Thinking about Crime

the money laundering consultancy

AML webinar:
Enemies inside and out

Jersey Compliance Officers Association

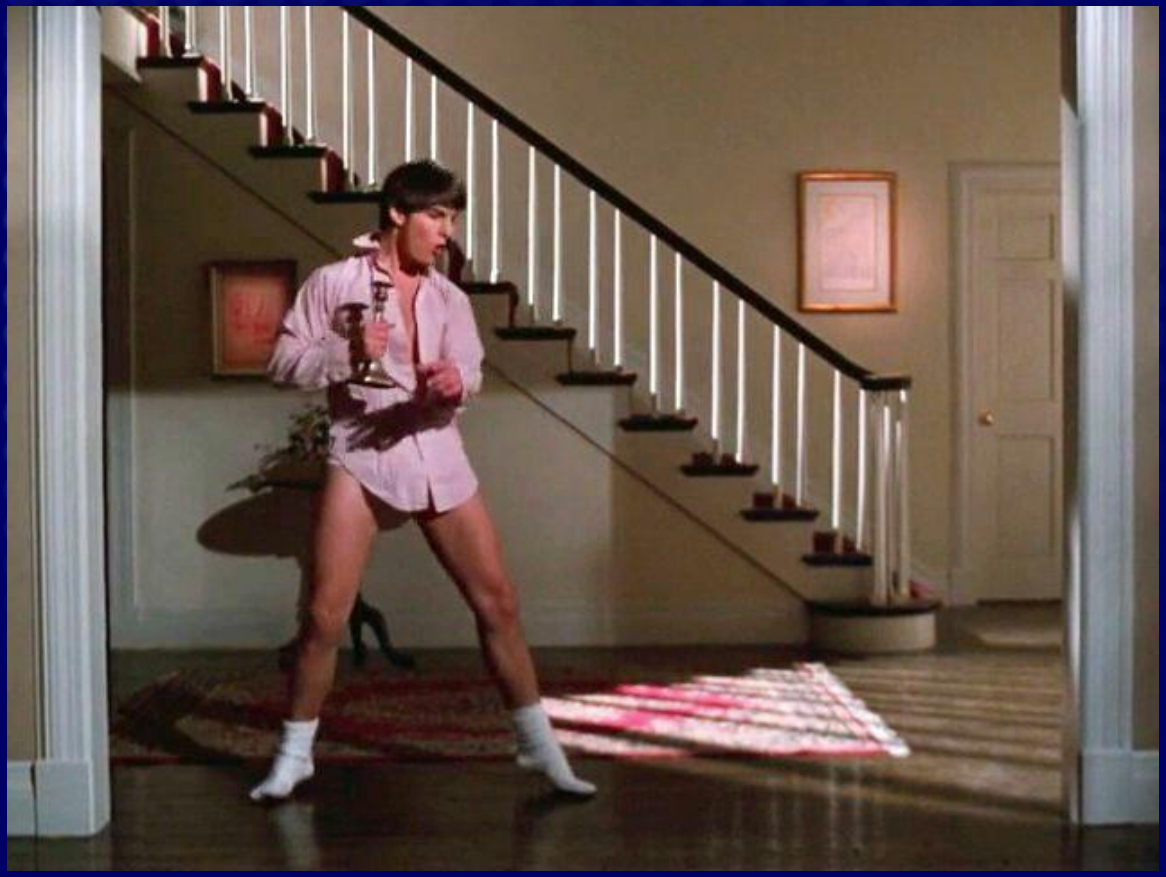
3 June 2020

JCOA
jersey compliance officers association

Today's agenda

- Risky business: gathering and assessing lists of high-risk jurisdictions
- The enemy within: staff concerns and conducting internal investigations

Risky business



Legislation

- As well as a general requirement for “countries and territories” and “geographic sphere” to be among the factors which contribute to a risk assessment, section 3.3.4.1 of the *Handbook* states that “country risk” must take note of:
  - countries on the FATF list (some of which count as “enhanced risk states” in the Order)
  - “major illicit drug producers or through which significant quantities of drugs are transited”
  - countries known for people trafficking, terrorism, proliferation of nuclear or other WMD, or corruption
  - countries “in which there is no, or little, confidence in the rule of law… or in government effectiveness”, or which are politically unstable
  - countries subject to sanctions
  - countries “that lack transparency or which have excessive secrecy laws”

Practicalities

- Many will choose to maintain a high risk countries list in the form of a grid
  - down the side are all the jurisdictions
  - across the top are the various characteristics
    - member of the FATF; appears on Corruption Perceptions Index, etc.
- This approach means that staff can quickly see where their due diligence enquiries should focus
  - this client is active in a jurisdiction known for endemic corruption
  - but this client's money is coming from a jurisdiction known for drug production and export
- It is important to keep historical versions of your list so that you can demonstrate, if required, that you were taking the correct steps and approach at any point in the past
  - it's easy to forget that once upon a time wildlife trafficking was on no-one's radar, ditto modern slavery

Concern number 1: non-cooperative tax jurisdictions

- In June 2015, as part of its “Action Plan for Fair and Efficient Taxation”, the European Commission published a consolidated list of all third countries named by Member States as being of concern with regard to tax
  - this consolidated list featured 121 jurisdictions
- The first agreed list was published on 5 December 2017, and featured seventeen jurisdictions on the “black list” (or Annex I) – these are the “non-cooperative jurisdictions for tax purposes”
- The others were put onto a “grey list” of “committed jurisdictions”, subject to ongoing monitoring

Concern number 1: non-cooperative tax jurisdictions

- On 23 January 2018 eight jurisdictions were moved from the black list, “following commitments made at a high political level to remedy EU concerns”
  - Barbados, Grenada, Macao SAR, Mongolia, Panama, South Korea, Tunisia and the United Arab Emirates
- On 13 March 2018 three were removed
  - Bahrain, the Marshall Islands and Saint Lucia
- And three were added
  - Bahamas, Saint Kitts and Nevis and US Virgin Islands
- On 25 May 2018 two were removed
  - Bahamas and Saint Kitts and Nevis
- On 2 October 2018 Palau was removed
- On 6 November 2018 Namibia was removed
- Left on the “black list” at this point were American Samoa, Guam, Samoa, Trinidad and Tobago, and US Virgin Islands

Concern number 1: non-cooperative tax jurisdictions

- On 12 March 2019 the EC moved to the “black list” (from the “grey list”) ten jurisdictions that “did not implement the commitments they had made to the EU by the agreed deadline”:
  - Aruba, Barbados, Belize, Bermuda, Dominica, Fiji, Marshall Islands, Oman, UAE and Vanuatu
- On 17 May 2019 Aruba was removed from the “black list”
- On 14 June 2019 Dominica was removed
- On 10 October 2019 the UAE was removed
- On 8 November 2019 Belize was removed
- On 18 February 2020 Cayman Islands, Palau, Panama and Seychelles were added
- There are now twelve jurisdictions on the “black list”:
  - American Samoa, Cayman Islands, Fiji, Guam, Oman, Palau, Panama, Samoa, Seychelles, Trinidad and Tobago, US Virgin Islands and Vanuatu

Concern number 1: non-cooperative tax jurisdictions

- The “grey list” (or Annex II) of “committed jurisdictions” now comprises:
  - Anguilla; Australia; Bosnia and Herzegovina; Botswana; Eswatini [formerly Swaziland]; Jordan; Maldives; Mongolia; Morocco; Namibia; Saint Lucia; Thailand; Turkey
- You can keep up with who’s in and who’s out:
  - https://ec.europa.eu/taxation_customs/tax-common-eu-list_en

Concern number 2: the FATF list

- Three times a year (in February, June and October) the Financial Action Task Force publishes a list of jurisdictions with poor AML/CFT regimes
- This list was last updated on 21 February 2020:
  - jurisdictions to which counter-measures apply:
    - Democratic People's Republic of Korea
  - jurisdictions to which compulsory EDD applies:
    - Iran
  - jurisdictions under the regular review regime:
    - Albania *[new entrant]*; Bahamas; Barbados *[new entrant]*; Botswana; Cambodia; Ghana; Iceland; Jamaica *[new entrant]*; Mauritius *[new entrant]*; Mongolia; Myanmar *[new entrant]*; Nicaragua *[new entrant]*; Pakistan; Panama; Syria; Uganda *[new entrant]*; Yemen; Zimbabwe
    - Trinidad and Tobago was removed from monitoring
- The first two groups are considered "enhanced risk states" and the Order requires that ECDD must be applied

Concern number 3: the EC list

- In February 2018, there were sixteen countries on the European Commission's list of jurisdictions considered to have weak AML/CFT regimes
- Since then the listing methodology has changed, taking more note – for example – of strictness around beneficial ownership information
  - https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en

Concern number 3: the EC list

- This would leave twelve adopted from the FATF list (at the time):
  - Bahamas, Botswana, Ethiopia, Ghana, Iran, North Korea, Pakistan, Sri Lanka, Syria, Trinidad and Tobago, Tunisia and Yemen
- Plus eleven added by the EU:
  - Afghanistan, American Samoa, Guam, Iraq, Libya, Nigeria, Panama, Puerto Rico, Samoa, Saudi Arabia and the US Virgin Islands
- On 8 March 2019 this revised list was unanimously rejected by the EU Member States and returned to the EC for another attempt

Concern number 3: the EC list

- On 7 May 2020 the EC published its new list
  - https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en
- From October 2020, closer scrutiny will be required of clients who have dealings with these countries
  - companies in the listed countries will also be banned from receiving new EU funding
- Jurisdictions on the list:
  - Afghanistan; Bahamas; Barbados; Botswana; Cambodia; Ghana; Iran; Iraq; Jamaica; Mauritius; Mongolia; Myanmar; Nicaragua; North Korea; Pakistan; Panama; Syria; Trinidad and Tobago; Uganda; Vanuatu; Yemen; Zimbabwe

Concern number 4: drugs

- The “International Narcotics Control Strategy Report 2020” was published by the US Department of State on 2 March 2020
  - https://www.state.gov/2020-international-narcotics-control-strategy-report/
- Volume II (“Money Laundering and Financial Crimes”) is the interesting one
- “The INCSR is mandated to identify ‘major money laundering countries’ [and] is required to report findings on each country’s adoption of laws and regulations to prevent narcotics-related money laundering.”
- “A ‘major money laundering country’ is one ‘whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking’. The determination is derived from the list of countries included in INCSR Volume I (which focuses on narcotics) and other countries proposed by US government experts based on indicia of significant drug-related money laundering activities.”
- Included in the list of 82 countries this time round are the US and the UK, but not Jersey (or Guernsey, or the Isle of Man, or Gibraltar)

Concern number 5: corruption

- Transparency International's Corruption Perceptions Index 2019 was published on 23 January 2020
  - https://www.transparency.org/en/cpi/2019
- Ranks 180 countries and territories by their perceived levels of corruption, as determined by thirteen surveys and expert assessments
- Least corrupt: New Zealand and Denmark, then Finland, then Switzerland, Singapore and Sweden, then Norway
  - UK is at position 12 [down from 11 last year]
- Most corrupt: Somalia, South Sudan, Syria, Yemen, then Afghanistan, Sudan, Equatorial Guinea and Venezuela
- "Our analysis also shows corruption is more pervasive in countries where big money can flow freely into electoral campaigns and where governments listen only to the voices of wealthy or well-connected individuals."
  - "Governments must urgently address the corrupting role of big money in political party financing and the undue influence it exerts on our political systems."

Concern number 6: sanctions

- Sanctions can target individuals, entities (companies, trusts, partnerships, charities, etc.) or entire jurisdictions
- Sanctions in Jersey are administered by the Ministry for External Relations
  - www.gov.je/Government/Departments/JerseyWorld/pages/sanctionsfaq.aspx
- Compliance with financial sanctions is overseen by the JFSC
  - www.jerseyfsc.org/industry/international-co-operation/sanctions/
- Jersey recognises sanctions issued by the UN, the UK and the EU, as well as its own sanctions, and sanctions – of varying types – are currently in place targeting individuals and entities in many jurisdictions/categories:
  - Afghanistan; Belarus; Burundi; Central African Republic; chemical weapons; cyber-attacks; Democratic Republic of Congo; Egypt; Haiti; Iran; Iraq; ISIL (Da'esh) and Al-Qiada terrorist organisations; Lebanon; Libya; Mali; Myanmar; Nicaragua; North Korea; Republic of Guinea; Republic of Guinea-Bissau; Russia; Serbia and Montenegro; Somalia; South Sudan; Sudan; Syria; Tunisia; Turkey; Ukraine; UNSCR 1373; Venezuela; Yemen; and Zimbabwe
- Penalties for breaching vary according to the individual piece of legislation, but it's always a fine and/or imprisonment

Concern number 7: political stability and rule of law

- The World Bank's Worldwide Governance Indicators "report on six broad dimensions of governance:
  - voice and accountability
  - political stability and absence of violence
  - government effectiveness
  - regulatory quality
  - rule of law
  - control of corruption"
- You can search on one or more indicators, for all countries, one country or a subset
  - https://info.worldbank.org/governance/wgi/

Concern number 7: political stability and rule of law

- Every March the World Justice Project publishes an annual Rule of Law Index
  - https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020
  - in 2020, the countries which ranked poorest were Venezuela, Cambodia, Democratic Republic of the Congo, Egypt, Cameroon, Mauritania and Afghanistan
  - top spots went to Denmark, Norway, Finland, Sweden and the Netherlands

Concern number 8: passports and “golden visas”

- According to the most recent Passport Index from Henley & Partners (“a global citizenship and residence advisory firm”), the most powerful passports in the world are:
  - Japan: allows visa-free access to 190 countries
  - Singapore / South Korea: 189
  - France / Germany: 188
  - Denmark / Finland / Italy / Sweden: 187
  - Luxembourg / Spain: 186
  - Austria / Netherlands / Norway / Portugal / Switzerland / UK / US: 185
- The price of a passport depends on its power and on the difficulty of obtaining a genuine one
  - in order to become Japanese you must have lived in Japan for more than five years, be of good moral character, demonstrate financial independence, surrender your birth nationality – and explain in a hand-written letter (in Japanese!) why you want to become a Japanese citizen

Concern number 8: passports and “golden visas”

- “Golden visa” schemes offer citizenship or residency in exchange for investment
  - EU countries offering such schemes include Austria, Cyprus, Hungary, Latvia, Lithuania, Malta, Portugal – and the UK
  - Montenegro (which hopes for EU membership) launched its scheme on 3 October 2019)
    - apparently it expects to raise a billion euros from its scheme by the end of 2021
  - Caribbean nations offering them are Antigua and Barbuda, Dominica, Grenada, St Kitts and St Lucia
- In this way, people can end up with multiple passports, and can pick and choose which one to offer, depending on what they think the reaction will be
  - one reaction they might hope for is a reduction in CDD checks…
- Useful research on current schemes is published by the Organised Crime and Corruption Reporting Project
  - www.occrp.org/en/goldforvisas/

Concern number 9: specific jurisdictions – Russia

- An oligarch is a ruler in an oligarchy (!)
  - an oligarchy is a power structure in which control and power rest with a small number of people
    - they often lead to tyranny and corruption
- In the context of Russia, “the Russian oligarchs” are business leaders of the former Soviet republics who rapidly accumulated wealth during the era of Russian privatisation in the aftermath of the dissolution of the Soviet Union in the 1990s
- According to *Forbes* magazine and the *Sunday Times* “Rich List 2018”, the two wealthiest Russian oligarchs living in the UK are:
  - Alisher Usmanov – steel and iron ore – once owned 30% of Arsenal FC – worth £11.79 billion
  - Roman Abramovich – oil – owns Chelsea FC – worth £9.3 billion

Concern number 9: specific jurisdictions – Russia

- Roman Abramovich also has rights of residency in Jersey
- In March 2018, Kevin Lemasney (director of high-value residency at Locate Jersey) confirmed to the *JEP* that four Russians have been accepted as high-value residents, who receive special tax breaks, under the '21E' laws in the past five years, but that all of the applicants faced strict approval procedures
  - "The criteria and process for approvals are rigorous and transparent and we do not do deals. All applicants – Russian or otherwise – have the same right to privacy under Jersey law, and we will continue to uphold that."

Concern number 9: specific jurisdictions – China

- China operates controls on its capital – Chinese citizens can take a maximum of US$50,000 out of China per year
- They have regular (often politically motivated) crackdowns on corruption
  - in 2013 the Central Commission for Discipline Inspection investigated 51,000 people for corruption, bribery, embezzlement and abuse of power – and punished 30,420 of them
- Between 1995 and 2008, more than 18,000 officials fled China, smuggling out assets totalling 800 billion yuan [about £77 billion]
  - but the numbers are falling, thanks to Operation Fox Hunt (looking for corrupt officials hiding overseas) and stiffer controls on the issuing of passports to officials and their families

Hints and tips for researching high risk situations

- Adverse information may not be found in mainstream national media, for various reasons
  - in some countries the media are tightly controlled and censored
  - the subject of the research may control or influence local media
  - high profile individuals can be highly litigious when it comes to negative coverage, which can deter journalists and news organisations
- Major commercial aggregators of news and media sources do not provide universal coverage
  - you should also look at local media coverage – particularly if not in English
  - look at coverage in the relevant trade press – and take into account both the range of publications and the extent of archived material

Hints and tips for researching high risk situations

- Commercial databases of PEPs and other high risk individuals are fallible
  - few jurisdictions publish official lists of PEPs, and so the commercial databases are aggregations of information that is not always complete or current
  - a ‘nil return’ on a commercial database does not guarantee that the individual is not (or never has been – still crucial in Jersey) a PEP or a high risk customer
  - foreign name translations or transliterations introduce additional complications
    - phonetic matching can help identify possible matches but this is slow and cumbersome – many systems default to exact matching only
- Consider varying your reviews – if you simply check the same things over and over again (the same search terms, or the same resources), you will get the same results

The enemy within

Employees in the Order

- Article 11(1):
  - " A relevant person must maintain appropriate and consistent policies and procedures relating to… screening of employees… in respect of that person's financial services business carried on in Jersey or elsewhere, or a financial services business carried on in Jersey or elsewhere by a subsidiary of that person, in order to prevent and detect money laundering."

The JFSC's position in the *Handbook* (Section 9.1)

- "The effective application of even the best designed systems and controls (including policies and procedures) can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, systems and controls (including policies and procedures), and are not adequately trained.
- "It is essential that a relevant person takes action to make sure that customer-facing and other employees are:
  - Competent and have probity;
  - Aware of policies and procedures and their obligations under the [relevant AML legislation]; and
  - Trained in the recognition of notable transactions or activities (which may indicate money laundering or financing of terrorism) or transactions and activity with enhanced risk states and/ or sanctioned countries."

The JFSC's position in the *Handbook* (Section 9.2)

- "A relevant person may demonstrate that employees are screened where it does one or more of the following, as appropriate for the nature of the employee's role and responsibilities:
  - Obtains and confirms references.
  - Obtains and confirms employment history and qualifications disclosed.
  - Obtains details of any regulatory action taken against the individual (or absence of such action).
  - Obtains and confirms details of any criminal convictions (or absence of such convictions)."

FATF typologies

- On 26 July 2018 the FATF published a research paper on "Professional Money Laundering"
  - www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf
- Much of it deals with people doing laundering as a job, but Section VI looks at "Complicit/criminal financial service providers and other professionals"
  - "Professional money launderers may occupy positions within the financial services industry (e.g. bankers and money value transfer service agents) and DNFBP sectors (e.g. lawyers, accountants and real estate professionals), and use their occupation, business infrastructure and knowledge to facilitate money laundering for criminal clients. The use of occupational professionals can provide a veneer of legitimacy to criminals and organised crime groups. As such, organised crime groups actively seek out insiders as potential accomplices to help launder illicit proceeds."
  - "In rare circumstances, criminals may be able to compromise entire institutions or businesses, including by acquiring ownership or control of the institution and appointing their own criminal management."

FATF typologies: bank employees

- “Complicit bank employees may perform functions such as:
  - creating counterfeit cheques
  - monitoring (or not appropriately monitoring) money flows between accounts controlled by the co-conspirators
  - co-ordinating financial transactions to avoid SAR reporting
  - accepting fictitious documents provided by clients as a basis for transactions, without asking any additional questions
  - performing ‘virtual transactions’ on the accounts of their clients – numerous transactions conducted, without an essential change of the net balance at the beginning and end of a working day.”

FATF typologies: bank employees

- “Private banking advisors may act as professional money launderers and provide services to conceal the nature, source, ownership and control of the funds in order to avoid scrutiny, by employing various techniques, including:
  - opening and transferring money to and from bank accounts held in the names of individuals or offshore entities, other than the true beneficial owners of the accounts
  - making false statements on bank documents required by the bank to identify customers and disclose the true beneficial owners of the accounts
  - using ‘consulting services’ agreements and other similar types of contracts to create an appearance of legitimacy for illicit wire transfers
  - maintaining and using multiple accounts at the same bank so that funds transfers between those accounts can be managed internally, without reliance on international clearing mechanisms that are more visible to law enforcement authorities
  - opening multiple bank accounts in the names of similarly-named companies at the same, or different, institutions so wires do not appear to be coming from third parties.”

FATF typologies: TCSP employees

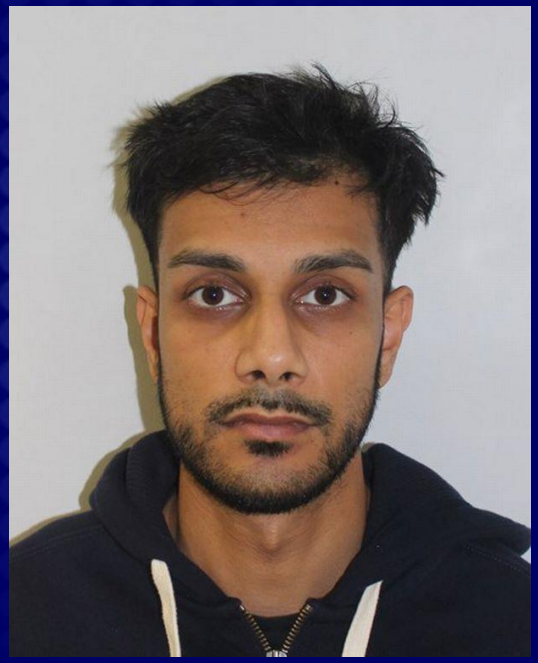
- “Professional services may be used, such as the services of a TCSP or a lawyer, when setting up a shell company. Such professionals can supply a full range of services, including the incorporation of the company, the provision of resident or nominee directors, and the facilitation of new bank accounts.”
- “TCSPs are often blind to what their clients actually use the companies for, and therefore do not consider themselves complicit in money laundering schemes. However, a number of case studies have demonstrated that some TCSPs market themselves as ‘no questions asked,’ or being immune from official inquires. Moreover, if the TCSP also acts as the director of the company, the TCSP has to perform these duties as a director and could be held liable for the offences committed by the company.”

FATF typologies: TCSP employees

- “A handful of current investigations across the globe have indicated that TCSPs act as nominee directors of corporate structures with similar behaviours, observed whether large corporates or smaller TCSPs, including:
  - using a ‘tick the box’ approach for compliance activity
  - distancing themselves from risk (i.e. downplaying their responsibility)
  - utilising chains of formation agents in multiple jurisdictions
  - engaging in deliberately negligent behaviour
  - forging signatures and fraudulently notarising documents.”

Inside job

- Moldovan cybercriminals Pavel Gincota and Ion Turcan used a Trojan horse virus to install Dridex malware on victims' computers
  - this enabled them to steal login information for online banking, and they made 42 separate bank transfers – stealing a total of £2.5 million
    - the medical firm Galen Research lost more than £500,000 after one of its employees clicked on a Word document attached to an email in May 2015
- Jinal Pethad worked at the Ealing branch of Barclays as a business support worker – his colleagues called him "the go-to guy" because he was so helpful



Inside job

- Pethad set up 105 bank accounts for Gincota and Turcan, using fake ID documents
  - he managed the accounts to ensure that incoming deposits were not blocked by the bank's security processes and that the pair could transfer money freely between the accounts
- According to the NCA:
  - "Pethad abused his position of trust at the bank to knowingly set up sham accounts for Gincota and Turcan, providing a vital service which enabled them to launder millions. Using his knowledge of the financial system, he made sure the stolen money was not blocked before entering these accounts, and provided the pair with reports to evidence his efforts and maintain the criminal relationship."
- On 12 December 2017 he was jailed for six years and four months
- Gincota and Turcan had already been jailed
  - five years and eight months for Gincota
  - seven years for Turcan

Inside job, part 2

- In a related case (in that it involves Gincota's brother Ryingota and Barclays) personal banking manager Nilesh Sheth helped a gang of five cybercriminals to launder £16 million
- He was tempted by cash payments and used his office at the bank to meet the gang
  - he opened 400 accounts for the five men by using fake ID documents
- The NCA tracked him and observed him meeting the men in restaurants and car parks
- On 2 November 2017 Sheth was jailed for four years
  - the five cybercriminals were jailed for a total of nearly thirty years

Inside job, part 3

- Taminder Virdi and Abubakar Salim worked at the Stoke Newington branch of TSB
- Accountant Babar Hussein worked in tandem with them to open 65 accounts at the branch, using stolen driving licences and fake utility bills
- They then stole £390,000 from TSB customers and transferred the money into these accounts
  - Virdi then moved on to Santander, where he continued offending
- All three were jailed on 7 May 2019
- Mike Hulett, Head of Operations at the NCA's National Cyber Crime Unit:
  - "Hussain is a professional money launderer who used his accountancy knowledge to steal hundreds of thousands of pounds from elderly banking customers. He was aided by two corrupt bank workers who abused their positions of trust, using false documents to set up bank accounts to launder the hard earned savings of their unsuspecting victims. As soon as the first victim reported the theft we used our specialist cyber capabilities to follow the money and established the real world identities of these criminals."
- The victims were reimbursed by the banks

Why do employees go over to the dark side?

- In November 2018 law firm White & Case and the University of Manchester published “Global White Collar Crime Survey: Anti-bribery and corruption”
  - www.whitecase.com/sites/whitecase/files/global-white-collar-crime-survey.pdf
  - 252 respondents around the world were asked 82 questions
- 19% do not have ABC policies
  - a further 10% don’t know whether they do or not
- 40% of respondents from legal/compliance functions say they have sometimes felt under pressure to approve third party engagement despite ABC red flags
- The benefits for those who accept bribes are seen to be multiple:
  - praise/promotion for bringing in new business
  - greater job security
  - being part of the “club”

New ABC guidance

- Transparency International has published new "Global Anti-Bribery Guidance: Best practice for companies in the UK and overseas"
  - www.antibriberyguidance.org
- It covers
  - top-level commitment
  - risk assessment and planning
  - policies and procedures
  - high risk areas
  - managing third parties
  - communications and training
  - monitor and review
  - reporting

Conducting internal investigations

- Two types:
  - where there is little likelihood of enforcement action – the investigation is conducted for internal purposes and may or may not be shared with the JFSC
  - where there is the possibility or likelihood of enforcement action by the JFSC
    - in this case, particularly great care must be taken with the conduct of the investigations

Conducting internal investigations: self-reporting

- Consider involving the JFSC early in the process, i.e. self-reporting
  - from the *Handbook* (Section 2.3): “The Board must notify the Commission immediately in writing of any material failures to comply with the requirements of the Money Laundering Order or of the AML/CFT Handbook.”
- Remember that self-reporting counts as mitigation when it comes to the assessment of penalties
  - “The particular enforcement measures, or combination of measures adopted, will depend on factors such as… the degree of cooperation and openness displayed by the person concerned” (from the JFSC’s guidance note on their use of enforcement powers)

Conducting internal investigations: co-operation

- The best way forward is often a co-operative investigation
  - the firm knows its own people, roles, responsibilities, procedures, processes and record-keeping arrangements
  - the JFSC offers independence
    - you can mimic this by paying a third party to conduct the investigation for you – but that costs money
- But you must be alive to the possibility that your own investigation could prejudice or hinder a subsequent JFSC investigation
  - discuss this with the JFSC before you launch your own investigation
- And sometimes the risks of prejudice to a JFSC investigation are insurmountable, particularly in the case of potential criminal offences
  - e.g. tipping-off risks might mean it is not possible for a firm to conduct its own investigation without alerting the individuals whom the JFSC would prefer to monitor covertly for the time being

Conducting internal investigations: ground rules

- When you are establishing the ground rules with the JFSC (i.e. who does what, and the scope of your internal investigation), they will want to establish:
  - to what extent will they be able to rely on the report of your investigation in any subsequent enforcement proceedings?
  - will they have access to the underlying evidence or information that was relied upon in producing the report?
  - will you be willing to disclose material over which you claim legal privilege?
  - how will evidence be recorded and retained?
  - have any conflicts of interest been identified, and how do you propose to manage them?
  - will the investigation be limited to ascertaining facts, or will it also include advice or opinions about breaches of JFSC rules or requirements?
  - how do you intend to inform the JFSC of progress and communicate the results of the investigation?
  - what is the expected timescale for completion of your investigation and report?

Conducting internal investigations: interviews

- Interviewing employees who are suspected of wrongdoing (or who are whistle-blowing about wrongdoing) is a skill
- Moreover, the circumstances in which a person is asked to give an account of events, or their own actions, can be critically important to the reliability and admissibility of that evidence in later proceedings
- You may well need to take legal advice on this
  - or indeed draft in someone with the legal skills needed to conduct such interviews

Conducting internal investigations: interviews

- Guidance from ACAS
  - www.acas.org.uk/index.aspx?articleid=5507
- Guidance from the (US) Society of Corporate Compliance and Ethics
  - www.assets.corporatecompliance.org/Portals/1/Users/169/29/60329/Workplace_Investigations_Guide.pdf
- (Detailed) guidance from the Health & Safety Executive
  - www.hse.gov.uk/enforce/enforcementguide/investigation/witness-questioning.htm
- (Very, very detailed) guidance from law firm Kingsley Napley – UK-focused but shows the level of decision-making involved
  - www.globalinvestigationsreview.com/benchmarking/the-practitioner%E2%80%99s-guide-to-global-investigations-third-edition/1179082/witness-interviews-in-internal-investigations-the-uk-perspective

What to do with an employee who is under suspicion

- Suspension
  - may be necessary if the alleged wrongdoing poses a threat to the business, colleagues or client
  - suspension should be kept under regular review
  - the employee should continue to receive their salary and benefits as normal
- Disciplinary procedure
  - the normal disciplinary process applies
    - i.e. the employee must be told what sanctions are being considered (including dismissal), written warnings must be given (unless the conduct amounts to gross misconduct), alternative sanctions should be considered, and a right of appeal must be given

What to do with an employee who is under suspicion

- Sanction
  - you do not have to wait for the outcome of criminal proceedings before conducting a disciplinary hearing and sanctioning (including dismissing) an employee
    - criminal cases can take months – even years – to get to court and waiting for the outcome could cause serious issues for you and your business
  - you are not bound by the outcome of a criminal trial
    - if you decide through the disciplinary process that an employee's conduct warrants dismissal, you are entitled to make this decision even if the employee is not charged or convicted
    - conversely, just because the employee is charged with a criminal offence, you do not have the automatic right to dismiss them – any dismissal must still be reasonable

What to do with an employee who is under suspicion

- Reputational considerations
  - you may wish to help your employee with the cost of legal representation for their defence
    - particularly if their interests and yours are aligned, e.g. convincing the JFSC that you did nothing wrong
  - and of course their conviction would have a negative impact on your firm's reputation, so facilitating their access to quality representation might given them a better chance of avoiding charge or conviction
  - it would be wise to make it a condition that any financial contribution is kept confidential
    - there could be extra reputational damage if they are found guilty and it's put about that you "tried to get them off it"

Protection for honest employees

- Previously, whistle-blower protection in the EU was fragmented
- But on 16 December 2019 the new Whistle-blower Directive came into force:
  - protects whistle-blowers who report a violation of EU law – e.g. tax fraud, money laundering, data protection violations
  - covers employees, trainees, volunteers and self-employed workers
  - requires companies with more than 50 employees to take measures to protect whistle-blowers and to establish confidential whistle-blower channels and clear reporting processes
  - whistle-blowers are encouraged – but not obliged – to report observations first through internal channels
  - whistle-blowers (and their supporters, such as colleagues or family members) benefit from special legal protection against all forms of retaliation (such as dismissal, degradation or intimidation) and are given access to legal, financial and psychological support
- Transposition deadline is 17 December 2021
- https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

Whistle-blowing in Jersey

- The JFSC runs a whistle-blowing hotline (01534 887557)
  - “Information we receive from whistleblowers helps us to identify cases of regulatory misconduct.
  - If you are aware or suspect that a business you work for or interact with may be involved in wrongdoing, we would ask you to contact us.
  - You can be assured that we treat any information we receive in the strictest confidence and will use it as intelligence for cases.
  - You can call our anonymous, untraceable whistleblowing line at any time.
  - If you call during office hours, you will speak to a member of our Enforcement team. If they are unavailable, or it is outside of normal working hours, you can leave a message.”

And finally…..

- Thank you for your attention and participation
- If you have any questions, please contact me:

Susan Grossey

01223 563636 or 07813 070771

susan@thinkingaboutcrime.com

www.ihatemoneylaundering.wordpress.com