COMMERCIAL CRIME International

June 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

India: raise loan underwriting standards to mitigate risks

LOAN underwriting standards must be raised to improve credit decisions and mitigate the risk of future wilful defaults arising, international fraud and asset recovery experts have emphasised.

Furthermore, bankers should be incentivised to recover assets, and the psychological and moral hazards of not holding banks accountable for their poor credit decisions should be removed from the equation when attempting to restore value from toxic debt.

The experts made this call in a candid presentation called '*Achieving Justice Against Wilful Defaulters in India - The Need for a Well-Coordinated Approach by Parliament, Law Enforcement and Banks'* during ICC FraudNet's meeting in Mumbai in April.

The panel said loan accounts that are in wilful default should be realistically valued or, if necessary, disposed of to an Asset Reconstruction Company (ARC) that will likely seek to enforce the obligation to pay.

Indian banks have had provision for US$100bn toxic debt to date. This figure is rising.

Also, a model to compel repayment of non-performing loans by using private sector asset recovery professionals to trace, discover, freeze and recover assets of wilful defaulters must be either; properly budgeted and funded internally or, where legally permissible, outsourced to asset recovery specialists who will absorb the risk of recovery in exchange for a success fee.

One suggestion for banks to address the problem of wilful default, was that they sell their stressed debt on a deeply discounted basis to hedge funds and other investors.

"While this approach may provide an immediate stop-gap measure to clean-up the banks' balance sheets, it will not change the culture of appeasement towards fraud because the responsible parties will be less likely to be held fully accountable," the panel said.

"A better alternative to selling loans on a deeply discounted basis to hedge funds may be to build and capitalise a 'bad bank' – which is a model that has been used with success in France, the US and elsewhere.

"A 'bad bank' is used to clean-up the balance sheets of existing banks; and as a platform from which to forcefully attack recalcitrant borrowers and promoters with sufficient specialist human and financial resources to be effective."

There is no quick remedy to fix a problem of this scale and complexity. Any solution must be built on a long term and aggressive loan enforcement strategy backed by the legislature, law enforcement agencies and private professionals acting on behalf of the banks themselves.

"This starts with a rejection of the status quo. Repeating the same approach repeatedly without success and expecting a different result is unhelpful.

"Wilful default is not a problem unique to India. Other countries' experiences in confronting financial crime and creditor fraud demonstrates that it is a problem that can be addressed successfully.

"There is a myriad of ways in which assets dishonestly concealed or retained by borrowers can be (and in other jurisdictions are) tracked, frozen and recovered with the use of modern cross-border asset recovery tools and experts," the panel said.

This technology has been in use for

Continued on page 3/

In This Issue of CCI

India wilful default potentially catastrophic to financial system

THE rules governing the compulsory disclosure of documents and bank and accounting records of an insolvent debtor currently within the Indian Bankruptcy Code 2016 should be simplified to be effective in countering wilful default.

Adjudicating Authorities must have the jurisdiction to grant extraordinary pre-emptive or *ex parte* disclosure orders on the application of insolvency resolution professionals and against third party holders of banking and asset and company ownership information (such as banks, law firms and accountants) wrapped in ancillary secrecy or gagging injunctions (sometimes called 'super injunctions' under English law). "This is the single most important and devastatingly effective tool to ferret out concealed assets and to gather objective evidence of their attribution to wrongdoers or victim insolvent companies," says ICC FraudNet member Martin Kenney, who is Managing Partner, Martin Kenney & Co, Solicitors (British Virgin Islands).

"However, a standard of review must be articulated for their availability in the interests of fairness and the protection to the right to privacy over confidential and private information enjoyed by all law-abiding people. I propose that the legal standard be a showing on the part of an applicant insolvency resolution professional of a good arguable case of a risk of asset flight on the part of a target of an asset recovery or corporate malfeasance inquiry. This is the same standard imposed on applicants for freeze orders under English law," he added.

Kenney, who was a panellist at ICC FraudNet's recent meeting in Mumbai, said the problem of wilful default within the Indian financial sector is severe and pervasive. "The true measure of the size of the problem sitting on bank balance sheets is unknown. It is a dark number. So far, US$100bn of non-performing loan have had to be provisioned for by the banks. The real figure is probably much greater than this." The consequences to the Indian financial system and to the Indian economy from this phenomenon are potentially catastrophic."

Kenney said finding credible numbers measuring the size of the problem of wilful default in the country was problematic. In February the media reported that banks had reported $9bn of wilful default loans. That was one week before the Nirav Modi disaster was announced, adding US$1.17bn to that figure. There are other reported estimates in the business press of US$120bn; and one at US$200bn.

"I have seen this before in other settings. The savings and loan crisis in America in the 1980's. Japan in the 1990's. Russia in the late 1990's. Cyprus about three years ago. And elsewhere," says Kenney. "Banks are extremely reticent to fess up to the real size of the problem as they then have to raise more capital or go bust. A lot of toxic debt goes hidden for a long time, increasing the risk of a huge and sudden implosion of the system. We are truly dealing with a dark number in India," he added.

In late April, India's Cabinet approved the Fugitive Economic Offenders Ordinance 2018 that provides for confiscating properties of corporate escapees. Under the new Bill, properties within or outside India may be subject to seizure or confiscation by the Central Bureau of Investigation or the Enforcement Directorate. Kenney said the problem of wilful default in India has grown in magnitude to the point where it is now imperative that it be tackled meaningfully. "When a culture of tolerance towards wilful default is allowed to permeate, banks must be rescued by the State to protect the savings of depositors. Government is therefore forced to intervene and recapitalise banks at a substantial cost to the public Exchequer. "To resolve this existential economic challenge, it is imperative that the culture of appeasement towards wilful defaulters be rejected. It is also important from both moral and financial perspectives that, when India tackles its wilful defaulters, it is done in a manner that is sustainable."

A multi-track approach to tackling wilful defaulters is advocated thus: (a) The Government of India must act, through its legislature, to provide a legal framework capable of supporting a credible and robust financial system, supported by capable and competent organisations;

(b) Robust law enforcement action should be taken to investigate the activities of wilful defaulters across national boundaries if necessary; successfully extradite economic fugitives who have fled India; and prosecute offenders for taking by deception or other economic crimes, and at the same time; and,

(c) Pre-emptive asset recovery measures should be undertaken by private sector specialists acting for Indian creditors or insolvency office holders and with the assistance of Courts in multiple jurisdictions to secretly trace, locate, freeze and recover the assets of a dishonest borrower, guarantor or promoter.

**This is an extract from the panel presentation 'Achieving Justice Against Wilful Defaulters in India - The Need for a Well-Coordinated Approach by Parliament, Law Enforcement and Banks' given during ICC FraudNet's meeting in Mumbai in April.*

The list of panellists is on Page 3.

Pan-European VAT fraud operation dismantled

AN organised criminal group involved in pan-European VAT fraud and money laundering has been dismantled in a joint operation led by the Spanish National Police, together with the Spanish Tax Agency and supported by Europol and Eurojust.

The investigation also saw the involvement of national authorities from Belgium, Bulgaria, Germany, Hungary, Italy, Portugal and Romania. In total, the damage caused to the EU economy due to this VAT fraud reached €60 million.

Fifty-eight suspects were arrested in Belgium, Germany, Portugal and Spain and 101 premises were searched in various EU countries. As a result, law enforcement seized 52 luxury cars, numerous documents, €400 000 in cash, IT material and one weapon.

The investigation began in 2015 when Spanish authorities were alerted to a criminal organisation specialised in VAT fraud and money laundering. The group carried out or simulated imports and purchases of electronic goods, both real and fake, which were sold online.

The criminal organisation was composed mainly of Italian, Portuguese and Spanish nationals and was allegedly managed from Spain by two men; father and son – Spanish nationals of Indian roots – believed to have been operating for more than nine years across Europe.

The group had a network of more than 100 companies (most of them shell companies registered under the name of frontmen) across Belgium, Bulgaria, Cyprus, Germany, Hungary, Italy, Portugal, Romania, Spain and the US.

The network also owned a production centre to create false invoices to perform VAT fraud on electronic goods and also on the import of luxury vehicles below invoice price.

Investigations revealed that the group issued false invoices for a value of over €250 million in three years.

Investigations also revealed that the money was layered among the large network of shell companies before being funnelled to Bulgarian or Hungarian bank accounts.

In particular, the organisation moved more than €140 million in two years through two Hungarian shell companies.

The group then used different methods to integrate its profits, such as investments in real estate and real businesses, or the purchase and sale of luxury vehicles. The final destinations of the proceeds of crime were Italy, Spain and the US.

Jari Liukku, Head of Europol's European Serious and Organised Crime Centre, said “MTIC Fraud remains one of the most significant transnational frauds targeting all Member States. Staggering sums of money are being taken directly from the citizens of the European Union by organised crime groups, depriving us all of essential services and infrastructure such as security, health, education or justice that should be funded by the proper collection of this revenue.”

He added, “By its very nature this is an international cross-border offence that requires a coordinated approach between Member States’ police services, customs administrations and tax authorities.”

from page 1 - India loan underwriting standards

more than twenty years. Many billions of dollars stolen from creditors and investors and hidden in Switzerland, Liechtenstein, London, and New York have been traced and recovered.

There is no reason why Indian creditors cannot follow the direction of major international banks which deploy well-established legal procedures to trace, locate, freeze and recover funds improperly transferred outside India and adopt modern methods of asset tracing.

If so, banks in India can bring wilful defaulters who are attempting to evade their legal obligations to justice.

The panel said ultimately, changing the culture of toleration of wilful defaulters (which rewards unethical and unlawful borrowing practices), will require robust Government regulation tied with targeted policy interventions by regulators and law enforcement and supported by private sector professionals acting on behalf of pro-active financial institutions (whose balance sheets are impaired by loans made in good faith to recalcitrant and dishonest borrowers, and who act to take robust action to recover their loss).

** The panel comprised Martin Kenney, Managing Partner, Martin Kenney & Co, Solicitors (British Virgin Islands); Shreyas Jayasimha, Partner, Aarna Law (Bangalore); Sandeep Baldava, Partner, Fraud Investigation and Dispute Services (Mumbai); and Christopher Redmond, Founder, Christopher Redmond Law Firm (Kansas City, MO).*

Will open beneficial ownership registers work?

THE UK parliament has controversially voted to force its overseas territories (OT) to create publicly accessible beneficial ownership registers by December 31, 2020. Critics say the move threatens the financial sectors and will not aid law enforcement. Is that true? Keith Nuthall *reports.*

LISTENING to the leaders of Britain's overseas territories, the beneficial ownership amendment to a UK Sanctions and Anti-Money Laundering Bill is a risk to their survival. The chief ministers of the Cayman Islands, Bermuda the British Virgin Islands (BVI) and Gibraltar have spoken out in anger, claiming the vote undermines long-established autonomy, embittered by the fact that UK crown dependencies the Isle of Man, Guernsey and Jersey will not have to follow suit (UK legislation usually does not apply to these three jurisdictions, but it does apply to OTs). Other territories covered by amendment to Britain's Sanctions and Anti-Money Laundering Bill are Anguilla, the Turks & Caicos Islands and Montserrat, who are less dependent on financial services.

BVI Premier Orlando Smith was typical, claiming: "This is a deeply flawed policy as the BVI already provides verified beneficial ownership information to the United Kingdom and other law enforcement authorities." He said the move would harm BVI efforts to recover from last year's devastating hurricane season.

And this line has been followed by his fellow chief ministers, who argue not only that they are already transparent and effective in detecting and weeding dirty money from their financial system, but their chosen approach - verified, but closed registers – with information made available to law enforcers worldwide, is better than an unverified public register.

Bermuda's Premier David Burt said his territory "already has some of the most responsive and comprehensive registers of beneficial ownership… those registers are updated in real time on every share transfer. This information has long been available to legitimate international competent authorities via the OECD Multilateral Tax Convention…"

The Cayman financial services and home affairs minister Tara Rivers said the decision was unnecessary given the Caymans' "high level of ongoing cooperation" on beneficial ownership, which enables more than 100 tax authorities globally, including HMRC, and UK crime agencies to access information "which states who owns what and how much in relation to Cayman companies".

Jude Scott, CEO of the Caribbean archipelago's financial industry organisation Cayman Finance, argued that verifiable beneficial ownership private registers, such as that operate in the Cayman Islands, which are searchable by appropriate tax authorities and law enforcement agencies, are more effective than open unverified public registers, such as the mainland UK system.

And there has been criticism of the UK register – which does not cover OTs and crown dependencies – noted a May (2018) report from the House of Commons Library. It noted that it is administered by Companies House, in London, which "is a registrar, not a regulator. By and large, it does not verify the accuracy of what it receives." Moreover, the responsible minister has stated in a parliamentary answer that "there are no plans to introduce 'automated verification' of the information on the register…" Instead, he stressed that Companies House will contact companies for more information where it believes a company has misunderstood the register's requirements; where they have not provided a statement required additional information; and seek compliance from companies where there has been a complaint about missing or incorrect beneficial ownership information.

Anti-corruption campaigners disagree with criticism of the OT reform. Indeed, most have been delighted by the amendment. One group, Global Witness said: "By agreeing to push the UK's Overseas Territories to publish public registers of the real owners of their companies, the UK has led the world in one of the biggest moves we have seen in the fight against corruption for years.

"Corrupt officials, McMafia style-mobsters and oligarchs use companies registered in these territories, places like the Cayman Islands and British Virgin Islands, to hide their criminal activities."

Of course, the publication of beneficial ownership data will give such groups plenty of data to chew on when looking for wrongdoing by wealthy individuals and corporations to evade or avoid taxes – whether in an unethical or criminal way.

But what system is really the most effective? A private verified one of public unverified one? The issue has been considered by global anti-money laundering body the Financial Action Task Force (FATF) and in its latest assessment – released in 2016 – it certainly comes down on the side of verification, if largely dodging the private/public register debate. Concerns it highlighted in how beneficial ownership registers operated included insufficient

Continued on page 6/

How banks should monitor suspicious shipping activity

Byron McKinney, Product Manager at Accuity, discusses the latest case of suspicious shipping activity and why financial institutions need to keep a close eye on the trades they finance, including how the goods are transported. Originally published by TXF News.

A number of news stories in 2017 detailed the radical methods being employed to evade sanctions controls, for example, through the transfer of commodities from ship-to-ship in international waters to avoid a vessel entering a sanctioned territory. This trend appears to have continued into 2018, with a recent case emerging in which a ship-to-ship transfer took place in a narrow strait between Crimea and Russia.

This latest report concerns the transportation of iron ore from Norway to Crimea by the vessel HHL MISSISSIPPI. A review of satellite data has uncovered that the vessel sailed to an anchorage zone within the Kerch Straits (between Crimea and Russia), where a series of smaller vessels then pulled up alongside it and transferred its cargo, discharging it at the port of Kamysj-Burun in Crimea.

Crimea is included on the OFAC sanctioned list and Norway, where the cargo was originally loaded, is a signatory to the EU Russian Sanctions Act of 2014. The delivery of this iron ore cargo therefore appears to be illegal.

This example throws up a number of questions; how is this type of activity regulated, who should take responsibility for monitoring the movement of cargo as part of a trade transaction, and how can the rules be enforced to prevent further illegal activity from occurring?

Regulation and the role of financial institutions

According to the trade finance principles published by the Wolfsburg Group, ICC and BAFT in 2017, financial institutions have a significant role to play in addressing the risks of financial crime associated with trade finance activities and aiding compliance with national and regional sanctions and embargoes. Additionally, agencies such as the Monetary Authority of Singapore (MAS) and the Hong Kong Association of Banks (HKAB) have issued compliance guidance to financial institutions undertaking trade finance activity.

The guidance paper published by the Monetary Authority of Singapore (MAS) was released in October 2015 and focused on identifying and managing red flags and risks in trade finance and correspondent banking. This paper outlined the major areas of attention to monitor as well as the best practices that banks and financial institutions should deploy, to ensure they act in compliance.

Similarly, the Hong Kong Association of Banks (HKAB) released its guidance paper on combatting trade-based money laundering in February 2016. In a similar vein to the MAS, the HKAB paper detailed some key areas of consideration for financial institutions to monitor in order to improve their trade compliance practices.

Whilst the agency guidelines from the Monetary Authority of Singapore and the Hong Kong Association of Banks do not specifically mention ship-to-ship transfers as in the HHL MISSISSIPPI case, they do highlight the need for trade finance providers to monitor vessels' journeys, to ensure they do not breach any sanctions.

Applying the principles in practice

Financial institutions must take a proactive approach to monitoring every element of a trade, which means not only understanding the companies involved, but also the goods, transportation, locations and beneficiaries connected to the transaction.

The MAS and HKAB guidance, when broken down, offer the following best practices and areas for financial institutions to prioritise when dealing with the shipment of commodities.

1. Risk Assessment – financial institutions should conduct a comprehensive review of their trade finance business, including the potential for financial crime relating to their customer base, geographical locations and products offered, and ensure the relevant controls are in place to mitigate risk.

2. Customer Due Diligence – financial institutions must check a customer or any instructing party involved in a trade finance transaction and enable the appropriate due diligence; checks on perceived 'high risk' customers should be the most extensive. The following should be reviewed:

- Customers' trading partners
- Nature of the goods and their potential dual-use (military and civilian)
- Country of origin
- Vessel name and IMO number
- Details of vessels – such as flag, journey history, name history
- Beneficial ownership of the vessel and checks on the shipping company
- Port of loading and discharge of the vessel
- Agents or third parties involved in the transaction
- Ports of call of the vessel for the particular transaction flow (origin port, destination port)

Continued on page 8/

Save the date - CCS Economic Crime Lecture

MEMBERS are invited to our *18th Annual CCS Economic Crime Lecture* on Fintech, Blockchain and Cryptocurrencies – risks and realities to be held on 27th June 2018.

The lecture will focus on how Fintech products are threatening to change the way in which financial institutions service their customers and the profound implications these are bound to have on their policies aimed at anti-money laundering, fraud prevention and control of proceeds of crime and compliance.

"Many regulators have recognised that these technologies could add to compliance and transparency in financial services. Products backed by blockchain mechanisms have been offered as a faster, more reliable and less expensive way of recording financial transactions," a CCS spokesman said. "Related to this the concept of Open Banking has been introduced in the UK and European banking system.

"Together these changes could have profound implications for policies aimed at anti-money laundering, fraud prevention and control of proceeds of crime and compliance in financial institutions and intermediaries. "In addition regulators and governments are seeking to monitor and regulate the growing use of cryptocurrencies," the spokesman added.

The *2018 CCS Economic Crime Lecture* will look at the risks in this emerging area, the solutions it offers, how realistic they are and what would be a practical timeline for them to be fully effective.

Speaker details
Peter Warrack is Chief Compliance Officer Bitfinex, formerly Director AML Advisory, Bank of Montreal. Peter was recruited to Canada by RBC following a career in law enforcement in the UK. In Canada he successfully built and pioneered RBC's intelligence-led fraud prevention approach setting the standard for the "culture of intelligence" and intelligence-led analytics before specialising in AML. His contribution to the AML profession was recognised by his peers in 2011 when he received the Association of Certified Money Laundering Specialists (ACAMS) Professional of the Year Award Places are still available but **please register ASAP.** RSVP: ccs@icc-ccs.org. Venue: Chartered Insurance Institute, 20 Aldermanbury, London EC2V 7HY.

from page 4 - open beneficial ownership registers

accuracy and insufficiently rigorous implementation of customer due diligence (CDD) measures by key gatekeepers such as company formation agents, lawyers, and trust-and-company service providers.

It said there was often a lack of sanctions on companies which fail to update information held by national company registries, including shareholder information. But it also raised concerns about insufficient transparency, where there are obstacles to information sharing such as data protection and privacy laws which impede competent authorities from getting timely access to adequate, accurate and up-to-date basic and beneficial ownership information. It also is concerned that in some jurisdictions there is a lack of accessibility to basic information relating to company registration.

Philip Anderson, director of corporate services provider Estera Services (Bermuda) Ltd, and an FCCA, questioned whether creating a public register delivered added value in terms of fighting crime. "Who wants to see the information? It it's to deal with tax evasion or money laundering – it's governments." And tax inspectors, anti-money laundering regulator and police already have the right to obtain information from OT beneficial ownership registers, he said. Moreover, the beneficial ownership registers do not operate in a vacuum. Jurisdictions such as Bermuda already have comprehensive anti-money laundering and combating the financing of terrorism (AML/CFT) controls, which involve the referral of suspicious transactions to the Bermuda Financial Intelligence agency, for follow up and potential legal action. Also, by making registers public, there are real downside, he suggested. The loss of privacy to wealthy investors and depositors could increase their security risks in their home countries, he suggested: "There are genuine threats of kidnapping. People who have such wealth need protection."

By contrast, anti-corruption group Transparency International disagrees, with Maira Martini, its knowledge coordinator, saying: "A public register is the best model. The information should be available as open data."

A TI note adds: "Obstacles to accessing this information or delays in transferring it to authorities make it harder to follow the money back to its source. This increases the likelihood that people who have engaged in corrupt or illegal acts will get away with their crimes." TI also wants robust verification through cross-checking information provided with other government databases (such as tax agencies, passport authorities, vehicle and property registries, and electoral registries), on-site inspections, use of software, and other reliable information.

US new customer due diligence rules comes into force

MEMBERS are reminded that the US' Financial Crimes Enforcement Network (FinCEN) Final Customer Due Diligence Rule (the CDD Rule) has now taken effect.

The CDD Final Rule adds a new requirement that financial institutions (including banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities), collect and verify the personal information of beneficial owners who own, control, and profit from companies when those companies open accounts.

The Final Rule also amends existing US Bank Secrecy Act (BSA) regulations to clarify and strengthen obligations of these entities. The CDD Final Rule harmonises BSA regulations and makes explicit several components of customer due diligence that have long been expected under existing regulations, as well as incorporating a new requirement for covered financial institutions (CFI) to collect beneficial ownership (BO) information.

Specifically, the rule contains three core requirements:
(1) identifying and verifying the identity of the beneficial owners of companies opening accounts;
(2) understanding the nature and purpose of customer relationships to develop customer risk profiles; and,
(3) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

With respect to the new requirement to obtain beneficial ownership information, financial institutions will have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity, and an individual who controls the legal entity.

Based upon comments received in response to the proposed rule that was published in August 2014, the final rule extends the proposed implementation period from one year to two years, expands the list of exemptions, and makes use of a standardised beneficial ownership form optional as long as a financial institution collects the required information.

FINCEN says the CDD Final Rule advances the BSA by making available to law enforcement valuable information needed to disrupt illicit finance networks. "This will in turn increase financial transparency and augment the ability of financial institutions and law enforcement to identify the assets and accounts of criminals and national security threats. This will also facilitate compliance with sanctions programs and other measures that cut off financial flows to these actors." FINCEN says.

By complying with these Anti-Money Laundering (AML) requirements, covered institutions may also reduce their risks under other federal laws such as the sanctions regulations implemented by the Treasury Department's Office of Foreign Assets Control, says Hogan Lovells.

Foodman CPAS & Advisors have produced FAQs on the new rules that might prove useful. These include;

- CFIs may choose to **implement stricter written** internal policies and procedures for the collection and verification of BO information than the requirements of the CDD Rule. CFIs can collect information on natural persons that own a lower percentage than 25%, as well as information on more than one individual that has managerial control. CFIs need **establish and maintain written procedures** to identify and verify the identity of BO of legal entity customers and include such procedures in their AML compliance program.
- CFIs must obtain from their legal entity customers the **identities of individuals** who satisfy the definition of BO, either directly or indirectly through multiple corporate structures and or complex ownership structures.
- CFIs must verify the identity of each BO according to risk-based procedures that contain the same elements that the CFIs use to verify the identity of individual customers under applicable Customer Identification Program (CIP) requirements. CFIs ought to conduct their own **risk-based analysis** to determine the methods of verification and the appropriate documents to accept.
- The CDD Rule authorises covered CFIs to use photocopies or other reproduction documents for documentary verification which includes unexpired Government issued identification (driver's license or passport). **Non-documentary methods** of verification include contacting a BO; verifying the BO's identity through the comparison of information provided by the legal entity customer (or the BO) with information obtained from other sources; checking references with other CFIs and obtaining a financial statement.
- Required **address requirements** for certification under CDD Rule are equal to those under CIP rule.
- There is no requirement for a CFI to use the **Certification Form** that was presented in the CDD Final Rule (Appendix A to the Rule). The Certification Form is optional and was presented as a possible method. CFI's must retain the Certification Forms that they choose to use and not file them with FinCEN.

** The full set of FAQS are available here.*

Corruption

MACN puts spotlight on maritime corruption

OVER 19,000 incidents of corrupt practices have been reported to date to the Maritime Anti-Corruption Network (MACN), the Network said in its 2017 Annual Report.

MACN has also collaborated with other shipping organisations to address the issue of maritime corruption more broadly in the industry and with maritime regulators.

"We now have over 90 companies in our network. Our collective voice and influence grows with our membership," MACN said.

In 2017, MACN together with the International Chamber of Shipping (ICS), initiated a cross-industry working group with the ambition of attracting engagement from traditional industry organisations and associations to collaborate and address key corruption issues in the shipping industry. By the end of 2017, the working group was well established and in 2018 will continue to work on raising awareness of maritime corruption.

MACN also started to explore partnerships with cadet schools in India to share MACN's Anti-corruption eLearning designed for ship masters and worked with the World Maritime University on a study to measure ethical corporate behaviour.

In the Suez Canal, MACN has also tackled facilitation demands during transits by implementing a collective "Say No" campaign. "The situation has improved every year, and feedback in 2017 showed that companies taking part in the campaign are transiting Suez without any delays or issues. Demands for cigarettes have decreased dramatically, or have been eliminated, while threats to the safety of both crew and vessel have also decreased significantly," MACN said.

The Network has trained over 570 government officials in the Nigerian ports of Lagos (Apapa), Lagos (Tin Can), Calabar, Onne, and Port-Harcourt. MACN's integrity training program has been welcomed and received high ratings from public and private sector stakeholders (for example, 90 percent felt this exercise was useful or relevant for their work).

The training covered integrity, corruption prevention, the rationale behind the new harmonised procedures in the port and vessel clearance procedures, and the Grievance Mechanism. The training linked well with the Nigerian Presidency's Executive Orders in 2017, which focused on ease of doing business in Nigeria. Surveys of MACN members demonstrate this project is having a positive effect on the operating environment.

For example, MACN member companies are periodically achieving a zero-tolerance approach to corrupt demands without threats or delays.

from page 5 - suspicious shipping activity

- Recent voyage history of the vessel and whether it has docked at any embargoed countries during previous voyages

3. Audit Trail – financial institutions should ensure that documentation of the review process for screening hits is well maintained and accessible. Justification for closing off screening hits as false positive hits should also be properly documented to facilitate second-level post-transaction reviews and audits.

4. Dual-Use Goods – financial institutions should determine whether the underlying goods being financed are embargoed goods and there should be special attention paid to dual-use goods. At the very least, a bank should have a process in place to identify any dual-use commodities and escalate them, for further review.

The MAS and HKAB guidelines are the basis for an effective trade compliance solution covering the shipment of commodities. Financial institutions should be seeking to implement such guidelines within their day-to-day operations as a means of remaining compliant with the shifting and expanding landscape of global regulation.

Conclusion

In the case of the shipment of iron ore from Norway to Crimea by HHL MISSISSIPPI, it is not known whether the financial institutions financing the trade had the appropriate screening capabilities set up to notify them of any illicit activity. However in practice, with the right technology implemented, a trigger could have alerted any concerned parties when the vessel entered a Crimean anchorage zone or port.

The financial institution would then have been in a position to quickly take action, follow the correct procedure to report any suspected breaches of regulation, and protect itself from involvement in any wrongdoing.

Credit: Byron McKinney, Product Manager, Accuity
https://accuity.com/accuity-insights-blog/navigating-trade-finance-banks-monitor-suspicious-shipping-activity/

Cyber insurance considerations for financial institutions

THE Federal Financial Institutions Examination Council (FFIEC) has issued a joint statement that discusses considerations for financial institutions contemplating the purchase of cyber insurance and its potential role in risk management programmes.

FFIEC says although its members do not require financial institutions to maintain cyber insurance, the evolving cyber insurance market and the shifting cyber threat landscape may prompt them to consider whether cyber insurance would be an effective part of their overall risk management programs.

FFIEC notes that;

- cyber attacks are increasing in volume and sophistication and that traditional general liability coverage insurance policies may not provide effective coverage for potential exposures caused by cyber events.
- cyber insurance may help reduce financial losses from a variety of exposures, such as data breaches resulting in the loss of sensitive customer information.
- cyber insurance does not diminish the importance of a sound control environment; rather, cyber insurance may be a component of a broader risk management strategy.

However, FFIEC cautions that purchasing cyber insurance does not remove the need for a sound control environment.

Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure.

"An effective system of controls remains the primary defence against cyber threats. If institution management is considering cyber insurance, the assessment of cyber insurance benefits should include an analysis of the institution's existing cybersecurity and IT risk management programs to evaluate the potential financial impact of residual risk," FFIEC says.

It advises financial institutions to consider the following;

- Involving multiple stakeholders in the cyber insurance decision.
- Performing proper due diligence to understand available cyber insurance coverage.
- Evaluating cyber insurance in the annual insurance review and budgeting process.

British brokers launch new guide

THE British Insurance Brokers' Association (BIBA) in collaboration with CFC has launched a new guide to help brokers understand cyber risks and the insurance solutions available to mitigate these risks.

Mike Hallam, BIBA's Head of Technical Services said, "As our reliance on technology grows so does the potential for cyber related incidents. It is important for brokers and their customers to understand and be able to manage these new risks which is why we were delighted to be able to work with sector leaders, CFC to create this new guide. Brokers will also appreciate the advice in the guide on how to address common objections from clients as to why they need cyber cover."

Taking on board that cyber insurance is for many one of the most misunderstood covers, the guide aims to cut through the jargon and bring simplicity to what has long been considered a complex line of business. Within it, brokers can learn about the evolution of cyber risk, read examples of cyber claims and appreciate how cyber policies work which will be invaluable in helping to identify client's risks.

James Burns, Cyber Product Leader at CFC added, "Cyber insurance policies tend to be modular in nature, consisting of a variety of different coverage areas so it's no wonder that this has led to confusion around what they cover and how they work. We wanted to provide straightforward and clear information about what cyber is all about and how brokers can articulate it to their clients."

BIBA's Cyber guide can be viewed here.

Ten Tips On Cyber Liability Insurance

WHAT do companies need to know about cyber insurance? Here are Top 10 Thoughts by Poyner Spruill LLP.

- Existing Policies Likely Will Not Protect You.
- No Standard Policies.
- Know Your Minimum Requirements.
- Examine the Fine Print.
- Watch out for Pitfalls. Common policy provisions can significantly undermine coverage.
- Beware the Contractual Exclusion.
- Evaluate proposed policies from the regulatory perspective.
- Cyber insurance offers analogous cost savings.
- Evaluate the Experts.
- Talk to your Broker and Counsel.

Freight forwarders, shipping firms warned over BEC attacks

FREIGHT forwarders, shipping agents and maritime-based firms are being warned of business email compromise (BECs) and business email spoofing (BES) fraud specifically targeting them.

The perpetrators, likely based in Nigeria, use a range of commodity remote access tools that have keylogging and password-stealing functionality to steal email account credentials, according to Secureworks.

The group routinely tests malware on its own systems and tracks detection rates via online virus scanners (for example NoDistribute).

The group uses a range of commodity remote access tools that have keylogging and password-stealing functionality to steal email account credentials.

Named GOLD GALLEON, Secureworks says the group does not target a wide range of businesses but appears to focus solely on global maritime shipping businesses and their customers.

Secureworks Counter Threat Unit (CTU) researchers estimate that between June 2017 and January 2018, GOLD GALLEON attempted to steal a minimum of US$3.9 million from maritime shipping businesses and their customers. The threat actors' theft attempts average US$6.7 million per year.

Secureworks said over the course of the investigation into GOLD GALLEON, its researchers have been able to develop unique and detailed insight into the threat group: how it operates, where it is based, and its likely affiliations.

"GOLD GALLEON is a collection of at least 20 criminal associates that collectively carry out BEC campaigns. The group appears to specifically target maritime organisations and their customers."

CTU researchers have observed GOLD GALLEON targeting firms in South Korea, Japan, Singapore, Philippines, Norway, US, Egypt, Saudi Arabia, and Colombia.

"The threat actors leverage tools, tactics, and procedures (TTPs) that are similar to those used by other BEC/BES groups that CTU researchers previously investigated.

"The groups have used the same calibre of publicly available malware (inexpensive and commodity remote access trojans (RATs), crypters, and email lures," Secureworks said.

DDoS admins arrested

A global crackdown on cyber attacks has led to the administrators of the Distributed Denial of Service (DDoS) marketplace webstresser.org being arrested.

Investigations were led by the Dutch Police and the UK's National Crime Agency with the support of Europol and a dozen law enforcement agencies from around the world.

The administrators were located in the United Kingdom, Croatia, Canada and Serbia. Further measures were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong. The illegal service was shut down and its infrastructure seized in the Netherlands, the US and Germany.

Webstresser.org was considered the world's biggest marketplace to hire DDoS services, with over 136,000 registered users and four million attacks measured by April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry. With webstresser.org, any registered user could pay a nominal fee using online payment systems or cryptocurrencies to rent out the use of stressers and booters. Fees on offer were as low as €15 a month.

Norway and Switzerland join EU cybercrime taskforce

NORWAY and Switzerland became new official members of European Union's Joint Cybercrime Action Taskforce (J-CAT).

At its board meeting in April, the chairmanship of J-CAT was handed over to the Netherlands for the upcoming year.

Netherlands is the third country to take over the position after the United Kingdom and Germany since the taskforce was launched in September 2014.

The Taskforce is hosted within Europol's European Cybercrime Centre (EC3) and comprises cyber liaison officers from 13 EU Member States and non-EU partners and 15 law enforcement agencies.

J-CAT's objective is to boost the cooperation between law enforcement authorities, drive intelligence-led, coordinated actions against the major cybercrime threats and facilitate cross-border investigations by its partners.

Account takeover based email attacks up 126%

CYBERCRIMINALS know that employees are the weak link in an organisation and need only to convince these targets that they are someone who should be trusted to achieve success. In terms of methods used to deceive employees, email spoofing and display name deception have been the "go-to" techniques.

However, security leaders charged with reducing this risk need to factor in yet another form of email-based identity deception tactic.

According to recent Agari research, there has been a 126 percent increase of targeted email attacks that exploits Account Takeovers (ATO).

Prior to 2017, concerns over ATO-based email attacks were virtually non-existent. However, in early 2017, the Google Docs ATO Worm Attack brought a spotlight to the problem when it struck over a million users in only a few hours.

Most recently, a new Osterman Survey found that 44 percent of organisations were victims of targeted email attacks launched via a compromised account in the past 12 months. As these attacks continue to rise, organisations should be evaluating whether their existing email security controls can analyse, detect, and block ATO-based email attacks.

What does a typical ATO-based email attack look like?
An Account Takeover (ATO)-based email attack is the process of gaining unauthorised access to a trusted email account and using this compromise to launch subsequent email attacks for financial gain or to execute a data breach.

Since ATO-based attacks originate from email accounts of trusted senders, traditional security controls cannot detect such attacks. Moreover, given the pre-existing trust relationships, launching a targeted attack such as a Business Email Compromise from such an account, increases the likelihood that the attack will succeed.

Account Takeover-based email attacks rely on leveraging a compromised account or endpoint as a launchpad for a targeted email attack such as Business Email Compromise.

Why are ATO-based email attacks so effective?
Based on internal research, Agari has seen a 126 percent increase month-over-month in early 2018 alone. The data was observed from Agari Enterprise Protect, an advanced email threat solution that filters email traffic after it has been scanned by a Secure Email Gateway (SEG). As part of the analysis Agari analysed over 1,400 messages considered untrusted, over a two-month period.

The reasons are due to two distinct adversary advantages:

1. Legitimate or established email accounts do not need to leverage impersonation techniques such as domain spoofing or display name deception to bypass email security controls.
2. Previously established trust relationships between the original user and their contact, makes targeting and convincing the contact to give up sensitive data or release funds, a significantly easier task.

However, not all ATO-based email attacks are the same and the effectiveness will depend on the type of compromised account used in the attack. According to the same research Agari determined that there are four account types used in ATO-based attacks.

Stranger - attacks using any legitimate email account of individuals unknown to the recipient (strangers) to boost reputation and leverage trusted infrastructure.

Employee webmail - attacks using personal employee webmail accounts (e.g. Gmail, Yahoo, Hotmail) accounts of individuals known to the recipient to exploit trust.

Trusted third parties - attacks using supply chain vendor accounts of individuals known to the recipient to launch spear phishing campaigns.

Insider business accounts - attacks that use employee corporate accounts of individuals known to the recipient to execute BEC or invoice scams.

Additionally, based on customer feedback attacks launched from a known employee webmail or insider business account had the highest chance of success.

The good news is that the large majority of today's attacks are still only using stranger email to launch attacks.

As attackers become more adept at identifying and compromising specific employees to target their own organisations, the effectiveness of ATO-based email attacks and real dollars lost associated with these attacks will be sure to rise.

~ *Source: Agari*

New initiative for Square Mile firms

MEMBERS operating in the City of London may want to take note of a new initiative by the City of London Police to make the Square Mile more secure from cyber attacks.

'Cyber Griffin' will see specially-trained officers lead a series of community focused exercises which will include threat briefings, incident response training and more.

The initiative is targeted at businesses within the City and aims to reach those with very little knowledge of cyber-enabled crime threats, all the way up to individuals who hold IT security and risk roles.

Cyber Griffin will be based around three key deliverables:

• Updates and threat briefings
Free-of-charge threat briefings will be designed to build basic defender skills in key areas with individuals from all levels of business welcome to attend.

The events will provide officers with the opportunity to deliver the latest updates in intelligence and members of the business community to network with each other and share their experiences.

• Incident response exercises
Officers will deliver three different levels of incident response, all of which will provide an invaluable insight into police decision making.

The exercises will cover a basic response right up to an expert response played out in real-time for more senior members of business.

• Advisory groups
These groups will be made up of a wide-range of experts, from industry and the private sector, capable of providing valuable insight to less experienced members of the business community.

Police officers will carefully select people from businesses with dedicated threat intelligence and experience in cyber security to act as a problem-solving group for other businesses with none.

As cybercrime increases and more online attacks are launched on UK businesses than ever before, officers in the force's Cyber Crime Unit felt a community-based approach to tackling the problem was needed.

More information here.

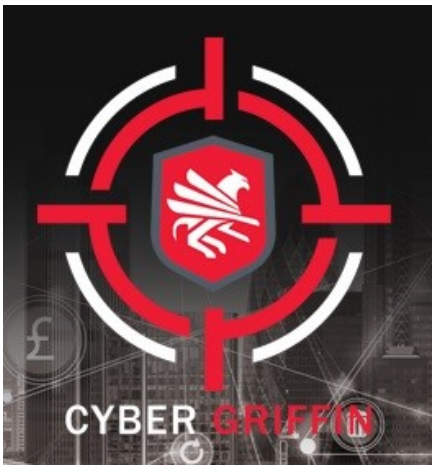

Image: City of London Police

Cloud-based KYC platform

BIG-data specialist Quantexa is partnering with compliance robotic automation leader Arachnys to identify and monitor customer risk.

Quantexa will be using Arachnys' cloud-based investigation platform and global news assets to dynamically screen against negative news, locate missing Know Your Customer (KYC) data and provide enhanced risk scoring.

This will give financial institutions a deeper understanding of the risks associated with their customers.

Arachnys will utilise Quantexa's software to compute relationship and network risk, to identify high-risk entities and Ultimate Beneficial Owner structures in a subject's network and to trigger events for KYC data collection.

The fusion of the technologies will reduce false positive matches and ensure complete views of customer risk across entire populations, while assuring compliance for new regulations

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