COMMERCIAL CRIME International

July 2018

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

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

FIB urges caution after resurgence of high value shipments

ICC Financial Investigation Bureau (FIB) has seen a resurgence in extraordinarily high value shipments and requests to verify these shipments.

A FIB spokesperson said recently there was a request to verify a very large shipment of gold being shipped by air from Ghana to other parts of Europe. The quantity was in excess of 70 metric tonnes of gold.

FIB says it is unlikely that if such large quantities are shipped it would be handled by small, unknown private companies.

"It is almost always the exclusive the domain of governments and central banks around the world who may move these kinds of cargoes between themselves," FIB says.

"Any private company who purports to be the buyer or seller of a shipment of this kind should be treated with suspicion and banks should not get involved in it unless the transaction is verified, and the parties have a verifiable track record in this trade." FIB advised.

If not, it could be part of a high value investment scam or an advanced fee fraud.

FIB said in either case the monies are likely to be proceeds of crime and could involve money laundering placing banks at risk if they choose to participate in the transaction either as financiers or recipients of funds.

Advanced fee fraud and money laundering will be one of the topics to be discussed at the *13th ICC FIB International Financial Crime Forum* to be held in Kuala Lumpur on July 18 and 19.

Changing technology and its implications on compliance policies, artificial intelligence solutions in identifying financial crime, cybercrime, digital money and cryptocurrencies and the challenge these bring for anti- money laundering regulation and compliance will be among the main topics discussed at the meet.

"The Forum will look at practical approaches to identifying and tackling the potential pitfalls faced by those using financial instruments within international banking and financial services," a FIB spokesman said.

"The unique approach of this specialist interactive Forum presents delegates from around the world with the latest fraud trends and developments, and assists them in dealing with financial crime, money laundering and counter terrorism financing issues."

FIB said the Forum also provides delegates the opportunity to gain awareness on the changes being affected due to technological innovations. Products forming part of the FinTech or RegTech world are increasingly being offered to banks as a way to accelerate processes, reduce costs and risk. Competent advice on what really works and what doesn't is invaluable to banks being pushed inexorably down this path.

It is ideal for those from financial sector institutions such as national FIU's, international bank compliance and risk departments, regulators, lawyers, accountancy firms, stock brokers and law enforcement agencies. Other main topics include; *Banking governance in the new era, Multiple jurisdictions - legal challenges, Red Flags in fraudulent documents and Insolvency and fraud – tracing and recovering losses.*

To register your interest, go to www.icc-ccs.org/KL2018
Or Contact: Cyrus Mody (cmody@icc-ccs.org)
Telephone: +44(0)207 423 6960
Fax: +44(0)207 423 6961
Email: FIB@icc-ccs.org

In This Issue of CCI

FinTech/Artificial Intelligence

Transaction monitoring has potential for AI use in banks

THE UK's Financial Conduct Authority (FCA) is making the case for banks to turn to technology to deal with financial crime.

FCA's own analysis suggests that transaction monitoring is the area with the most potential, said Megan Butler, Executive Director of Supervision - Investment, Wholesale and Specialists at the FCA in a speech prepared for the recent Anti-Money Laundering (AML) TechSprint event in London.

"But it is by no means the only one. Onboarding, maintenance, client screening and reporting - among other issues – are frequently cited.

At the moment, we see a lot of firms using compliance technology to automate existing processes, so they keep on top of volume. Particularly reducing false positives in transaction monitoring," she said.

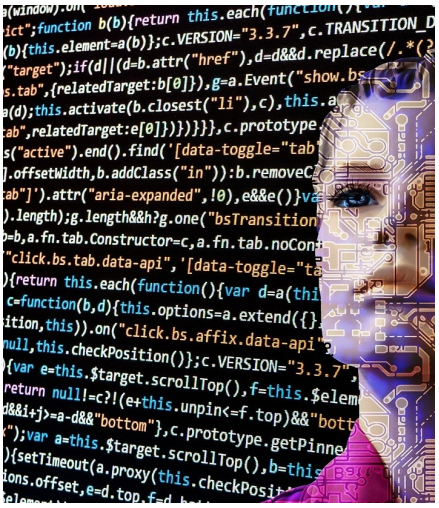
She added, "The next big step is to apply intelligent technologies - like AI, robotics, natural language processing and machine learning - so that firms can spot suspicious transactions in real time from unstructured account and transaction data."

However, the use of AI may not be that simple. "First, there are practical obstacles. A lot of large firms, for example, need to integrate legacy systems – in some cases dating back to the seventies. Others face significant clean-up exercises to address issues around fragmented, poor-quality data," said Ms Butler.

"Second, there are important questions around issues including bias and transparency. Proprietary algorithms, for instance, can become black boxes. Meaning developers themselves don't necessarily know why a machine is making the recommendations its making.

"In fact, last year the Financial Stability Board made a point of saying that communication mechanisms used by machine learning may be 'incomprehensible to humans'," she added.

What leeway is there for firms if something goes wrong?
"The question we get asked by financial institutions is essentially this: 'will you let me off the hook if we introduce new tech'? The answer to that is no.



"But that is not to say that new technology can't significantly reduce your risk exposure if you implement it in a way that you would any other – involving proper testing, governance and management," said Ms Butler.

Indeed, as reported on CCS' website recently, there are further indications that banks are increasingly teaming-up with technology firms to boost their financial crime fighting capacity by the use of AI.

In April, big data start-up Quantexa announced that following a successful pilot, its technology is supporting HSBC with the bank's work to combat money laundering.

HSBC will integrate Quantexa technology into its systems this year.

The technology will allow HSBC to spot potential money laundering activity by analysing internal, publicly available, and transactional data within a customer's wider network.

The deployment of the technology follows a pilot of the software with HSBC in 2017 and will see the global bank and data start-up work together to better detect potentially illegal activity in its broader context, helping the bank fulfil its regulatory responsibilities and provide better understanding of the overall risk.

In a similar development, Crèdit Andorrà Financial Group says it has selected NICE Actimize to strengthen its AML solutions strategy.

The bank will integrate a suite of NICE Actimize AML solutions into its financial crime operations to more effectively address AML regulations.

The move by both banks follow recent developments in RBS and OCBC Bank which have also turned to FinTech to guide their suspicious activity reports and AML work.

In November last year, OCBC said that it became the first Singapore bank to tap AI and machine learning to combat financial crime. The bank partnered with Fintech firm, Thetaray, to use its AI solution to identify potential suspicious transactions.

OCBC says the solution has reduced the volume of transactions reviewed by AML compliance analysts by 35 percent and increased the accuracy rate of identifying suspicious transactions by more than four times.

The bank also says it the first bank in Singapore to establish an AI unit to strategically develop in-house AI capabilities, with an initial investment of $10 million over three years.

AI in risk management and compliance to see 40% growth

ARTIFICIAL Intelligence (AI) in the Banking, Financial Services and Insurance (BFSI) sector is set to cross US$25 billion by 2024, according to a report by Global Market Insights.

When it comes to risk management, compliance, and security applications of AI in BFSI, a CAGR of 40 percent is forecast.

According to the report, the market is driven by the improved demand for advanced machine learning algorithms in Anti-Money Laundering (AML) and fraud detection applications.

Unlike the traditional security systems, the AI-powered system can actively learn and calibrate as per the new potential security threats. This solution can detect unique security issues and vulnerabilities and flag the security teams.

Meanwhile the insurance market is estimated to grow at a CAGR of over 38 percent during 2018-2024.

The growth of the market is credited with the adoption of advanced data models and analytics solution among the insurance companies to identify and quantify risks in a better manner.

Furthermore, increasing collaboration and partnership activities between insurers and FinTech companies are also the major factors propelling the growth of AI in BFSI sector.

Europe held more than 20 percent share in AI in BFSI. The investments by tech giants in the region support market growth.

Asia Pacific AI in BFSI market is estimated to grow at a CAGR of over 40 percent. The growth is owing to the rising venture capital investments in AI and FinTech.

The report says China is leading the investment landscape in Asia Pacific and similarly, India also accounts for significant investments in the AI and fintech sectors.

BERLIN-based SolarisBank has teamed up with Clarus.io, an Israeli Regtech startup that develops tools for detecting and preventing financial crime. The partnership will enable SolarisBank to streamline its compliance processes and thus scale its local and international activity using Clarus's transaction monitoring platform.

Transaction monitoring is often the overlooked element of AML Compliance. By analysing customer information procured during the KYC process, against the customers actual activity, suspicious patterns, outliers and activity that mirrors known money laundering schemes can be identified, investigated and reported.

'More laws needed' to tackle illicit use of digital currencies

THE US Secret Service says that additional laws are needed to tackle money laundering and the growing illicit use of digital currencies.

The organisation has urged US Congress to consider additional legislative or regulatory actions to address potential challenges related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e. cryptocurrency tumblers or mixers) and cryptocurrency mining pools.

Robert Novy, Deputy Assistant Director Office of Investigations US Secret Service said this in a testimony before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance last month.

He said the recently enacted CLOUD Act was an important step in this regard, but further legislative or regulatory action may be needed, as case law and business practices continue to develop.

"Such legislative or regulatory actions could take the form of new reporting requirements or data collection, retention, and accessibility requirements for certain businesses or business activities," Novy said.

The key US laws relevant to Secret Service investigations involving the illicit uses of digital currencies include the Bank Secrecy Act of 1970, the Annunzio-Wylie Anti-Money Laundering Act, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001, in addition to other associated laws and Federal regulations.

Novy said Congressional attention to the positive effects of these laws is especially needed, being in a period of significant technology innovation within the financial sector.

He said from Financial Year 2015 to present, the Secret Service has seized over $28 million in cryptocurrencies in the course of its criminal investigations, 12 primarily in the form of Bitcoin.

Survey: nearly 50% of global firms hit by fraud

ALMOST half of large global organisations have been the victims of fraud, theft, money laundering or other financial crimes, according to a Thomson Reuters survey.

Thomson Reuters commissioned the survey of more than 2,300 senior business leaders in large companies to shine a light on how pervasive such crimes have become across the world.

The report, 'Revealing the True Cost of Financial Crime', shows that 47 percent of people questioned admitted that their organisation had suffered at least one incident of financial crime over the past 12 months, with cybercrime and fraud cited as the most common financial crimes. The companies surveyed estimated a total aggregated loss of $1.45 trillion, or around 3.5 percent of their global turnover.

The difficulty of tackling financial crime is starkly set out in the survey. Thomson Reuters found that organisations questioned do business with an average of five million customers or clients every year, and 9 percent of organisations have dealt with over 10,000 third party vendors, suppliers or partners over the last 12 months.

According to the report, however, only 36 percent of relationships are regularly screened for criminal connections. The survey suggests that 41 percent of parties that respondents did business with over the past 12 months were not screened at all.

Furthermore, 41 percent of known instances of financial crime are not reported, either internally or externally.

The reasons for this include 69 percent of detected bribery and corruption involving someone internally, 55 percent of privately owned companies concerned about reputational damage and financial loss, and 60 percent of publicly listed companies which claimed there would be a significant negative impact on investor confidence if such crimes came to light.

The report reveals the scale of the challenges society faces in fighting financial crime, with its impact felt well beyond large companies.

Taking money laundering as an example, 46 percent of respondents think that it leads to higher prices for consumers and 42 percent believe it leads to lower government revenues.

Almost all those surveyed recognised that greater collaboration is vital to winning the war against financial crime, with 94 percent of companies believing there should be more sharing of financial crime intelligence, while 93 percent said that public-private partnerships should be increased and improved.

95 arrested in global online fraud crackdown

IN a major crackdown against online fraud, 95 fraudsters and members of internet-based criminal networks suspected of online fraud activities were arrested during an operation carried out by Europol.

The 2018 e-Commerce Action (eComm 2018), held from June 4 to 15, was supported by 28 countries.

Europol said the suspects arrested during the operation were responsible for more than 20,000 fraudulent transactions with compromised credit cards, with an estimated value exceeding €8 million.

After several months of preparation, police carried out house searches, arrests, interviews, confiscation of fraudulently purchased goods like mobile phones or expensive clothes and financial instruments.

Photo: Europol

More than 200 house searches were carried out involving more than 200 private sector partners.

Europol said investigative measures were very complex due to the virtual and international dimension of this crime. They revealed that not only individual fraudsters, but the involvement of organised crime groups.

There are indications of professionalism and links to other forms of crime like phishing, malware attacks, creating websites and using social media platforms for frauds.

Banks may need to do more to support APP fraud victims

UK's Financial Conduct Authority (FCA) has proposed changes to complaint handling rules to help victims of authorised push payment fraud (APP).

UK Finance data on APP fraud or bank transfer fraud show there were 43,875 cases of APP fraud and total losses of £236 million in 2017.

Where their own payment services provider (PSP) is not at fault, victims of APP fraud cannot at present complain to the PSP receiving their payment. The FCA is consulting to require firms to handle these complaints in line with complaints handling rules in the FCA Handbook.

The FCA is also proposing to allow eligible complainants to refer these complaints to the Financial Ombudsman Service if they are unhappy with the outcome reached by the receiving PSP, or if they have not received a response to the complaint at all.

The FCA also plans to consult, later in the year, on requiring PSPs to report data on the complaints about alleged APP fraud that they receive. This data can be used by the industry as an indicator of progress on APP fraud and to inform FCA supervisory work.

The newspaper *Telegraph Money* says the move is a major victory for its 'Make Banks Act on Fraud' campaign, allowing victims to complain to a bank despite not being a customer.

Telegraph Money says it has consistently called on the banks which received the stolen money, and often breached money laundering regulations by allowing an account to be opened with false credentials, to do more to support victims.

Most are told they must liaise with their own bank and are given spurious reasons, including data protection, for the recipient bank's silence.

Many of these sorts of scams involve life-changing sums. One of the most common types of case involves a criminal impersonating a conveyancer and stealing money for a house deposit. The worst case *Telegraph Money* has seen resulted in the victim losing £600,000.

The FCA shares concerns with the Payment Systems Regulator (PSR) and the industry that APP fraud is a growing problem. This consultation published today builds on the work of the FCA and PSR to better protect consumers from APP fraud. The FCA and PSR investigated APP fraud and found that PSPs could do more to identify fraudulent incoming payments and prevent accounts from being compromised by fraudsters.

"UK Finance data on APP fraud show there were 43,875 cases of APP fraud and total losses of £236 million in 2017.

Christopher Woolard, FCA Executive Director of Strategy and Competition, said, "The FCA takes push payment fraud and the harm it causes to consumers very seriously. Our proposals build on our work in this area and seek to reduce the harm experienced by victims of push payment fraud where they believe the bank who received the money did not do enough to prevent it.

"We are proposing to require payment service providers to handle complaints about this in line with our complaint handling rules, and to provide the victims with access to the Financial Ombudsman Service."

THE stage is being set for a legal battle in Malaysia's 1MDB fraud case against former prime minister Najib Abdul Razak.

Malaysian press are reporting that the country's Attorney General will lead the prosecution team, assisted by former attorney-general Abdul Gani Patail, who co-heads the special task force investigating the 1MDB.

The government is seeking to recover $4.5 billion following allegations of corruption, money laundering and fraud. Press reports say Mr Najib has assembled a formidable US-based legal team, led by former US attorney-general John Ashcroft. Ashcroft Law Firm registered Mr Najib as a client on the United States Foreign Agents Registration Act (FARA) register.

Ashcroft is known for handling high-profile international cases involving global players. According to Reuters' sources, another US lawyer in the team is star litigator David Boies, who specialises in antitrust cases, including acting for the US government in its case against IT giant Microsoft and aided fallen financiers that included AIG's Hank Greenberg and Enron's Andy Fastow.

The same sources claimed that another top American lawyer, Mr Matthew Schwartz, is also part of Mr Najib's legal team. Mr Schwartz, has handled several high-profile cases including the investigation into Bernie Madoff

Art market: controls tighten as fears over criminal abuse grows

A series of money laundering and illicit trade incidents in recent years has brought the art market under the watchful eye of anti-money laundering authorities. Commercial Crime International investigates the extent of the problem and the way the sector will be affected by new European anti-money laundering regulations.

By Michael Kosmides in London

IN July 2016, the US authorities accused Malaysian officials of embezzling more than US$3 billion from Malaysia's sovereign fund 1Malaysia Development Berhad (1MDB) – alleging significant portions of the proceeds bought paintings by Monet, Picasso, Van Gogh and others.

The case is now coming to a head with the fall from power of former Malaysian Prime Minister Najib Razak, who is accused of profiting from 1MDB. The alleged thefts have brought into light the alleged practice of auction houses functioning as unofficial banks, providing loans of dubious provenance to customers with art pieces as collateral. According to experts, such transactions may make money laundering possible as the borrower may repay the loan by selling the artwork, ending up with cleaned loan money.

On March 2, (2018) the US Department of Justice prosecuted in federal court a case where a ring, including a British art dealer, offered to an undercover FBI agent he opportunity to launder US$50 million from a stock exchange fraud through the sale of Picasso's painting 'Personnages'.

According to an Interpol statement, "the black market in works of art is becoming as lucrative as those for drugs, weapons and counterfeit goods." Dr Christos Tsirogiannis, Forensic Archaeologist, Lecturer for the Association for Research into Crimes against Art (ARCA), told *Commercial Crime International* that "the exact amount will always remain unknown due to the numbers that will never been known exactly. We can only judge from the cases that are being revealed as illicit and we can be certain only for these amounts and from then onwards we can only speculate."

"The art market, like any other market, is exposed to risks of money laundering," Sandrine Giroud, partner with LALIVE law firm in Geneva, and RAM (Responsible Art Market Initiative) task force member told *Commercial Crime International*. But she said that despite the cases of fraud that have made the headlines, it is "difficult to articulate any figure…but definitely a reality."

5th anti-money laundering directive

However, art dealers are soon to face anti-money laundering controls comparable to those in the financial industry. The European Union's fifth anti-money laundering directive (5AMLD), whole rules should largely be implemented by the end of 2019, includes in its list of high-risk transactions subject to special monitoring by financial institutions and dealers those "related to… artefacts and other items of archaeological, historical, cultural and religious importance." Traders will have to verify the identity of clients for any transaction over €10,000 under any payment method.

The International Confederation of Art and Antique Dealer Associations (CINOA) says in a position paper that the directive will "have an enormous impact on the European antiques, art and antiquities market by creating an unacceptable burden" and that the "measures are disproportionate to the risk".

At present, only a relatively small group of 'high value dealers' dealing with cash only need to comply with EU money laundering rules – and their national implementation regulations. However, the 5AMLD will affect most major traders, said Janet Ulph, commercial law professor at the University of Leicester Law School.

There also questions, she said, in relation to whether the 5AMLD will affect sellers on platforms such as eBay. Within the key UK art market, any dealer falling with the scope of the directive will probably need to register with Her Majesty's Revenue & Customs (HMRC) and to pay a fee for doing so.

Funding of terrorism has been of major concern within the art market. "Over the past decade we have seen an increasing trend of illicit trafficking in cultural objects from counties in the Middle East affected by armed conflict," said a note from Interpol. In its June (2018) report to the Parliamentary Assembly of the Council of Europe (not part of the EU), its committee on culture, science, education and media noted that the black-market trade in antiquities, art and artefacts is "moving away from the traditional means of trading towards social media and internet."

The report said, "it has been suggested that cultural property is the third most lucrative source of funding for illegal activities…Evidence suggests that the trade in objects looted in conflict zones follows routes already established by networks of handlers which may then be utilised for the purpose of funding terrorism."

Continued on page 7/

Singapore recommendations against trade-based ML

SINGAPORE'S Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) Industry Partnership (ACIP) has recommended a set of best practices for financial institutions to guard against trade-based money laundering and the misuse of company structures for illicit purposes. The ACIP best practice papers highlight the "red flag" customer behaviours or transaction patterns that financial institutions can look out for to detect illicit financial activities.

The first paper is Legal Persons-Misuse Typologies and Best Practices, and the second paper is Best Practices for Countering Trade Based Money Laundering. They also recommend measures that financial institutions can take to identify or prevent such activities.

The Papers were produced by two industry-led working groups, comprising representatives from major banks, professional service providers and government agencies in Singapore. The recommendations are also relevant for professional service providers outside the financial sector, such as lawyers, accountants and company services providers.

The Papers are available on the website of the Association of Banks in Singapore (ABS). The Commercial Affairs Department (CAD) and the Monetary Authority of Singapore (MAS) encourage all relevant firms to adopt the red flag indicators and recommended measures to strengthen resilience against money-laundering and terrorism-financing risks.

from page 6 - art market and money laundering

At the centre of money laundering allegations has been the Chinese art market which is growing in value as well as in the number of collectors and artworks. "As such, there is a risk that best practices may not keep up with the pace of growth," said Giroud. But she noted that "the Chinese government has emphasised the need for a healthy and regulated development of culture and the art market."

Sergey Skaterschikov, managing director at Zurich-based wealth management firm, Lighthouse Capital, told *Commercial Crime International* that the Chinese authorities did not want the market structure to be compromised by "bad behaviour and they cracked down on those involved by changing business models and using the People's Liberation Army and all the other tools at their disposal to bring discipline and regulation to the market."

KYC checks

The risks for art traders depend "on the parties involved, the artwork in question and the nature of the transaction," noted Giroud. RAM has published an art transaction due diligence toolkit that analyses the issues in these categories and can be used by art businesses to help them comply with an evolving regulatory framework. But while "big institutions like big auction houses and galleries are clearly aware of the problem and have adopted certain policies to learn and reduce the risk," said Skaterschikov, the problem is that "most of the art trade is really happening outside of the auctions in private deals".

The evolution of cryptocurrencies, such as Bitcoin, makes the market even more complex. The Dadiani Syndicate is the world's first special purpose vehicle that facilitates foreign investment into the UK markets utilising crypto-economic means. This includes accepting cryptocurrencies as payment for works of fine art.

Its founder, Eleesa Dadiani, told *Commercial Crime International* that trading with cryptocurrencies rather than in money transactions can be very different "because indeed there are instances when individuals simply want to have outlets for their questionable gains, and this to some provides the perfect avenue to do that." However, she argued, the right checks eliminate that risk, allowing for "efficiencies far and away beyond anything ever experienced in trade."

"As with any 'ordinary' trade (via fiat currency), we carry out a KYC - know your client [assessment]. We do not do trades with anonymous individuals... Motive, is an important factor here - do they want to transact for the purpose of anonymity or simply because they have made substantial profits from early investments and wish to use that against real assets, and understanding motive is key - this goes beyond the standardised checks," said Dadiani.

The art world seems to be in the grip of a tightening noose regarding money laundering. In the USA, the House of Representatives financial services committee is currently considering legislation under the proposed 'Illicit Art and Antiquities Trafficking Protection Act (H.R. 5886)' which would add "dealers of art and antiquities" to the list of regulated financial institutions under the USA Bank Secrecy Act, increasing controls in the US$26.6 billion American art market.

Cybercrime

74 arrested over business email compromise scheme

SEVENTY-four people have been arrested in a coordinated international enforcement operation targeting hundreds of individuals in Business Email Compromise (BEC) schemes

Operation Wire Wire was carried out by the US Department of Justice, US Department of Homeland Security, US Department of the Treasury and the US Postal Inspection Service, was conducted over a six-month period.

The arrests were made in the US (and other countries, including 29 people in Nigeria, and three in Canada, Mauritius and Poland.

The operation also resulted in the seizure of nearly $2.4 million, and the disruption and recovery of approximately $14 million in fraudulent wire transfers.

The US authorities worked with partners in Nigeria, Poland, Canada, Mauritius, Indonesia, and Malaysia to enforce the operation.

Since the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) began keeping track of BEC and its variant, Email Account Compromise (EAC), as a complaint category, there has been a loss of over $3.7 billion reported to the IC3.

US Department of Justice said money mules may be witting or unwitting accomplices who receive ill-gotten funds from the victims and then transfer the funds as directed by the fraudsters.

The money is wired or sent by check to the money mule who then deposits it in his or her own bank account.

Usually the mules keep a fraction for "their trouble" and then wire the money as directed by the fraudster.

The fraudsters enlist and manipulate the money mules through romance scams or 'work-at-home' scams.

BUSINESS Email Compromise (BEC), also known as 'cyber-enabled financial fraud,' is a sophisticated scam often targeting employees with access to company finances and businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

The same criminal organisations that perpetrate BEC also exploit individual victims, often real estate purchasers, the elderly, and others, by convincing them to make wire transfers to bank accounts controlled by the criminals.

This is often accomplished by impersonating a key employee or business partner after obtaining access to that person's email account or sometimes done through romance and lottery scams.

BEC scams may involve fraudulent requests for checks rather than wire transfers; they may target sensitive information such as personally identifiable information (PII) or employee tax records instead of, or in addition to, money; and they may not involve an actual 'compromise' of an email account or computer network.

Here are the most current and frequent BEC scenarios identified by the FBI.:

Business Executive

Criminals spoof or compromise e-mail accounts of high-level business executives, including chief information officers and chief financial officers, which result in the processing of a wire transfer to a fraudulent account

Real Estate Transactions

Criminal impersonate sellers, realtors, title companies, or law firms during a real estate transaction to ask the home buyer for funds to be sent to a fraudulent account

Data and W-2 Theft

Criminals, using a compromised business executive's e-mail account, send fraudulent requests for W-2 information or other personally identifiable information to an entity in an organisation that routinely maintains that sort of information.

Supply Chain

Criminals send fraudulent requests to redirect funds during a pending business deal, transaction, or invoice payment to an account controlled by a money mule or bad actor

Law Firms

Criminals find out about trust accounts or litigation and impersonate a law firm client to change the recipient bank information to a fraudulent account.

UK financial watchdog issues crypto assets guidance

BRITAIN'S Financial Conduct Authority (FCA) has written to banks' chief executive officers about good practice to handle the risks posed by crypto assets.

FCA says that while there are many non-criminal motives for using crypto assets, such product can also be abused because it offers potential anonymity and the ability to move money between countries.

It has cautioned banks to take reasonable and proportionate measures to lessen the risk of facilitating financial crimes which are enabled by crypto assets.

FCA says where banks offer banking services to current or prospective clients who derive significant business activities or revenues from crypto-related activities, it may be necessary to enhance their scrutiny of these clients and their activities.

Services may include:

- where banks offer services to crypto asset exchanges which effect conversions between fiat currency and crypto assets and/or between different crypto assets.
- trading activities where banks clients' or counterparties' source of wealth arises or is derived from crypto assets.
- where banks wish to arrange, advise on, or take part in an 'initial coin offering' (ICO).

In these situations, FCA says appropriate steps or actions to consider may, subject to the circumstances and services being provided, include:

- developing staff knowledge and expertise on crypto assets to help them identify the clients or activities which pose a high risk of financial crime
- ensuring that existing financial crime frameworks adequately reflect the crypto-related activities which the firm is involved in, and that they are capable of keeping pace with fast-moving developments
- engaging with clients to understand the nature of their businesses and the risks they pose
- carrying out due diligence on key individuals in the client business including consideration of any adverse intelligence
- in relation to clients offering forms of crypto-exchange services, assessing the adequacy of those clients' own due diligence arrangements
- for clients which are involved in ICOs, considering the issuance's investor-base, organisers, the functionality of tokens (including intended use) and the jurisdiction.

"Following a risk-based approach does not mean banks should approach all clients operating in these activities in the same way," FCA says.

"Instead, we expect banks to recognise that the risk associated with different business relationships in a single broad category can vary, and to manage those risks appropriately," FCA added.

Customers using crypto assets
Some banks' customers or clients may be holding or trading crypto assets and selling them may be the source of a customer's wealth or funds. In a retail context, this may be discovered by, for example, enquiring about the source of a deposit, or because the customer has previously made large transactions with crypto asset exchanges.

Existing requirements for checking the source of wealth and funds are risk-sensitive; firms are given the flexibility to adapt their actions to the perceived risks.

Firms should assess the risks posed by a customer whose wealth or funds derive from the sale of crypto assets, or other crypto asset-related activities, using the same criteria that would be applied to other sources of wealth or funds.

For example, in the case of retail clients, the criteria they would apply to a property transaction, inheritance, or sale of a valuable artwork or car.

FCA says one way crypto assets differ from other sources of wealth is that the evidence trail behind transactions may be weaker.

"This does not justify applying a different evidential test on the source of wealth and we expect firms to exercise particular care in these cases. Where a firm identifies that a customer or client is using a state-sponsored crypto asset which is designed to evade international financial sanctions, we would see this as a high-risk indicator," advises FCA.

It adds that retail customers contributing large sums to ICOs may be at a heightened risk of falling victim to investment fraud. In 2012 the Financial Services Authority (FSA) reviewed how banks then handled the risk of investment fraud, including the risk of retail customers becoming victims of this crime.

GOLDMAN Sachs has teamed up with a UK security firm, Immersive Labs, to enhance the cyber security skills of its employees, according to a statement. The bank will teach its employees about combating cyber threats using gamification, via a virtual learning programme created by Immersive Labs.

It gives users different cyber attack scenarios and teaches them how to deal with the threats.

Cobalt group still active and targeting financial firms

THERE are warnings that the Cobalt hacking group are still active despite the arrest of their leader with a report of a recent phishing attack on financial institutions.

On May 23, Group IB's threat intelligence experts recorded a new large-scale cyberattack made by the group on the leading banks of Russia and the CIS. The last attacks in Russia were made five months ago, in December 2017.

The first wave of the phishing campaign was tracked on May 23 at 13:21 Moscow time. Phishing emails were sent purporting to be from a major anti-virus vendor. The user received a "complaint" in English that activity was recorded from their computer that violated existing legislation.

The recipient was asked to read the attached letter and provide detailed explanations. If the response was not received within 48 hours, the 'anti-virus company' threatened to impose sanctions on the recipient's web resources.

In order to download the letter, the user was asked to follow a link, which would then infect the Bank employee's computer.

A few days later on May 28, 2018, 1 pm (Moscow time), Group-IB staff detected another phishing campaign. Emails purporting to be from the European Central Bank were sent from the email address "v.constancio@ecb-europa[.]info" to financial institutions.

The phishing letter contained a link to the file '67972318.doc', designed to appear as a document describing financial risks.

The Microsoft Word triggers the exploitation of the CVE-2017-11882 vulnerability. After the file is executed, the malware infects the bank's system. Group-IB experts say that there are potentially other victims, not only banks in Russia and CIS countries, as the spear phishing emails were written in English suggesting foreign banks as targets.

As with the earlier attack, Group IB says the quality of phishing emails as high. For example, in the May 23 attack, the text in English worded as a "legal complaint", and the fake website kaspersky-corporate.com is also of high quality, which is not typical of Cobalt's modus operandi.

Group IB says these and other signs again point to the possibility that the remaining members of the Cobalt group were conducting a joint operation with other criminal groups, in particular, Anunak.

Cobalt's evolution

Cobalt first conducted attacks against banks in Hong Kong and the Ukraine which resulted in SWIFT incidents in the spring of 2016.

In both events advanced understanding of banking technology and money laundering capabilities enabled the group to perform the attacks and successfully launder money.

Following the 2016 SWIFT incidents, attacks involving interbank transfer systems ceased and Cobalt switched focus to other critical systems in banks such as ATMs.

This was followed by Card Processing attacks which provide a safer withdraw process for money mules. Cobalt's first major attack was against First Bank in Taiwan where attackers managed to steal over $2 million dollars.

Following this, Cobalt was then successful in targeting the card processing systems at a bank in Kazakhstan taking over two months to prepare their attack and successfully steal $600,000 through card processing. These attacks were then perfected and intensified in 2017 across tens of incidents.

Cobalt only conducted new attacks on SWIFT 18 months after the April 2016 incidents. In December 2017 for the first time in Russia, they made a successful attack on a bank through SWIFT. This incident was the first SWIFT theft in the history of the Russian banking industry.

According to Europol, these threat actors have been linked to thefts of approximately one billion euros. One of the largest single attempted thefts was of over €25 million from a European bank via card processing.

Supply chain attacks and Cobalt's non-typical targets

Throughout the last two years of activity, Cobalt's has been highly active with group members continuously testing new methods and tools. In addition to banks, Cobalt has also targeted supply chain attacks.

In February 2017 Group-IB responded to a successful attack

Continued on page 11/

Asset managers plan to increase cybersecurity spending

A new report has revealed that improving cybersecurity is one of the key business priorities for asset managers this year in response to a greater perceived threat of cybersecurity attacks.

The report, from Osney Media and BackBay Communications, shows that cybersecurity improvements are a key business priority for 33 percent of asset managers. It was launched recently at The Summit for Asset Management (TSAM) in London.

Two-thirds (65 percent) of the senior asset management professionals surveyed believe that the threat posed to their organisation from cybercrime this year is greater than in 2017; this compares with just 2 percent who said it is less of a threat.

As a result, investments to improve cybersecurity measures by the asset management industry are anticipated to rise, with 50 percent of respondents saying their organisation plans to increase expenditure in this area in 2018.

The findings follow a spate of high profile and disruptive cyber attacks and data breaches in 2017 across a number of sectors, including financial services.

With millions of trades placed each day and huge amounts of financial data held by asset managers, it is a sector considered to be at particular risk.

For firms with clients and operations in the EU, the introduction of GDPR, in May is also likely to sharpen their focus on cybersecurity.

"Cybersecurity is clearly in focus for asset managers right now," said Jonathan Wiser, Director at Osney Media. He added, "Not only is it firmly on the agenda for regulators, but with the vast majority of firms turning to technology to enhance the services they offer to customers and drive down costs, they need to make sure they have appropriate cyber defences in place. The potential operational and reputational risks from a breach are immense."

The research reveals that 66 percent of respondent firms are currently undergoing a digital transformation project - to incorporate new technologies into the heart of their business operations and processes - with a further 18 percent planning such a project.

The main reasons cited for such projects were to improve or automate middle- and back-office processes (71 percent), improve fund distribution and enhance the client experience (65 percent), and improve research and investment decision-making (35 percent).

from page 10 - Cobalt hackers still active

on a system integrator which Cobalt used as a vehicle to conduct further attacks on organisations in Russia and former CIS countries.

In the nine months following this incident, Cobalt infiltrated at least four IT Integrators including those in the US.

Cobalt's attacks include other non-typical targets. In March 2017, they infiltrated a company providing electronic wallets and payment terminals, successfully stealing through a payment gateway.

Back then Group-IB staff detected phishing emails disguised as "Moneta.ru", an e-wallet payment system. It was a spear-phishing attack on the companies providing electronic wallets and payment terminals. Eight companies in Russia and Ukraine were the targets of this attack.

"Cobalt hackers are armed and still dangerous."

~ Group IB

During the incident, attackers managed to transfer more than US$2 million. Cobalt has continued supply chain attack insurance agencies and the media.

In these attacks, they obtain control of mail servers or accounts to further use the victim's infrastructure for attacks on banks.

In September, Cobalt successfully attacked a company which produces software for payment terminals.

In this incident Group-IB was able to discover clear evidence of Anunak involvement and ultimately confirmed the hypothesis of joint operations between the two groups.

Detailed information with technical indicators of the groups' operation is provided in the report 'Cobalt: Evolution and Joint Operations'.

Cybercrime

TSB sees rise in phishing emails attacks

UK's Action Fraud has warned about a sharp rise in fraudsters sending out fake text messages and phishing emails claiming to be from British retail bank TSB.

Action Fraud says since the start of May, there have been 321 phishing reports made to Action Fraud – an increase on the previous month where 30 reports were made.

In the same reporting period, there have been 51 reports of cybercrime to Action Fraud which mention TSB – an increase on the previous month, where 24 reports were made.

Action Fraud and TSB are working together to combat fraud and help keep all consumers safe.

The increase in the number of reports being sent to Action Fraud is in part linked to the system issue some TSB customers have experienced over recent weeks.

Opportunistic fraudsters are using TSB's system issue to target people with this type of fraud.

Fraudsters are commonly using text messages as a way to defraud unsuspecting victims out of money.

This is called 'smishing' (SMS plus phishing). Of the smishing attempts reported to Action Fraud, 80 percent requested that the recipient click onto a website link. The second most common delivery technique reported has been email.

Action Fraud says fraudsters are using specialist software which changes the sender ID on text messages so that it looks like messages are being sent by TSB.

In some instances, this spoofed text is being added to existing TSB message threads on victim's phones.

Should someone click on the link within a spoofed text message and enter their personal information, the fraudsters then call the victim back and persuade them to hand over their one-off code from their mobile phone. The fraudsters can then empty the victim's account.

A TSB Fraud spokesperson has said that, "While our systems are safe and secure, unfortunately fraudsters are increasingly sophisticated and looking to take advantage of situations like these by approaching customers."

TSB said that protecting its customers' information is our number one priority, and that it is doing all it can to ensure customers don't become a victim of fraud, whether they bank with us in branch, online or via the telephone and this is something it is working on with Action Fraud and a number of external organisations.

"We are also working with these organisations to help them identify fraudulent sites so we can take them down as quickly as possible," said TSB.

THE INTERPOL National Central Bureau (NCB) in Brasilia and Banco do Brasil S/A have signed an agreement for cooperation and information sharing to tackle cybercrime.

This public-private partnership, which came into effect on May 7, aims to establish a systematic exchange of data related to cyber threats so as to enhance cyber security activities undertaken by INTERPOL and its 192-member countries.

As part of the agreement, Banco do Brasil will second a representative to INTERPOL's Global Complex for Innovation (IGCI) in Singapore to work alongside specialists from other technology and financial companies, as well as with INTERPOL officers on secondment from member countries.

The bank already works with the Brazilian Justice and Federal Police.

The signing of the agreement will trigger the development of information technology solutions and strategic tools to prevent and fight cybercrime.

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