Of these, 12 were on vessels underway at an average of 70 nautical miles off the coast.

All vessel types are being targeted, IMB says, adding that the perpetrators are usually armed. They approach in speedboats, boarding ships in order to steal stores or cargo and abduct crew members to demand a ransom.
In the first quarter of this year, four ships were reported being fired at within Nigeria's Exclusive Economic Zone, a worrying trend seeing as the total for last year was 10. This includes a container ship underway around 130 nautical miles southwest of Brass.

In another incident around 102 nautical miles northwest of Sao Tome Island, another container ship was boarded by pirates. The crew retreated into the citadel and raised the alarm. On receiving the alert, PRC liaised with the relevant regional authorities and the vessel operator until the vessel was safe and the crew had emerged from the citadel.

"The IMB PRC commends Regional coastal state response agencies and international navies in the Gulf of Guinea region for actively responding to reported incidents," said Michael Howlett, IMB Director.

With many more attacks going unreported, IMB is advising

Continued on page 2/

In This Issue of CCI

Coronavirus

FIB urges due diligence as PPE scams surface

MEMBERS are being warned of a possible resurgence of 'old-school' buyer and seller frauds surrounding coronavirus equipment.

In recent weeks ICC Financial Investigation Bureau (FIB) has been made aware of the issue of suspect Personal Protective Equipment (PPE) and already there have been several attempts of fraud being perpetrated.

The modus operandi typically involves a company being created or a shelf company used, whose name closely resembles that of a genuine PPE supplier. The unscrupulous sellers will then advertise high stocks of PPE for sale. Payment is by cash in advance normally of between 50 percent and 100 percent. The amounts involved in the transactions that FIB has come across have been above US$10 million, with one for over US$100 million. Shipments are usually from Asia (especially China) to Europe.

Such scams present a real risk to the various parties that possibly could be entangled in these dubious transactions including banks, as fraudsters leverage on the advantage they have, preying on fears over the current shortage and high demand for such equipment.

The Federal Bureau of Investigation for example warns that based on the current stress on the supply chain, scammers may promise equipment they do not have access to in order to capitalise on the medical community's urgent needs, the FBI said. It asks that buyers exercise due diligence and appropriate caution when dealing with any vendors with whom they have never worked and/or of which they have never heard, and when relying on unidentified third-party brokers in the supply chain.
Red-flag that could raise suspicions include; unusual payment terms (for example a 'supplier' asking for upfront payments or proof of payment), last-minute price changes, last-minute excuses for delay in shipment (e.g. claims that the equipment was seized at port or stuck in Customs) and unexplained source of bulk supply.

Similarly, the Organized Crime and Corruption Reporting Project recently detailed how a shipment of one million much-needed medical masks arriving in Romania turned out to be substandard and the middleman company arranging the shipment had links to organised crime.

ICC FIB says the danger is that, given the current urgency and universal demand for PPE supplies, proper due diligence and Know Your Customer (KYC) checks may not be done as thoroughly as usual. There have also been cases in which genuine counterparties have been affected because the intermediaries they use to source the PPE equipment are not credible; in these cases, KYC and Know Your Customers' Customer are hugely important, says FIB.

Members are therefore reminded to carry out proper due diligence, banks should check for proven trading histories in the relevant commodity and should ensure their genuine clients know the technical difficulties in sourcing these cargoes. Continuous Transaction Monitoring is also advised, and any client who is remitting to a first-time beneficiary should also be closely checked.

***FIB carries out checks on behalf of members.** Details here.*

from page 1 - piracy still poses a real risk to seafarers

seafarers in the region to follow the recently published Best Management Practices West Africa – BMP WA. *(This can be found here)*

Call for cooperation

With no sign of a reduction in attacks worldwide, IMB is encouraging shipowners to stay vigilant and is calling for continued international cooperation.

"Navy patrols, onboard security measures, cooperation and transparent information exchange between authorities, are all factors which help address the crimes of piracy and armed robbery," Michael says, adding, that the threat to crew is still real – whether from violent gangs, or opportunistic armed thieves inadvertently coming face-to-face with the crew.

"Ships' masters must continue to follow industry best practice diligently and maintain watches. Early detection of an approaching pirate skiff is often key to avoiding an attack," he says.

Elsewhere in the world

No incidents were reported off Somalia but vessels are urged to continue implementing BMP5 recommended practices while transiting those waters. Somali pirates still maintain the capability for carrying out attacks. Five incidents were reported against ships underway in the Singapore Straits. These were mainly opportunistic in nature however perpetrators were armed with knives.

IMB says that the information sharing cooperation between the Indonesian marine police and PRC continues with positive results. In the first quarter of this year five anchored vessels were boarded.

In Callao anchorage, Peru, one seafarer was taken hostage and two others injured on a reefer ship.

** Go here for more about IMB PRC.*

Europol: criminals adapting to profit from pandemic

EUROPOL has published a report entitled Pandemic Profiteering: how criminals exploit the Covid-19 crisis.

The report provides an overview of how criminals adapt their misdeeds to the Covid-19 pandemic.

It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States' law enforcement authorities in their work.

On fraud the report highlights these case studies involving supply scams. Europol says businesses seeking to purchase supplies such as protective masks and other equipment are being targeted by scammers.

In one case a Member State's investigation focused on the transfer of €6.6 million from a company to another company in Singapore to purchase alcohol gels and FFP2 and FFP3 masks. The goods were never received.

In another case reported by a Member State, a company attempted to purchase 3.85 million masks and lost €300 000. Similar supply scams of sought-after products have been reported by other Member States.

Outlook for fraud

Fraud linked to the current pandemic is likely highly profitable for the criminals involved and they will attempt to capitalise on the anxieties and fears of victims throughout this crisis period. A large number of new or adapted fraud and scam schemes can be expected to emerge over the coming weeks and months with the potential for substantial financial damage to citizens, businesses and public organisations.

Criminals have also adapted investment scams to elicit speculative investments in stocks related to Covid-19 with promises of substantial profits.

The emergence of new fraud schemes and a further increase in the number of victims targeted can be expected. Even when the current crisis ends, criminals are likely to adapt fraud schemes in order to exploit the post-pandemic situation.

When it comes to cybercrime, the key findings from the Europol report include;

* Criminals have used the Covid-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC).

* There is a long list of cyber-attacks against organisations and individuals, including phishing campaigns that distribute malware via malicious links and attachments, and execute malware and ransomware attacks that aim to profit from the global health concern.

* The pandemic has an impact on Darkweb operations. Certain illicit goods will become more expensive, as source materials become unavailable. Vendors on the Darkweb offer special corona goods (scam material) at discounts.

Outlook for cybercrime

The number of cyber-attacks is significant and expected to increase further. Cybercriminals will continue to innovate in the deployment of various malware and ransomware packages themed around the COVID-19 pandemic. They may expand their activities to include other types of online attacks.

Cybercriminals are likely to seek to exploit an increasing number of attack vectors as a greater number of employers adopt telework and allow connections to their organisations' systems.

* *The report can be downloaded via this link.*

EU Fraud Office actively pursuing cases amid crisis

THE European Anti-Fraud Office (OLAF) has said that it remains fully operational and committed to fighting fraud in order to protect the financial and other interests of the European Union, and its citizens amid coronavirus.

It said that since March 16;

- 48 new selection cases were opened based on information of investigative interest.
- 82 selections were closed resulting in 23 new investigations, in five coordination cases and in 54 dismissed cases. During the first three months of 2020, OLAF opened a total of 104 new investigations, which is a historical record.
- 19 investigations were completed, out of which 12 were closed with recommendations to relevant authorities.
- Two coordination cases were concluded.
- In a fast-track procedure, OLAF developed specific rules for conducting interviews during times when travelling is not recommended.

On March 19, OLAF launched coordination activities spanning the world, where together with international customs authorities OLAF actively counters the illicit traffic of counterfeit products used in the fight against the Covid-19 infection. The investigation already discovered illicit trade in masks, medical devices, disinfectants, sanitisers and test kits

Coronavirus

Gard urges shipowners to be cyber alert

MARITIME insurer Gard is asking shipowners to stay cyber alert and avoid all Covid-19 phishing expeditions.

In an article on its website, Gard said that to cope with operational and crewing issues such as denied physical access, quarantined vessels and travel restrictions, shipowners are now actively opening for remote access and implementing remote digital survey tools towards vessels and encouraging shore staff to work remotely from home.

There is also increased use of mobile devices to access operational systems onboard vessels and core business systems in the company.

Unprotected devices could lead to the loss of data, privacy breaches, and systems being held at ransom. Data is an asset and protecting it requires a good balance between confidentiality, integrity and availability.

Shipowners can stay alert by;

⇒ Exercising caution in handling any email with a Covid-19 related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to Covid-19.

⇒ Using trusted sources - such as legitimate, government websites for up-to-date, fact-based information about cyber security and Covid-19.

⇒ Not revealing personal or financial information in email, and do not respond to email solicitations for this information.

⇒ Remembering to disconnect or close temporary remote access given to any external party after finishing the job.

"Our recommendation is to take a holistic approach to the cyber risks to protect the confidentiality, integrity and accessibility of both IT and OT systems through measures covering processes, technology and most importantly people," Gard said, adding that the easiest and most common way for cyber criminals to gain access, is through negligent or poorly trained individuals.

It has put forward these recommendations;.

- Focus on policies, procedures and risk assessments.
- Ensure that system design and configuration are safe and fully understood and followed.
- Provide proper onboard awareness and training.

* The full set of recommendations and more resources can be found here.

~ *Source: Gard*

THE Australian Transaction Reports and Analysis Centre (AUSTRAC) and its law enforcement and national intelligence partners are monitoring and preparing for a shift in the risks that criminals may pose to the financial system and the community.

They are encouraging reporting entities to monitor for new and emerging threats and submit suspicious matter reports (SMRs) to AUSTRAC because submitting high-quality, accurate and timely SMRs provides the best chance to detect, deter and disrupt criminal activity.

AUSTRAC has identified areas of criminal exploitation where the financial system may be more vulnerable during the Covid-19 pandemic. These include:

1. Targeting of government assistance programmes through fraudulent applications and phishing scams.
2. Movement of large amounts of cash following the purchase or sale of illegal or stockpiled goods.
3. Out of character purchases of precious metals and gold bullion.
4. Exploitation of workers or trafficking of vulnerable persons in the community.

Reporting entities have also been asked to share with AUSTRAC any significant shifts they observe in relation to financial crime and fraud monitoring, so these can be disseminated wider industry.

Fraud.org warns of tsunami of coronavirus scams

UNITED STATES based Fraud.org has warned about the coming coronavirus scam 'tsunami' saying that robocalls and stimulus cheque scams are two forms of fraud expected to increase due to the pandemic.

It says YouMail, a cloud-based telecommunications provider that tracks robocall volumes, estimates that at least one million robocalls per day are inundating Americans' mobile phones.

Fraudulent robocallers are offering air duct sanitation services, work-from-home opportunities, cut-rate health insurance, and immune-system boosting nutritional supplements. Yet others have reportedly offered free insulin kits to diabetics, along with free coronavirus testing kits.

Stimulus cheque scams that have been reported involve crooks promising to expedite payment in exchange for a fee, impersonating a government official, and requesting sensitive personal information in order to process a cheque.

FAFT encouraging digital onboarding and data sharing

THE Financial Action Task Force (FATF) is encouraging governments to work with financial institutions and other businesses to use the flexibility built into the FATF's risk-based approach to address the challenges posed by Covid-19 whilst remaining alert to new and emerging illicit finance risks.

It is urging the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures.

"The continued implementation of the FATF Standards facilitates integrity and security of the global payments system during and after the pandemic through legitimate and transparent channels with appropriate levels of risk-based due diligence," FAFT President Xiangmin Liu said in a statement.

Addressing Covid-19-related financial crime risks by remaining vigilant.

FAFT says supervisors, financial intelligence units and law enforcement agencies should continue to share information with the private sector to prioritise and address key money laundering (ML) risks, particularly those related to fraud, and terrorist financing (TF) risks linked to Covid-19.

Additionally, criminals and terrorists may seek to exploit gaps and weaknesses in national anti-money laundering/counter-financing of terrorism (AML/CFT) systems while they assume resources are focused elsewhere, making risk-based supervision and enforcement activity more critical than ever.

Financial institutions and other businesses should remain vigilant to emerging ML and TF risks and ensure that they continue to effectively mitigate these risks and are able to detect and report suspicious activity.

Criminals are taking advantage of the Covid-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears.

Malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims are likely to increase, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about Covid-19.

National authorities and international bodies are alerting citizens and businesses of these scams, which include impostor, investment and product scams, as well as insider trading in relation to Covid-19. Like criminals, terrorists may also exploit these opportunities to raise funds.

Digital onboarding and simplified due diligence

FAFT is also advocating digital onboarding to reduce the risk of spreading the virus.

With people around the world facing confinement or strict social distancing measures, in-person banking and access to other financial services is difficult, and unnecessarily exposes people to the risk of infection.

As such, FAFT says the use of financial technology (Fintech) provides significant opportunities to manage some of the issues presented by Covid-19. In line with the FATF Standards, the FATF encourages the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible.

When financial institutions or other businesses identify lower ML/TF risks, the FATF Standards allow them to take simplified due diligence measures, which may help them adapt to the current situation.

The FATF encourages countries and financial service providers to explore the appropriate use of simplified measures to facilitate the delivery of government benefits in response to the pandemic.

Delivery of aid through non-profit organisations

When it comes to charities and non-profit organisations (NPOs) FAFT said it is important to recognise that FATF Standards do not require that all NPOs be considered high-risk and that most NPOs carry little or no TF risk.

"The aim of the FATF Standards is not to prevent all financial transactions with jurisdictions where there may be high ML/TF risks, but rather to ensure these are done through legitimate and transparent channels and money reaches its legitimate intended recipient.

"National authorities and financial institutions should apply a risk-based approach to ensure that legitimate NPO activity is not unnecessarily delayed, disrupted or discouraged," FAFT said.

Ongoing outreach and advice

Regulators, supervisors, financial intelligence units, law enforcement authorities and other relevant agencies can provide support, guidance and assistance for the private sector on how national AML/CFT laws and regulations will be applied during the current crisis.

Continued on page 6/

Coronavirus

British insurers warn of bogus products and ghost brokers

FRAUDSTERS looking to make quick money from the current pandemic could offer bogus insurance products and high-risk investment and pension products and the Association of British Insurers (ABI) is warning people to be on their guard.

ABI is urging consumers and businesses to be aware of these scams:

- Robocalls or automated texts that falsely claim to be legitimate, mainstream insurance companies. They may claim, for a fee, they can help recover losses by submitting a claim, for the cost of a holiday or event such as a wedding cancelled due to coronavirus.
- Pension and investment scams, which might claim that they will guarantee higher returns than current savings.
- Cold calls about people's pension. It is illegal for firms to contact people out of the blue about their pension. The caller may offer to help people access their pension before age 55, or offer a "free pensions review".
- Phishing emails. These attempt to trick people into opening malicious attachments or reveal personal or financial information.
- Ghost brokers. Fraudsters may attempt to use an insurer's branding to promote and sell fake or invalid insurance products, including products such as travel and business interruption which may claim to offer Covid-19 protection.
- False insurance cancellation. Callers will say people's insurance has been cancelled and they promise to reinstate it if they pay an additional fee over the phone.

FBI forecasts rise in Covid-19 BEC schemes

THE Federal Bureau of Investigation (FBI) is anticipating a rise in Business Email Compromise schemes related to the Covid-19 pandemic.

Recent examples of such BEC attempts include:
1. A financial institution received an email allegedly from the CEO of a company, who had previously scheduled a transfer of US$1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email address with only one letter changed.

2. A bank customer was emailed by someone claiming to be one of the customer's clients in China. The client requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus audits." The victim sent several wires to the new bank account for a significant loss before discovering the fraud.

As of April 21, 2020, the FBI's Internet Crime Complaint Center has received and reviewed more than 3,600 complaints related to Covid-19 scams, according to a Department of Justice statement.

The FBI is also seeing a rise in fraud schemes, specifically fake emails purportedly from the Centers for Disease Control and Prevention (CDC) or other organisations claiming to offer information on the virus.

Other popular tricks involve criminals sending phishing emails asking people to verify their personal information in order to receive an economic stimulus check from the government and phishing emails related to charitable contributions, general financial relief, airline carrier refunds, fake cures and vaccines and fake testing kits. Scammers are also approaching people selling products that claim to prevent, treat, diagnose, or cure Covid-19 such as sanitising products and Personal Protective Equipment.

Additionally, the FBI warns of fraudsters using ordinary people as money mules during the pandemic. Two areas that the FBI is advising people to be on the lookout for are; work-from-home schemes and online job postings and emails from individuals promising easy money for little to no effort.

Common red flags include; (1) People are asked to receive funds in their personal bank account and then "process" or "transfer" funds via wire transfer, mail, or money service businesses, such as Western Union or MoneyGram and, (2) people are asked to open bank accounts in their name for a business.

from page 5 - FAFT

Such guidance can give financial institutions and other businesses reassurance that the authorities share their understanding of challenges and risks involved in the current situation, and of the appropriate actions to take.

Authorities in some countries have already taken swift action and provided this type of advice. Mechanisms by which victims, financial institutions, and other businesses can report Covid-19 related fraud may be especially useful.

At the international level, the FATF is working with the Committee on Payment and Market Infrastructures and the World Bank to help ensure coordinated policy responses for the continued provision of critical payment services against the backdrop of the Covid-19 crisis.

European Commission urged to recover €3m from fraud case

FOLLOWING the closure of a carefully coordinated investigation into suspected fraud committed by a Dutch company in Mauritania this January, European Anti-Fraud Office (OLAF) recommended that the European Commission undertake appropriate measures to recover a total of €3.07m.

The Dutch Fiscal Information and Investigation Service (FIOD) contacted the European Anti-Fraud Office (OLAF) in April 2016 concerning a Dutch company, which was under investigation for tax evasion.

The company had won a large EU-funded contract managed by the Mauritanian authorities for the removal of 57 shipwrecks from the Bay of Nouadhibou in Mauritania. Based on the information provided by FIOD, OLAF suspected that the company had defrauded the European Union budget as well.

OLAF worked closely with the FIOD and the Dutch prosecution service, carrying out on-the-spot checks, interviewing witnesses, and analysing a large amount of technical data. In addition to the Dutch company at the centre of the fraud, a number of additional persons concerned were identified, including Mauritanian officials.

OLAF's investigation established three main findings; a breach of the procurement procedures, a violation of the rules on subcontracting, and strong indications of the active corruption of two Mauritanian officials.

OLAF concluded the investigation on January 7 2020, issuing recommendations to the European Commission to recuperate €3,068,000 and to the Dutch authorities to prosecute the suspected fraudsters.

OLAF also recommended that the European Commission should flag the Dutch company in the Commission's Early Detection and Exclusion System (EDES), which would exclude the company from possible access to European taxpayers' money.

Company director defrauded 5 banks

A COMPANY director in Hong Kong has admitted in court to defrauding five banks of 33 loans totalling about HK$25 million and banking facilities totalling HK$22.5 million, as well as deceiving a government department and a public body into acting as guarantors for loans and trade facilities totalling HK$15.8 million granted by the banks.

The case arose from a corruption complaint investigated by Hong Kong's Independent Commission Against Corruption (ICAC).
The offences occurred between February 2010 and February 2013.

The company was set up purportedly for the purpose of trading audio equipment.

The defendant conspired with another to defraud the banks by dishonestly falsely representing that supporting documents submitted by the company in relation to its applications of banking facilities were genuine, causing the four banks to grant banking facilities totalling HK$22.5 million.

The defendant also convinced Hong Kong's Trade and Industry Department (TID) Ng into providing the company with various loan guarantees through a scheme it offered.

Dallas woman sentenced

A WOMAN in Dallas Untied States was sentenced via video teleconference to 46 months in jail for her role in a US$1.4 million real estate title insurance scheme.

She was a former employee of a real estate title company and admitted to fraudulently transferring more than $1.4 million from her employer's escrow accounts into bank accounts belonging to her co-conspirator.

Between 2002 and 2007, she initiated at least 51 wire transfers and wrote 11 cheques.

THE European Union Intellectual Property Office (EUIPO) has issued an alert about a new misleading invoice in circulation, which takes the form of a fake EUIPO decision.

The misleading invoice, which can be viewed here, has been reported to the Office by users.

This latest misleading invoice uses the EUIPO's logo, name, acronym and letterhead, and purports to be a decision signed by the Office.

It is mailed to users from Madrid, Spain, and includes a demand for a "registration fee" to be transferred to a Polish bank account with a PL IBAN prefix.

The EUIPO has contacted the relevant Polish banks and has lodged a criminal complaint with the Office of the Public Prosecutor in Warsaw, Poland. A criminal investigation is now pending.

Nevertheless, many of these invoices may still be in circulation, EUIPO says.

United Kingdom: Understanding fraud and regulation

UK Finance reported that in 2018 alone, criminals successfully stole £1.2 billion through fraud and scams in the United Kingdom.

The organisation has published an article on its website written by Marc Docherty, Head of UK Acquiring, Ingenico Enterprise Retail.

There are hundreds of different fraud tactics out there; here are those that tend to be most prevalent.

False claims

This type of fraud occurs when a consumer makes an online shopping purchase with their own credit card, but then requests the money back from the issuing bank after receiving the purchased goods or services. This is commonly called a chargeback and can often occur unknowingly, such as if a child buys credits for a game using their parents' linked credit card without the parent realising. However, it is also often done with malicious intent.

Data breaches

If a company's network lacks adequate security, this leaves its systems wide open to a data breach. This is when criminals gain unauthorised access to a whole host of information, including sensitive business information and personal customer data including bank details, passwords, addresses and more. Stolen customer personal and financial data is typically sold on to fraudsters who then use the information for making purchases, taking over accounts and applying for credit.

Phishing

Phishing is the process by which fraudsters obtain customers' private details by masquerading as a legitimate company. For example, a fraudster sends an email convincing the recipient that it's from a retailer they frequently shop with. The consumer follows the directions to click a link and fill out the details 'necessary to continue shopping with the retailer' or similar. The fraudster then harvests these details to either commit identity fraud or simply take the money directly from the victim's account.

The risks

The main risk businesses consider when they think 'fraud' is financial. If a company is out of line with regulations and suffers a data breach, for example, they can be fined up to £17.5 million. If merchants don't keep a check on false claims, they can lose out on money as well as stock. Furthermore, fraud doesn't only affect businesses financially. If companies are associated with data breaches or poor fraud prevention management, they risk damaging their reputation.

A note on regulation

One of the most recent security measures, the General Data Protection Regulation (GDPR), came into force in May 2018 to tighten up the processing of personal data.

As is often the case when new regulations are implemented, businesses were at first worried about how this may impact their operations, but over time and with the help of experts, these fears were alleviated. Thanks to GDPR, consumers now enjoy greater trust in merchants when they shop online.

In terms of payments, some other important regulations to understand are the Second Payments Services Directive (PSD2) and Strong Customer Authentication (SCA). PSD2 has improved customer rights, enhanced security through SCA, and provided a framework for new payment and account services by enabling third-party access to account information. Meanwhile SCA itself has increased security by enforcing extra authentication measures at checkout.

How merchants can act.

⇒ Learn
As a merchant, take time to understand the latest regulations and fraud practices as best as you can, reading expert blogs and following industry-specific news publications.

⇒ Educate
Warning them against current fraud practices like phishing, for example, will reduce their risk of falling victim to scams of this nature. Similarly, letting them know any updates to expect in terms of fraud prevention or regulation can contribute to a seamless user experience. For example, SCA's Two Factor Authentication policy has been seen to flummox customers, leading them to abandon online shopping baskets. User experience issues such as this can be avoided by communicating with your clients.

⇒ Act
Make sure to implement measures earlier rather than later. The best way to combat fraud and related issues is to hand over to a professional who can advise on and implement the best course for your business. Although fraud is complicated, a secure payments system backed by a team of experts is an essential step to helping prevent fraud and optimising business operations.

~ Source: UK Finance

Fewer cases involving bribery of foreign officials reported

THE number of global and United States enforcement cases involving bribery of foreign officials dropped in 2019, with a 19 percent decrease in US enforcement actions and a 45 percent decrease in non-US enforcement actions.

These were some of the findings contained in the 2019 Global Enforcement Report, compiled by TRACE.

The report, TRACE's tenth annual compilation, provides anti-bribery enforcement data from 2019 and summarizes 43 years of anti-bribery enforcement activity.

"While 2019 saw a decrease in transnational anti-bribery enforcement actions, the trends are not out of line with fluctuations we have seen in the past," TRACE President Alexandra Wrage said.

"The record-setting Airbus settlement in January makes it clear that the risk of very substantial penalties for companies that don't take compliance seriously remains real," he added.

Companies in the extractive industries faced the most investigations globally in 2019.

There was also an increase in US investigations into bribery of foreign officials in the aerospace, defence and security industries.

China again had the highest prevalence of alleged bribery by foreign companies, with Chinese officials being the alleged recipients of bribes in more than 110 enforcement events since 1977. Iraq has the next-highest number of enforcement events, followed by Brazil.

"Governments that invest in anti-bribery enforcement will continue to lead in shaping the global anti-corruption landscape," Wrage said, adding, "We anticipate continued international cooperation between enforcement authorities, who are sending a consistent message that corruption will not be tolerated."

TRACE's key findings and the entire Global Enforcement Report can be found at www.traceinternational.org

Ex financial controller jailed for corruption

A former financial controller of a listed company, charged by Hong Kong's Independent Commission Against Corruption (ICAC) has been sentenced to three years and seven months' imprisonment for conspiracy to accept an illegal rebate of about HK$590,000 for engaging an accounting firm to provide services, and defrauding the listed company of over HK$2 million by outsourcing other services to a consultant firm owned by him.

The court heard that at the material time, the defendant was the financial controller and company secretary of Southeast Asia Properties, handling all accounting and financial matters of Southeast Asia Properties and its subsidiaries.

In May 2015, Southeast Asia Properties resolved to acquire a company at a consideration of over HK$336 million. The defendant suggested outsourcing the preparation work to an independent third party. The proposal was agreed by Southeast Asia Properties.

The defendant then outsourced the internal control review, taxation, financial advisory and consultancy services in relation to the acquisition to an accounting firm.

Between May 2015 and June 2016, Southeast Asia Properties and its subsidiaries released payments totalling HK$754,000 to the accounting firm for its services. Out of that amount, about hk$590,000 was eventually transferred to the defendant's bank account while the remaining sum was retained by the accounting firm.

In June 2015, the defendant set up Wishful Bright Enterprise Consultancy Limited (Wishful Bright), of which he was its sole director cum shareholder.

Without disclosing his interest in Wishful Bright and obtaining quotations from other contractors, the defendant caused Southeast Asia Properties and its subsidiaries to engage Wishful Bright to provide various accounting, taxation, research, financial advisory and consultancy services between June 2015 and October 2016.

As the head of Southeast Asia Properties' accounts department, the defendant endorsed and approved the payments of 15 invoices issued by Wishful Bright. As a result, a total of over HK$2 million was released to Wishful Bright.

Had Southeast Asia Properties known that the defendant was the director of Wishful Bright or held any interest in it, Southeast Asia Properties would not have engaged Wishful Bright to provide those services and settled the payments.

Southeast Asia Properties had rendered full assistance to the ICAC during its investigation into the case.

What does the future hold for global cyber legislation?

HOW will cyber legislation change in the next decade?

Kat Sommer, NCC Group head of public affairs, explores why collaboration is crucial when it comes to the future of cyber security law around the world.

As the level of connectivity around the world increases, so does the associated level of risk. Governments have become increasingly aware of this over the last decade, and we've seen cyber security placed firmly on the legislative agenda as a result.

The scope and definition of cyber security has also evolved rapidly. From the protection of personally identifiable information (PII) to securing critical national infrastructure, there are many facets of security for governments to cover – a number that is only likely to increase in the future.

Already, a complex network of rules and regulations spanning jurisdictions around the world has been woven, and this will serve as the baseline for the future. We've taken a look at some of the legislation in place today, and while this is by no means a comprehensive review, looking beyond our own borders at how other nations have addressed the shared challenge of cyber security could give us a glimpse of what the future could hold for global cyber legislation.

What does cyber legislation around the world currently look like?

Cyber legislation varies significantly between countries, shaped by their political systems, and culture, as well as their pace of digitisation and internet penetration. For example, African countries devising cybercrime legislation now are able to leapfrog a lot of the iterative approaches European countries have taken, and develop a more modern framework from the outset.

However, perhaps unsurprisingly when faced with similar challenges, there are shared themes across individual jurisdictions' approaches to cyber legislation. Many governments are focusing on driving collaboration between policymakers, academia and the cyber security industry itself.

While consensus has seemingly been reached that leaving cyber resilience to market forces will not deliver the right outcomes, debate on the extent to which government intervention is required continues.

This includes discussion on whether advice and guidance will suffice, or whether incentives to encourage desired behaviours could prove more effective than enforceable and sanctionable rules.

In light of often limited public sector resources and capacity, a considered approach needs to be taken when deciding on the areas in which government action can make the biggest difference, and where partnerships, or trusting the private and third sectors to pick up the slack, will offer the best value for money.

In the UK specifically, one significant driver of collaboration between industry, academia and government has been the establishment of the National Cyber Security Centre (NCSC) in 2016.

By providing accessible advice, research and expertise, the NCSC now serves as a one-stop-shop for citizens, businesses, public sector and SMEs in the UK that are looking for cyber security guidance, as well as the clear technical authority to manage cyber incidents and offer advice to policymakers.

We have also seen cross-border collaboration increase in the past years, with the introduction of more data and security requirements that flow down from European level, such as the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive.

There is also a question of the role of the cyber security industry in tackling emerging cyber threats. The Netherlands has a more unique approach to vulnerability disclosure, helping to mitigate common issues around the discovery, reporting and resolution of vulnerabilities.

One example is the introduction of prosecutorial guidelines to safeguard security researchers better from criminal prosecution where they are acting in good faith.

We have also seen an increasingly robust approach to building business resilience in many parts of the world. For example, the Australian government has introduced the ASX 100 health check, which offers companies a baseline to assess themselves against, a model which has been replicated around the world.

In other countries, industry-specific advice and regulation is on the rise. For example, in the US, sectors such as aviation and healthcare benefit from specific security advice, which cover issues from how the government tackles cyber espionage to advice from the FDA for manufacturers of medical devices.

What does the future hold?

In a rapidly changing global cyber landscape, one thing is clear – there is no such thing as one 'right' approach to cyber security.

Continued on page 11/

Cyber trading crime group dismantled

WITH the support of Eurojust, authorities in Austria, Bulgaria, Germany and Serbia have successfully carried out operations against two organised criminal groups (OCGs) suspected of large-scale investment fraud in cyber-trading.

Despite the challenges of the current coronavirus crisis, an action day took place on 2 April, with all participants adhering to the measures imposed to prevent further contagion.

Four suspects were arrested in Bulgaria. In Germany, €2.5 million were frozen on the bank account of a company involved in the fraud scheme.

Serbian authorities arrested five suspects and searched nine places, seizing five apartments, three cars, a considerable amount of cash, and IT equipment.

Additionally, more than 30 bank accounts were put under surveillance. Based on the information gathered during the action day, authorities engaged in another operation against a company in Belgrade on 4 April, arresting one suspect and seizing servers, other IT equipment, and documents.

The OCGs lured thousands of victims in several countries into investing in non-existent financial products. Throughout Europe, advertising banners and mass emails promising above-average profits encouraged investors to register on unlicensed online trading platforms for a €250 fee.

They were then contacted by so-called agents or brokers operating from call centres who announced the opportunity of even higher profits, seducing victims into transferring more money to various accounts or releasing the debiting of additional amounts from their credit cards.

Subsequently, the perpetrators simulated the alleged trading of financial products, misguiding the victims with fake positive outcomes displayed on the online trading platforms. In reality, no actual trading took place.

Instead, the money was distributed to a large number of participants in a complex money laundering network installed across Europe. The companies at the end of this chain were under the control of the criminals, allowing them to withdraw the funds for themselves.

Thousands of investors suffered a complete loss of their money. In Germany, for example, the Bavarian Central Office for the Prosecution of Cybercrime at the Bamberg General Prosecutor's Office registered hundreds of victims and damages exceeding €10 million.

In Austria, the Central Prosecutor's Office for Combatting Economic Crime and Corruption reported around 850 victims, with presumed damages of at least €2.2 million.

The total damage caused by the OCGs exceeds these figures, given that the perpetrators targeted people in numerous countries in Europe and beyond.

Furthermore, investigators assume a high number of unreported cases, since many investors may have mistakenly considered their losses a result of the high risks associated with the trading of certain financial products.

From page 10

Watch out for online Covid-19 scams

However, as cyber security threats and defensive capabilities continue to evolve over the next decade, it's important that governments and businesses share knowledge and experiences even more openly.

By encouraging more cross-border collaboration between governments, businesses and the cyber security industry, global cyber legislation can be kept as up to date as possible and ultimately keep our global society safer.

THE National Insurance Crime Bureau (NICB) and the Cybercrime Support Network (CSN) are partnering to educate online users about scams surrounding Covid-19, and what consumers need to watch out for when surfing the web, working online, or e-learning from home.

They are advising people who believe they have been victimised by online coronavirus scams, to first notify their bank or financial institution about the theft of your personal data. They should also run a credit report and check for any unusual activity and if they notice a change, to freeze their credit with Equifax, Experian, or TransUnion.

The organisations have published the COVID-19 NICB Resource Center, which is a comprehensive web page that highlights national and state resources that are available to identify and fight the insurance fraud that is sure to come as a result of this crisis.

~ *Source: NCC Group*

Consultation paper published

A CONSULTATION report on Effective Practices for Cyber Incident Response and Recovery, has been published by The Financial Stability Board (FSB) and sent to G20 Finance Ministers and Central Bank Governors.

The toolkit of effective practices aims to assist financial institutions in their cyber incident response and recovery activities.

FSB says efficient and effective response to and recovery from a cyber incident by organisations in the financial ecosystem are essential to limiting any related financial stability risks.

Such risks could arise, for example, from interconnected information technology systems between multiple financial institutions or between financial institutions and third-party service providers, from loss of confidence in a major financial institution or group of financial institutions, or from impacts on capital arising from losses due to the incident.

The toolkit lists 46 effective practices, structured across seven components:

Governance - frames how cyber incident and recovery is organised and managed.

Preparation – to establish and maintain capabilities to respond to cyber incidents, and to restore critical functions, processes, activities, systems and data affected by cyber incidents to normal operations.

Analysis – to ensure effective response and recovery activities, including forensic analysis, and to determine the severity, impact and root cause of the cyber incident to drive appropriate response and recovery activities.

Mitigation – to prevent the aggravation of the situation and eradicates cyber threats in a timely manner to alleviate their impact on business operations and services.

Restoration – to repair and restore systems or assets affected by a cyber incident to safely resume business-as-usual delivery of impacted services.

Improvement – to establish processes to improve response and recovery capabilities through lessons learnt from past cyber incidents and from proactive tools, such as tabletop exercises, tests and drills.

Coordination and communication – to coordinate with stakeholders to maintain good cyber situational awareness and enhances the cyber resilience of the ecosystem.

The FSB welcomes comments and responses to the questions set out in the consultation report, by 20July 2020. The final toolkit, taking on board the feedback from this public consultation, will be sent to the October G20 Finance Ministers and Central Bank Governors meeting and published. ~ *The consultation report can be found here.*

Phishing persists

PHISHING attacks are not going away, according to recent research conducted by NCC Group.

The cyber security and risk mitigation company analysed 1,300 phishing campaigns from its phishing simulation service, Piranha, used to help our customers learn more about phishing attempts.

A total of 360,000 emails were analysed, which contained a fake link where users were asked to submit their credentials.

Some of the main findings included:

- Charities, IT services, and local public sector had the highest click rate.
- Retail, health, and financial services had the lowest click rate.
- Once clicking through, half of all targets were likely to supply credentials, regardless of sector.

Apart from the surprising finding that users from IT services had a high click rate, NCC Group's research showed that phishing attempts are becoming more sophisticated, and highlights how it's not so easy to spot them.
* *See the research here.*

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