COMMERCIAL CRIME
International
April 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

FraudNet meet to discuss toxic debt and wilful defaulters

MOST, if not all members will by now be familiar with the estimated $1.8bn Nirav Modi fraud in India since the case made international headlines earlier in the year.

While investigators try and get to the bottom of how the fraudulent transactions were allowed to go on for a considerable amount of time, the case raises serious questions as to the robustness of banks' internal monitoring systems.

Furthermore, the jurisdictions and borders are numerous, so what is being done to bring the case to a successful conclusion; or is it simply too complicated to investigate and draw to a close?

These are some of the pertinent issues set to be discussed at ICC FraudNet conference to be held in Mumbai, India, on April 27.

Indian banks have a problem with substantial 'toxic debt.' This debt has been incurred by loan defaulters, some of whom have wilfully defaulted to illicitly transfer funds offshore.

Others are simply concealing their assets. FraudNet has identified that there is a misconception that once assets have left India, they are out of reach.

This is not the case; nor is this problem confined to India, it is an international problem.

"A key message is that these assets can be recovered. As experts in the investigation of international fraud and cross-border asset recovery, FraudNet members have experience in successfully bridging the jurisdictional gap and clawing back substantial sums of value for creditors and victims alike," says a FraudNet spokesman.

ICC FraudNet falls under the auspices of ICC Commercial Crime Services and currently has 75 members in 64 countries.

Indeed, it's cross-border network and expertise in investigating and recovering assets is what enables FraudNet to be effective in what it does; since its formation in 2004 it has recovered hundreds of millions of dollars for victims of fraud.

One recent success story involved a Jersey-based FraudNet member who was instructed by a Russian company to help enforce a Russian arbitration award.

The judgment debtor - a Jersey company owned by a well-known Russian company - had ignored the arbitration award against it.

The FraudNet member obtained a Norwich Pharmacal type disclosure order on the Jersey trust and corporate service provider which administered the Jersey company.

The member discovered the debtor held a Jersey Bank account and two Swiss bank accounts. Working with another FraudNet member in Switzerland, the two Swiss bank accounts were frozen. The accounts contained double the amount of the arbitration award, and the full arbitration award was paid within a week.

Working closely with members' strategic partners is also paramount when embarking on the investigation of an international fraud and cross-jurisdiction asset recovery because such investigations are dynamic and fast-moving.

FraudNet's strategic partners are fundamental to our success, providing multi-disciplinary expertise and additional cross-border-reach, says the spokesman.

An interesting session at the conference is a judge's perspective on international asset recovery where a panel of judges will offer

Continued on page 2/

In This Issue of CCI

from page 1 - FraudNet meeting

their pointers on what they look for when hearing a case; what is persuasive evidence; what thresholds they set when an application for a court order hits their bench; and how they arrive at their decisions.

Another panel will discuss offshore jurisdictions and how sometimes they can be barriers to asset recovery. The panel will describe how value moved into offshore jurisdictions can raise challenges to the role of the international fraud investigator, in terms of their cross-border asset recovery remit.

However, they will explain how these challenges can be met and ultimately defeated; clarifying the issues surrounding the presumed necessity to first obtain an Indian judgment before embarking on a campaign to locate and freeze concealed assets pending the outcome of loan enforcement proceedings, to manage risk and effectuate such recoveries and filings. The use of cross-border insolvency law tools to recover assets will also be discussed.

A case study of Petroforte Brasilero and Banco Santos (both in bankruptcy) and how FraudNet traced and recovered hundreds of millions of dollars across national boundaries for Brazilian creditors will also be presented at the conference.

Ten years ago, creditors in Brazil rarely ventured abroad in search for assets of dishonest borrowers and debtors. This has changed substantially due to the introduction of FraudNet's cross-border asset recovery model to Brazil.

The meeting will be opened by Ed Davis, FraudNet Executive Director, and founding partner of Sequor Law based in Miami.

Ed will touch upon the scope and extent of FraudNet's existing work for persons harmed by economic crime and other forms of iniquity, plus outline its significant historical successes, and the various means of funding the investigations and recovery processes.

ICC FraudNet
COMMERCIAL CRIME SERVICES
est. 2004

About FraudNet

FraudNet is an **international network** of independent lawyers who are the leading civil asset recovery specialists in each country.
Its membership extends to every continent and the world's major economies, as well as leading offshore wealth havens that have complex bank secrecy laws and institutions where the proceeds of fraud often are hidden.
Using sophisticated investigation and forensic tools and cutting-edge civil procedures, FraudNet members have **recovered billions of dollars** for victims of some of the world's largest and most sophisticated global frauds involving insurance, commodities, banking, grand corruption and bankruptcy/insolvency.
Members – all some of the world's most respected law firms - work together to pursue and recoup assets transferred across borders.

How FraudNet works

FraudNet's lead lawyer begins by assembling a strategic **multidisciplinary transnational team** that includes asset recovery lawyers, investigators and forensic accountants from within the network.
The FraudNet team promptly organises a **forensic investigation** and selects the optimum jurisdiction to commence court proceedings.
The team moves quickly and diligently, **using specialised disclosure,** gag and seal and investigative orders. With their specialised arsenal of civil remedies, FraudNet lawyers can force third-party financial institutions hiding assets to covertly disclose critical information, **without tipping off targeted fraudsters**. Other civil court orders grant FraudNet teams the authority to obtain documents and perform search and seizures to retrieve critical information for the investigation. In jurisdictions where civil remedies do not exist, FraudNet teams collaborate with law enforcement to **freeze local assets and track assets** in other jurisdictions for use in civil or criminal proceedings.
After successful investigation, the FraudNet team freezes the target's assets across the globe in multiple, simultaneous civil court actions.
FraudNet lawyers use injunctions or freeze orders to **prevent fraudsters** and their accomplices from selling or transferring assets before they can be liquidated to satisfy victims' claims.

**More details, including finding a FraudNet member, can be found at https://www.icc-ccs.org/home/fraudnet*
Follow FraudNet on Twitter at @ICCFraudNet

The challenge presented to India by wilful defaulters

AS of December 31, 2016, the Finance Minister of India, the Hon. Arun Jaitley, informed Parliament that there were a total of 9,130 wilful defaulters who collectively owed banks in the region of INR91,155 Crore (or approximately USD14 billion). This large portfolio of wilful default is a key challenge facing India.

This culture of wilful defaulters frustrating the banking and law enforcement authorities does not show any signs of abating. As recently as 14 February 2018, the public was alerted by the Punjab National Bank (India's second biggest state-run lender and fourth-biggest overall in assets), that Nirav Modi and his affiliates had allegedly defrauded it of amounts worth $1.17 billion.

When federal agencies stepped in it emerged that Mr. Nirav Modi and his associates were no longer in India. It is fair to conclude that unless active steps are taken by law enforcement to respond to such occurrences by building and deploying multi-disciplinary teams of professionals, the situation is likely to deteriorate further.

This episode drew a stern response form Indian Finance Minister Arun Jaitley saying, "With regard to lack of ethics that a faction of Indian business follows, it is incumbent on us as a State, till the last legitimate capacity of the State, to chase these people to the last possible conclusion to make sure that the country is not cheated."

Sustained economic growth is dependent on a sound banking system. Changing the culture of tolerating wilful defaulters requires robust Government regulation, tied with targeted policy interventions by regulators and law enforcement. This is conducive to attracting and retaining foreign capital; and to maintaining the nation's solvency and security as a whole.

When a culture of wilful default is allowed to permeate, the Government is required to intervene and recapitalize banks at a substantial cost to the public Exchequer. There is no quick remedy to fix a problem of this scale and complexity.

To tackle this problem, it will be important for India to have a court system that is capable of dealing with cases of wilful default. The Insolvency and Bankruptcy Code, 2016 (the "Code") is a welcome step in reforming India's insolvency laws. It provides for a quick and efficient system of debt recovery from wilful defaulters; and includes provisions relating to bilateral agreements with foreign countries to help track down cross-border offenders.

A special unit of the Central Bureau of Investigation, along with Special Divisions of the Economic Offences Wings of the State Police Forces, should also be constituted with a mandate to review cases of suspected wilful default and determine if criminal investigations should be instituted. In addition, the Central & State Governments should consider forming a team of highly experienced specialist prosecuting counsel, supported by forensic accountants and investigators, to address and prosecute these cases. The work of these multi-disciplinary teams of professionals should be centrally coordinated by the Office of the Attorney General for India, the Solicitor General, and additional Solicitor Generals; and at the State level by the Advocate General.

The Courts could also take the assistance of the Office of the Central and the State Auditor Generals to liaise with external professionals to help trace assets that may have been hidden by some wilful defaulters in tax havens and other offshore jurisdictions with a culture of protection over the confidential nature of bank and company ownership records. Wilful default is not a uniquely Indian problem. There are myriad ways in which assets dishonestly concealed or retained by borrowers can be tracked, frozen and recovered with the use of modern cross-border asset recovery tools and experts.

Large debts to the tune of 2,000 – 10,000 Crore left unpaid by wilful defaulters cause such a risk that in the short term they may reduce confidence in the banking system. Their impact is also felt by other customers of the bank who end up paying higher fees and interest rates. In the long run this phenomenon unleashes a loss of confidence in the psychology of foreign investors. It thereby diminishes India's basic economic infrastructure as there is a loss of confidence by foreign investors, and companies fail to invest.

The new Bankruptcy Code is in its infancy. Like all law reform initiatives, it will be refined and improved by amendments by Parliament or by case law as it is tested through the Courts. No new law of this complexity and importance is smoothly implemented over-night. It is, however, very encouraging that the Government has introduced such legislation.

In many wilful default cases, sophisticated and ethically challenged borrowers claim to 'lose' loan capital through legitimate loss-making activity, ostensibly involving arm's -length trading counter-parties abroad who hail from any one or more of the jurisdictions that recalcitrant debtors from India are drawn to – Mauritius; Dubai; Singapore; Hong Kong; the Seychelles; Switzerland and the like.

It will also be important to confront those who facilitate these criminal activities.

Continued on page 5/

High stakes chess match

By John Miles, Managing Director, John Miles Arbitration

LET's say you've won a tender to represent regulators of publicly listed stocks in a high-stakes ($200 million) investigation of a major corporation that was hollowed out by thieving managers. The place is a nation I dare not name for fear of dooming my professional reputation, or worse. It's an African nation, if you must know, although it could easily have been a South American nation or any country still identified as "developing."

You know going into the game is set against you. You will have to tread with extreme care through a minefield created by titans of industry and their political cohorts, all of whom bask in the knowledge that no matter what you manage to uncover, they're not going to prison.

They'll protect each other to the end and back and along the way treat you with unabashed arrogance. Because your firm isn't local you have the outsider's advantage, which likely helped you win over the regulators. You're independent of political attachments and not as susceptible to those kinds of pressures as a homegrown entity. Of course there are pressures to which we're all susceptible and we'll get to that later.

First you assemble a strong forensics team with a local branch of a global accounting firm and a top local law firm. Your worldwide network of colleagues will come in handy when you have to do things like determine whether a particular intimidation technique is endemic or ad hoc—and what to do about it.

The subject company deals in soft commodities and hard realities. Its history is divisible into three time periods: firstly, when it's cash rich and a household name; secondly, when it expands into related and unrelated fields and submits to the control of a criminal mastermind we'll call The Professor (with apologies to Sir Arthur's Moriarty), and thirdly, when the enterprise collapses amid loan defaults because of corruption during the middle period.

The company employs about 4,500 people and you start by informally and anonymously interviewing 100 non-managers, also known as "small fish." You count this effort as a success when about a third of them give you the lowdown on what went on during the dark days of the middle period. Another third of the group benefitted from the wrongdoing and paint a far rosier picture.

Documents also prove crucial. You find them totally disorganized but plough through upwards of three million papers. Emails were deliberately deleted and hardware and software were destroyed to cover tracks and destroy incriminating evidence. But one or two functionaries failed to do the job properly and you retrieve some electronic nuggets.

All this effort pays off when the real and virtual paper trail leads you to a whistleblower who spills about what happened in the dead of night. You emerge with a global schematic of the hollowing-out phase. You learn that during The Professor's tenure the company was run by middle managers on the ground who didn't confide in the board for painfully obvious reasons.

Tenders for major projects that should have been conducted under a public procurement program were instead fixed and the prices were highly inflated, generating a lot of cash that management pocketed.

On the more sophisticated side of the theft, certain goods nominally taxed by one nation were instead sold, without taxes, to another, providing kickbacks that wound up in private accounts. Working with government investigators, you find the relevant bank accounts and kick-start criminal prosecutions.

Here's where the wicket gets especially sticky. Senior management was involved with politicians raising money for upcoming general elections (Did I mention the government once owned and still retains a stake in the company?). To date no senior politician has been sent to prison. You would like to say the prospects for retribution are good, except historically they are not.

Towards the end of the investigation the company's helpful general counsel is assassinated. The crime remains unsolved. This naturally gets your full attention, but even before it happens, you find yourself taking extraordinary security measures.

You hire private protection and these hulks escort you everywhere. Doors you normally wouldn't think about locking must be locked. Cameras and tracking devices are ubiquitous.

You vary your routes driving to and from work. Documents and even board presentations are watermarked and, when you issue your report, there is only one hard copy. You are proud of the report because it is written in a reader-friendly style that is readily comprehensible to a non-professional. An accountant is not trained to do this.

There are a myriad of other challenges. You don't want a leak because not only could it undermine the investigation, if it gets to third parties, you're the one subject to civil action.

Continued on page 5/

India: public sector banks poll

THE recent frauds involving public sector banks (PSBs) in India raised concerns among Indian citizens about various aspects of business-banker nexus and gaps that exist.

LocalCircles, an Indian community-based online platform invited Indian citizens to have their say on PSBs in a survey. The survey received more than 50,000 votes and over 20,000 people from across India took part.

The first question asked how common people thought collusive corruption between businesses and staff at Public Sector Banks in India is. Around 53 percent said it is 'a norm' and 43 percent said it happens only in limited cases of loans/credit.

Participants were also asked what they thought was the best solution to fix the state of PSU banks in India.

Fifty-two percent said having an effective vigilance system was the answer, while 13 percent believed that placing of top private sector professionals in senior management and boards was needed. Thirty-two percent said privatisation is the way forward.

The third question asked if a systematic external audit of loans and credit with common auditing standards should be done at all PSU banks to find out if there were any other fraudulent transactions in the system.

Around 89 percent said yes, while 3 percent disagreed, saying the billion-dollar Punjab National Bank fraud was 'an exceptional case'. Seven percent said an audit was not required as PSU banks have strong auditing systems.

To prevent defaulters from escaping the law and fleeing the country people were asked if banks should use passports as collateral for loan payment defaulters. The passports of defaulters who wanted to travel abroad would be released based on the status of their accounts. Around 67 percent agreed with such a move while 27 percent did not.

Thirty-five percent said they felt secure putting their money in banks. Sixteen percent said they planned to move their savings to a private bank, while 8 percent said they would move to gold or property.

from page 3 - India

Including the pursuit of damages actions against 'enablers' such as accountants, lawyers and bankers who engage in unethical and unlawful activities. Where appropriate, governments and financial institutions should consider pursuing civil and criminal actions against these parties in order to bring them to book. The rule of law is vital to the preservation of an orderly and well governed society. What fraudsters fear most is to have their secrets revealed, their assets pre-emptorily frozen, and being forced to pay their valid obligations. As 19th century English clergyman Frederick Robinson observed: "There are three things in the world that deserve no mercy - hypocrisy, fraud and tyranny."

* *Authored by Shreyas Jayasimha, Partner, Aarna Law & ICC FraudNet member India, Sandeep Baldava, Partner, Fraud Investigation and Dispute Services, Ernst & Young (India), Christopher Redmond, Christopher Redmond Law Firm & ICC FraudNet member Mid-Western United States and Martin Kenney, Managing Partner, Martin Kenney & Co, Solicitors & ICC FraudNet British Virgin Islands.*

from page 4 - high stakes chess match

The press could say you're a donkey and it would be hard to litigate against them, but the courts tend to sympathize with libel plaintiffs, not defendants. You're the one at risk, not the publication.

You can't count on the law or police officials or judicial agencies to take measures against the fraud from which any or all of them may benefit. When something does finally get to court, it drops into a black hole and disappears for years on end. Here you find no shortage of players with contrary agendas trying to shut down or slow the process even more. Members of this establishment have never heard that justice delayed is justice denied.

An active whistleblower is a mixed blessing because there's a clear need for anonymity of key witnesses in politically sensitive investigations. The laws that protect and encourage whistleblowing in nations like the United States are undeveloped here.

So why take on projects like this? Just as Magnus Carlsen must play chess, you must do this. The regulator is processing your findings and is in court proceeding against the people you identified as part of the ongoing scandal. You did your job well and courageously--despite the dangers--and the resolution is out of your hands.

You played chess. You gained an advantage. You left if unfinished but with your head held high.

* *This article arises from a case that John Miles and his team handled for an East African Regulator over a period of a year. John is the only ICC FraudNet member in the East African region.*

Brexit: UK and EU face up to crime fighting challenges

THE CHALLENGES facing Britain as it deals with the consequences of the June 2016 referendum vote to quit the European Union (EU) are manifold. However, unpicking British involvement in joint anti-crime arrangements with the EU maybe the toughest of all. Keith Nuthall reports.

AFTER almost a year of negotiations on how the UK might extricate itself from a European Union (EU), of which it has been a member (in the EU's developing forms since 1973), there are now, at last, some solid proposals on how this might take place.

The European Commission, on February 28 released a draft withdrawal agreement that lays down in detail how Brussels would like to see Britain exit the EU. It includes a transitional period from March 29, 2019, (the date the UK will officially leave the EU), until December 31, 2020, when existing EU laws will continue to apply.

This would include criminal cooperation rules and regulations, but once the clock strikes 12 on Midnight of New Year's Eve on 2020, these would fall away, and years of painstakingly negotiated legislation and cooperative arrangements would expire, as far as the UK is concerned.

Of course, the joint investigations and judicial proceedings that spring from this work would not have such a neat end, and the Commission draft proposes that not only should these proceedings and probes continue, but they should be backed by the full force of EU law, until they are completed.

Take European arrest warrants, which require an EU member state to arrest and transfer a criminal suspect or sentenced person to the issuing EU country. Under the Commission proposals, these would stay in force, even if a suspect sought by British police was being held by an EU member state when the transition period expires.

The same principle would apply to cross border freezing orders, confiscation orders, court judgements, supervision orders, protection orders, plus requests for exchanges of criminal records, customs, suspicious transaction, travel and conviction information, which are submitted before the end of the transition period but have yet to be carried out.

And it would also apply regarding European Investigation Orders received before the December 31, 2020. Indeed, the Commission wants UK police and other law enforcers to continue participating in joint investigation teams set up before this date under the EU Convention on Mutual Assistance in Criminal Matters. Requests for cross-border surveillance under the EU's Schengen Implementing Convention would also stay in force, with previously approved UK participation in such operations continuing until they are completed. So, would requests for controlled deliveries made under the EU convention on mutual assistance and cooperation between customs administrations.

What happens after these inquires and proceedings have been completed, however, is another question altogether. And these questions will have to be answered during negotiations for a longer term post-Brexit UK-EU agreement, that – it is hoped – will be struck, before the 2020 deadline rolls around.

However, given the number of EU instruments in place, and the fact they are interlinked, and underpinned by rights enjoyed by all EU citizens for countries that remain member states, this hope may well not be realised. This is certainly the view of the UK House of Lords home affairs sub-committee, in a paper released in December (2017) on 'Brexit: future EU-UK security and police co-operation.' It brims with recommendations from senior UK law enforcement officials of the value of British participance in the European arrest warrant scheme, EU police agency Europol, the European investigation order, the European supervision order, and more.

But in many cases, the report quotes expert views that negotiating a close, yet separate, relationship between the UK and the EU regarding these institutions, that delivered law enforcement results sought by senior UK police executives, could take years to complete. (*See https://publications.parliament.uk/pa/ld201617/ldselect/ldeucom/77/7707.htm#_idTextAnchor047*)

On the plus side (as far as British law enforcers are concerned), the UK government certainly wants to develop a close relationship with the EU criminal law institutions that Britain is about to leave. Indeed, in its future partnership paper on security law enforcement and criminal justice (released last June - 2017), the government said it wanted a closer criminal justice relationship the EU than any other non-member state had yet to achieve, including Norway.

"The UK and the EU need to look beyond existing third country precedents, designing instead comprehensive arrangements that reflect the exceptionally broad and deep security relationship that exists today, and which are capable of evolving as threats change in the future."

Continued on page 7/

Bribery/Fraud

Denmark: new initiative to tackle facilitation payments

DENMARK's Foreign Ministry and The Confederation of Danish Industry (DI) have launched a new initiative aimed at tackling facilitation payments.

The Fight Against Facilitation Payments Initiative (FAFPI) provides a platform for companies to share their experiences and includes a reporting tool for members to lodge the types of facilitation payments they are asked to make.

"The problem of 'facilitation payments' has long been an intractable one. If the Danish embassies are to be of help, concrete information is needed regarding where firms and organisations run into bottlenecks," Susanne Hyldelund from the Foreign Ministry's trade council told *CPH Post Online.*

"With FAFPI, we are able to get to the root of the matter and take it up directly on a local level with our partners and the authorities," she added.

According to the FAFPI website, members will work to change the rules of the game by creating solid internal company and organisational policies and gathering data on when and where they meet demands for facilitation payment.

Data submitted through FAFPI will be shared with the Danish Ministry of Foreign Affairs who, through their diplomatic channels, can address the issue with their local counterparts in order to terminate the demands.

DI is an organisation that represents 10,000 companies having activities worldwide. "It's striking how little international co-operation there is across sectors regarding this kind of challenge," Christine Jøker Lohmann, a chief consultant at DI told *CPH Post Online*.

"An initiative like this is definitely part of the solution, because it is both a reporting tool that everyone can use and a network for exchanging information. It is vital that we break the taboo that still surrounds facilitation payments," added Lohmann. ~ *Source: CPH Post Online*

*Global shipping giant, Maersk has successfully reduced facilitation payments by 96 percent on Maersk Line-owned ships in 2017 compared to 2016, the company said in its latest Sustainability Report. *(members are referred to the March 2018 edition of CCI).*

from page 6 - Brexit and crime fighting

See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/645416/Security_law_enforcement_and_criminal_justice_-_a_future_partnership_paper.PDF

But whether this is achievable remains to be seen. EU member states may baulk at allowing the UK government to demand their police arrest a suspect and deliver them to the tender mercy of British justice, when their civil rights guaranteed in other member states through their EU citizenship are denied in a Brexited Britain.

So far, formal European Commission position papers have restricted themselves to more technical matters, with a June 2017 note on 'Ongoing Police and Judicial Cooperation in Criminal matters' looking at how relations with EU institutions and procedures should be wound up rather than renewed.

One bright note for law enforcers is that the Commission thinks that post-Brexit, the UK can keep and continue to use all criminal intelligence information, including personal data, obtained before the withdrawal date from other member states or EU institutions and bodies. And the remaining 27 member states can hold onto information transmitted in the past by the UK.

But that is about all in terms of future long-term arrangements.
See https://ec.europa.eu/commission/sites/beta-political/files/essential_principles_ongoing_police_and_judicial_coop_en.pdf

Moreover, one particular knotty issue to resolve will be the future status of Northern Ireland, which was addressed by a particularly controversial annexe tabled by the Commission in its draft withdrawal agreement.

These say that Northern Ireland would have to abide by EU laws, while the rest of the UK does not (to preserve a soft land border with the Republic of Ireland). This would mean that EU criminal law rules would continue to apply in the province. Moreover, there is a special clause in the annexe that the EU and the UK would be bound to work together to "counter fraud and any other illegal activities affecting the financial interests of the EU or the UK in respect of Northern Ireland." That would mean joint criminal work to police public spending on UK and EU programmes in Northern Ireland and to prevent VAT and customs fraud – giving a continued role in the province to the EU's anti-fraud agency OLAF.
**https://ec.europa.eu/commission/sites/beta-political/files/draft_withdrawal_agreement.pdf*

What are Unexplained Wealth Orders?

AN Unexplained Wealth Order ('UWO') is an order created by Section 1 of the Criminal Finance Act 2017. They entered into force in law in the UK on the 31 January 2018 (except Northern Ireland, at the time of writing).

However, they have been thrust into use quickly, with the National Crime Agency ("the NCA") obtaining two on the 28 February 2018. So in light of their first use, it seems sensible to ask, what is an Unexplained Wealth Order?

Simply, they are a civil court order and investigatory tool requiring the person subject to it to give information about the ownership of a property and the means by which it was obtained. It doesn't of itself involve the recovery of assets and is in addition to the recovery provisions under the Proceeds of Crime Act.

The use of a UWO is reserved to cases where it is suspected that a person's property has been purchased with the proceeds or corruption, money laundering or the proceeds of serious organised crime. The orders are retrospective and can apply where property has been obtained before the 31 January 2018.

Who can apply for a UWO?

The agencies that can apply for a UWO are limited. In England and Wales, the following agencies can apply:

- The NCA
- HMRC
- The FCA
- The SFO
- The CPS

That said, other prosecution agencies that are not on the list above can refer their cases to one of the above, thereby enabling them to access the use of a UWO, though through an intermediate agency.

What is the test for a UWO to be issued?

Broadly, the test for a UWO to be issued is as follows:

- Does the person own the relevant property (alone or with others)?
- Is it worth more than £50,000?

Are they a Politically Exposed Person (a prominent public official, or a friend or relative of one)? If not, are they either of the following:

- Reasonably suspected of being involved in serious crime (in the UK or elsewhere), or
- Reasonably suspected of being connected to a person involved in serious crime (in the UK or elsewhere)?

If the above is the case, then the next limb applies:

- Are there reasonable grounds to suspect that the person's known lawful income would be insufficient to allow the person to own the property considered?

The High Court must be satisfied of the above before they will make such an order.

How are UWOs used in practice?

There have, at the time of writing, only been two UWOs obtained, both by the NCA. It appears they have used them as investigatory tools - to determine how the properties were to be purchased and whether they could be recovered under a Civil Recovery Order.

There is of course a concern that any evidence produced in response to a UWO could be used against the person subject to the UWO.

Generally any evidence produced in response to a UWO cannot be used to prosecute the person subject to the order. Similarly to SFO compelled interviews, information provided in compliance with a UWO cannot be used against the giver except in limited circumstances.

These circumstances include:

- Recovery proceedings under Part 2 of POCA
- If false information is given in response (as described below)
- If the response is perjury.

How do you respond to a UWO?

The court will set a date by which the UWO (or sections of the UWO) will need to be responded to by, to whom the response needs to be sent and what form it should take.

The response will need to include information about the interest in the relevant property, and explain how the property was obtained including how any relevant costs were paid. The response will also need to cover how the property is owned.

What other powers accompany UWOs?

As took place in the two UWOs obtained to date by the NCA, Interim Freezing Orders ("IFOs") were also obtained. These must be applied for by the same authority applying for the UWO, and must be applied for at the same time.

An IFO can be made by the court when it considers it necessary to avoid a future recovery order being frustrated by the property being sold or dissipated. They essentially prevent the owner from dealing with the property. Whilst standard practice is hard to extrapolate from just two UWOs, it seems likely that such orders will be commonplace in order to protect any future application for recovery.

What if you don't comply?

There is a defence available of being unable to comply with the

Continued on page 9/

Fall in US enforcement actions against foreign officials

THE number of US enforcement actions concerning alleged bribery of foreign officials dropped to 14 in 2017, compared to a high of 29 in 2016, returning to a level more typically seen in the first half of the decade.

The number of non-US enforcement actions last year was 12, marginally up from 11 the year before, according to TRACE International Global Enforcement Report 2017.

European countries continue to predominate US investigations and enforcement actions in cases involving non-US companies and individuals, notably including the United Kingdom, Switzerland, Germany, and the Netherlands.

The report shows the US conducted 114 investigations concerning alleged bribery of foreign officials in 23 countries from 1977 to 31 December 2017.

There were 46 investigations involving companies headquartered outside of the US or individuals with non-US citizenship, representing 40 percent of all such investigations being conducted by the US.

Of the investigations concerning alleged bribery of foreign officials being conducted against non-US companies and individuals, the highest number involved companies or individuals in the United Kingdom, followed by Switzerland and Germany.

Companies or individuals from Europe made up 72 percent of US investigations concerning alleged bribery of foreign officials being conducted against non-US companies and individuals, followed by the Americas (excluding the US) with 13 percent, Asia Pacific with 11 percent, and the Middle East with 2 percent.

TRACE's report further shows that the US carried out 236 enforcement actions concerning alleged bribery of foreign officials, from 1977–2017. A total of 71 of these enforcement actions have involved companies headquartered outside of the US or individuals with non-US citizenship, representing approximately 30 percent of all enforcement actions initiated by the US.

Of the enforcement actions taken against non-US companies and individuals, the highest number involved companies or individuals in the United Kingdom, followed by the Netherlands and Switzerland.

Companies or individuals from Europe represent approximately 66 percent of US enforcement actions undertaken against non-US companies and individuals, followed by Asia Pacific with 20 percent, the Americas (excluding the US) with approximately 11 percent and Africa and the Middle East with 1.4 percent each.

With regards to bribes allegedly made by US companies, there appears to be an increasing focus on payments to European officials, for which the share of investigations increased to 20 percent from the 17 percent reported last year. The Asia Pacific region showed relative decreases in its share of both investigations and enforcement actions related to official bribery to US companies. *Source: TRACE International*

from page 8 - Unexplained Wealth Orders

requirements of a UWO in the given time to respond, that of "reasonable excuse".

What excuses may qualify are beyond the scope of this article, which instead will consider failure to comply without excuse. Suffice to say it would be risky to rely on the above argument, as the court will decide whether an excuse really was as "reasonable" as claimed.

Failure to respond results in the property (or the persons' interest in that property) being presumed to be recoverable, unless the contrary can be shown.

This obviously makes it easier for that property to be recovered at a later date by the enforcing agency.

So are there any related criminal offences?

Where a person makes a materially false or misleading statement in response to a requirement under a UWO, or recklessly makes such a statement they are guilty of an offence.

This offence can be tried at the Magistrates' Court for a maximum penalty of 6 months' imprisonment and/or a fine, and in the Crown Court for a maximum penalty of 2 years' imprisonment and/or a fine.

Conclusion

Overall the new UWO appears to be another useful tool in the arsenal of those UK agencies investigating and prosecuting corruption (and other serious crime) inside and outside the United Kingdom.

** This article has been written by Jeremy Asher, James Crighton and Stephen Sadler and first appeared on Ashfords website. https://www.ashfords.co.uk/article/what-are-unexplained-wealth-orders Source: Ashfords*

Cost of cyber attacks to financial services firms

CYBER attacks cost financial services' firms more to address and contain than in any other industry, and the rate of breaches in the industry has tripled over the past five years, according to a report from Accenture and the Ponemon Institute.

The report, 'Cost of Cyber Crime Study,' examines the costs that organisations incur when responding to cybercrime incidents and applies a costing methodology that allows year-over-year comparisons.

It found that the average cost of cybercrime for financial services companies globally has increased by more than 40 percent over the past three years, from US$12.97 million per firm in 2014 to US$18.28 million in 2017 – significantly higher than the average cost of US$11.7 million per firm across all industries included in the study.

The analysis focuses on the direct costs of the incidents and does not include the longer-term costs of remediation.

However, the report also notes while cyberattacks have a greater financial impact on the financial services industry than on any other industry, financial services firms continue to make prudent and sophisticated security technology investments that contribute to reducing the cost of breaches significantly.

The greatest proportion of financial services firms' cyber defence spending is for more advanced solutions like security intelligence systems, followed by automation, orchestration and machine-learning technologies.

"While the cost of cybercrime for financial services companies continues to rise, our research found that these companies have considerably more balanced and appropriate spending levels on key security technologies to combat sophisticated attacks than do those in other industries," said Chris Thompson, a senior managing director at Accenture who leads financial services security and resilience in the company's Security practice.

"This is particularly true with regard to the use of automation, artificial intelligence and machine-learning technologies, which could be critical to future cybersecurity efforts," he said. Among the key findings for the financial services industry:

- The average number of breaches per company has more than tripled over the past five years, from 40 in 2012 to 125 in 2017; that is slightly below the global average of 130 across all industries.
- Nearly two-thirds (60 percent) of financial services companies' total security costs is spent on containment and detection of cyber breaches.
- The greatest impact of cyber breaches on financial services firms are business disruption and information loss, which together account for 87 percent of the cost to respond to cybercrime incidents, with revenue loss accounting for only 13 percent.

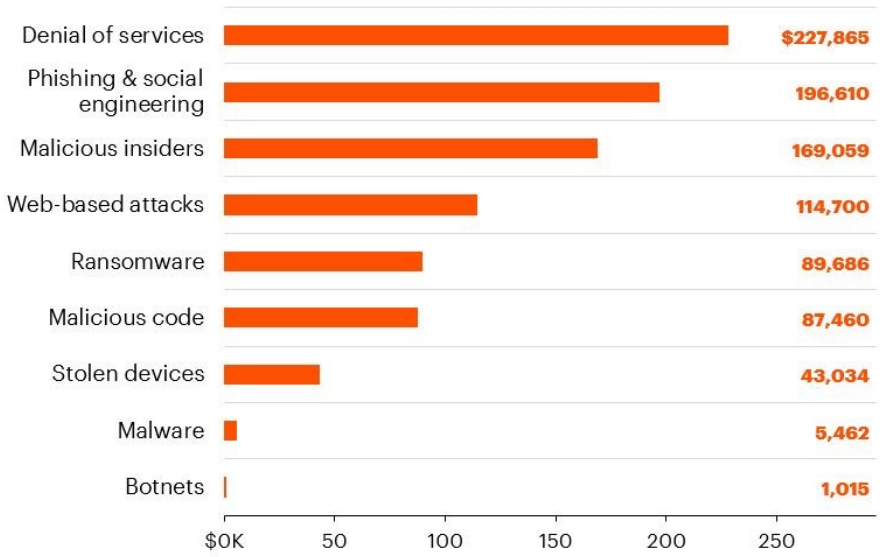

Image: Accenture

The report notes that more can be done with regards to security technologies deployed in financial services. Only one-quarter (26 percent) of financial-services companies have actually deployed AI security technologies, and fewer than one-third (31 percent) use advanced analytics to fight cybercrime. "Banks and other financial services firms have implemented advanced solutions for malware, reducing the susceptibility to such attacks, so the cybercrimes they're currently grappling with are largely different from those affecting other industries," Thompson said.

Source: Accenture

Employee training and infrastructure upgrades vital

EMPLOYEE training and infrastructure upgrades are considered as top priorities for securing financial institutions against cyber attacks, a survey has shown.

Thirty-five percent of the Chief Information Security Officers (CISOs) surveyed by the Financial Services Information Sharing and Analysis Center (FS-ISAC) said employee training was a top priority, while 25 percent said infrastructure upgrades and network defence were key. Seventeen percent said breach prevention was the most critical defence.

While cybersecurity used to be handled in the server room, it is now a board room topic, according to respondents.

On the frequency of reporting, the survey found that quarterly reports to the board of directors were most common (53 percent) with some CISOs (eight percent) reporting more than four times a year or even on a monthly basis.

"In the era of increasing security threats and vulnerabilities, CISOs know that keeping top leadership and boards updated regularly on these security risks and effective defences is a top priority," FS-ISAC said.

FS-ISAC recommends training employees be prioritised for all CISOs, regardless of reporting structure because employees serve as the first line of defence.

Employee training should include awareness about downloading and executing unknown applications on company assets, and in accordance with corporate policies and relevant regulations, and training employees on how to report suspicious emails and attachments.

FS-ISAC encourages more frequent and timely reporting to the board of directors to ensure businesses maintain an 'at the ready' risk posture and that cyber practices are transparent to board members.

As the threat landscape shifts, FS-ISAC recommends CISOs having expanded reporting responsibilities or dual-reporting responsibilities within the corporate structure to ensure critical information flows freely.

IN today's fast-moving world, getting access to information quickly and cheaply has never been more important, for as the saying goes, "who knows wins".

In this context the Internet provides an unrivalled facility to collect information and carry out research, yet some of its most useful specialised and publicly available search tools are largely unknown. There is also a considerable lack of knowledge as to how to use the Internet to maximum effect.

Acquiring useful and relevant Open Source Intelligence (OSINT) requires much more than just an ability to surf the Web - many valuable sources of intelligence are unknown and untapped by investigators.

Online and social media research and investigation skills are essential requirements at all levels of an organisation, from routine investigations conducted by frontline personnel to global, tactical and strategic Open Source Intelligence operations. ICC Commercial Crime Services has developed a three-day course at Queens' College, Cambridge University from 9 – 12 September 2018 aimed at managers, front-line investigators, researchers and analysts.

This comprehensive three-day training course taught by OSINT experts Toddington International Inc, will provide detailed instruction in effectively using the Internet as an Open Source Investigation and Research Tool.

What delegates will learn.

- An overview of the Internet and how it works.
- The ability to use the Internet in a more effective way as an open source/competitive intelligence tool.
- Advanced techniques to mine data using different search tools and uncover hidden information.
- Strategies for filtering, analysing and organising research data.
- An awareness of security and privacy issues, including techniques to both hide and increase visibilities of sites.

The course is highly practical and interactive and is led by David Toddington, who is a leading expert with a wealth of experience in his field. It will be of interest to a range of different individuals including:

- Corporate security professionals in banks, insurers and multinationals
- Fraud investigators, lawyers, accountants and analysts
- Competitive intelligence researchers
- Government and private sector investigators
- Law enforcement officers
- Knowledge workers and researchers

Fr more information go here. Alternatively e-mail: agalloway@icc-ccs.org.

Australia proposes prudential standard

THE Australian Prudential Regulation Authority (APRA) is seeking to introduce its first prudential standard aimed at tackling the threat of cyber attacks in the financial sector.

APRA has released a package of measures, titled Information Security Management: A new cross-industry prudential standard, for industry consultation.

The package is aimed at shoring up the ability of PRA-regulated entities to repel cyber adversaries or respond swiftly and effectively in the event of a breach.

The proposed new standard, CPS 234, would require regulated entities to:

- clearly define the information security-related roles and responsibilities of the board, senior management, governing bodies and individuals;
- maintain information security capability commensurate with the size and extent of threats to information assets, and which enables the continued sound operation of the entity;
- implement information security controls to protect its information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls;
- have robust mechanisms in place to detect and respond to information security incidents in a timely manner; and
- notify APRA of material information security incidents.

Executive Board Member Geoff Summerhayes said the draft standard built on prudential guidance first released by APRA in 2010 and backed it with the force of law.

"Australian financial institutions are among the top targets of cyber criminals seeking money or customer data, and the threat is accelerating," Mr Summerhayes said. "No APRA-regulated entity has experienced a material loss due to a cyber incident, but a significant breach is probably inevitable. In a worst-case scenario, a cyber attack could even force a company out of business."

Key areas where APRA is hoping to lift standards include assurance over the cyber capabilities of third parties such as service providers and enhancing entities' ability to respond to and recover from cyber incidents.

"Cyber security is generally well-handled across the financial sector, but with criminals constantly refining and expanding their tools and capabilities, complacency is not an option. Implementing legally binding minimum standards on information security is aimed at increasing the safety of the data Australians entrust to their financial institutions and enhance overall system stability, " said Mr Summerhayes.

New York issues VC guidance

NEW York State Department of Financial Services (DFS) has issued guidance reminding all virtual currency entities licensed by New York State, that they are required to implement measures designed to effectively detect, prevent, and respond to fraud, attempted fraud, and similar wrongdoing. DFS directed virtual currency entities to adopt measures that include, at a minimum, effective implementation of a written policy that:

- Identifies and assesses the full range of fraud-related and similar risk areas, including, as applicable, market manipulation;
- Provides effective procedures and controls to protect against identified risks;
- Allocates responsibility for monitoring risks; and
- As part of its procedures and controls to protect against identified risks, virtual currency entities must provide for the effective investigation of fraud and other wrongdoing, whether suspected or actual, including, as applicable, market manipulation.

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