PARAMETRIC INSIGHTS

ECONOMIC CRIME UPDATES

HELLO!

Welcome to the fifth edition of our newsletter! We hope that you will find our content useful, practical and engaging.

At Parametric Global Consulting, we focus on helping our clients navigate complex economic crime issues effectively through independent and impartial investigations and reviews, tailored training, and strategic advice.

We want you to be prepared to respond to legislative, policy and geopolitical changes, and our newsletter will keep you abreast of the swiftly evolving landscape.

Get in touch with us if you need our assistance with any investigation, consulting, or training needs in your organisation.

Do share the newsletter and sign up to our mailing list so that you are kept up to date!

I hope that the month ahead is fab and productive!

Best,

Lloydette
Founding Partner

Parametric Global Consulting

Follow us on Linkedin and Twitter!

WHAT'S IN STORE?

Please click on headings to go to section

CONTACT US

Tel No: +44 208 058 3120

Email: info@parametricglobal.co.uk

Website

Linkedin

Twitter

CASE UPDATES

FORMER FORMULA ONE BOSS, BERNIE ECCLESTONE, CHARGED WITH FRAUD BY FALSE REPRESENTATION AFTER HMRC INVESTIGATION.

Former Formula One boss and billionaire Bernie Ecclestone will face a charge of fraud by false representation after a HMRC investigation allegedly found undeclared offshore assets in the excess of £400m. The CPS said earlier this month that it authorised the charge following Ecclestone's failure to declare the assets' existence. The first hearing is scheduled to take place in August 2022. Simon York, director of HMRC's fraud investigations services, described the tax authority's criminal investigation into Ecclestone as "complex and worldwide … HMRC is on the side of honest taxpayers and we will take tough action wherever we suspect tax fraud. Our message is clear – no one is beyond our reach."

APPLE'S FORMER SENIOR LAWYER ADMITS INSIDER TRADING SCHEME

Apple's former director of corporate law (2008-2013) and co-chairman of the company's Disclosure Committee pleaded guilty to engaging in an insider trading scheme spanning five years. Gene Levoff pleaded guilty before a U.S. District Judge to six criminal counts of securities fraud. Levoff is described to have "betrayed the trust of one of the world's largest tech companies for his own financial gain". Despite being responsible for enforcing Apple's own ban on insider trading, Levoff ignored both the related policy and regular quarterly blackout periods and used his position of trust to commit insider trading. From February 2011-April 2016, Levoff misappropriated material and non-public information about Apple's financial results, and executed trades involving the company's stock. This scheme allowed him to realize profits of approximately $227,000 on certain trades and avoid losses of approximately $377,000 on others. The securities fraud counts each carry a maximum penalty of 20 years in prison and a $5m (around £4.1m) fine. Sentencing is scheduled for November 2022.

THIRD UNAOIL CONVICTION QUASHED BY THE U.K COURT OF APPEAL

This month, the UK's Court of Appeal quashed a third criminal conviction in Unaoil, one of the SFO's biggest corruption cases. At the same time, a government-ordered review exposed serious failings in the high-profile bribery case. Four men were jailed for conspiracy to provide corrupt payments, after the SFO's investigation into bribes to secure profitable oil contracts in post-occupation Iraq. The quashing of the conviction of Stephen Whiteley, former vice president at SBM and Unaoil's territory manager for Iraq, follows the overturned convictions of two other defendants - Ziad Akle (former territory manager for Iraq) and Paul Bond (former senior sales manager at SBM Offshore). The review shows that SFO errors, which deprived defendants of the right to a fair trial, bolstered the overturned convictions.

OFSI FINES COMPANY FOR SYRIA SANCTIONS BREACHES

In late June, OFSI announced the imposition of a £15,000 penalty on a UK-registered company, for breaching financial sanctions. Tracerco Limited, which provides measuring products and services to the oil and gas industry, was found to have made funds available for a designated person breaching financial sanctions on Syria. Tracerco is a UAE-based subsidiary of UK-registered company Johnson Matthey. Between May 2017-August 2018, they made two payments in the total of £2,956.43 to a sanctioned Syrian airline (designated entity Syrian Arab Airlines) for flights to take an employee home. They booked the flights through a UAE travel agency and then refunded them. They voluntarily disclosed the breach, which led to a 50% monetary penalty reduction, in accordance with OFSI guidance. This follows recent promises by the regulator to tighten up standards for sanctions enforcement. This case is a timely reminder that UK financial sanctions also apply to actions of UK companies operating abroad. All companies with a UK nexus must ensure compliance with sanctions restrictions in place and check that their subsidiaries are also compliant.

THE DEEP DIVE

PROVIDING CERTAINTY AND REBUILDING TRUST SHOULD BE AT THE HEART OF SFO REFORMS

The Unaoil investigation was announced in July 2016, in connection with allegations of bribery, corruption and money laundering by the Ahsani family and other Unaoil employees.

In December 2021, the Court of Appeal decided to quash the conviction of Ziad Akle as a result of the SFO's contact with David Tinsley, a fixer for the Ahsanis, and the failure of the agency to disclose those communications. The Attorney General began a review into the Unaoil investigation, led by Sir David Calvert-Smith. Three out of four convictions in the Unaoil case have now been overturned by the Court of Appeal, Criminal Division.

On 22 July 2022, Sir Calvert-Smith published his findings and it makes for deeply uncomfortable reading for the SFO and its supporters. It will also be sticks of dynamite to be thrown at the SFO's critics and detractors for years to come.

The review highlights serious failings by senior leadership at the SFO, including errors of judgement by the Director, Lisa Osofsky.

Much of the discourse following the Review has been focused on the funding of the SFO and undoubtably, this is a major stumbling block for the agency. However, it is now imperative that the sword of Damocles that permanently hangs over the SFO and its existence is done away with.

It places an inordinate amount of pressure on the agency to “perform”. The SFO should be held to account for its successes and its failures but this incessant focus on whether it should even exist is deeply damaging and a significant distraction for the agency in fulfilling its mandate. It would be virtually unthinkable to countenance a discussion about the DOJ’s FCPA division and whether it should exist. Certainty is needed so that the agency does not continually have to “fight” for its survival or justify its existence. An environment of uncertainty does not aid performance, but rather, creates a pressured environment leading to misjudgements and mistakes.

I know, as a former SFO prosecutor, the weight that is on the shoulders of case teams managing these very complex, vast, and often high-profile cases. The idea of making a big mistake is terrifying and causes one’s blood to run cold as you picture being the person that puts the SFO’s future in jeopardy. That is an unhealthy and unsustainable environment for all concerned. The pressure is immense, and it is important to note that the Review found that “many emails were sent and actions taken at hours late into the night, and that key players were working on the case while on annual leave or, in one case, while unwell.”

Reform the agency, improve its funding, make it accountable - but guarantee its independence and its existence. That is how it can begin to move forward from this difficult moment.

The Review identified the major issues it found that lead to the decision by the Court of Appeal, and categorised them under the following themes:

Casework

- There was a lack of casework quality assurance and record keeping. No one within the agency had a proper and complete understanding of the issues in the multiple-stranded Unaoil investigation.
- The significant one-year gap without a General Counsel in place, as the agency transitioned from one General Counsel to another. This meant that there was a lacuna in quality advice that could have been given to the Director and the case team in relation to Tinsley.
- The priorities and focus of the case team and senior management were at odds. The former was focused on trial readiness, and the latter on repairing the damaged relationship with the DOJ and working up new cases. The DOJ’s relationship with the SFO has had its fair share of ups and down over the years. The extradition of the Ashani family to the U.S. instead of the UK marked a significant low point in the relationship between law enforcement authorities.

Resources

- The case team lacked the capacity and resources needed to manage the demands of the Unaoil case. Some were also working on other cases. This impacted the team’s ability to effectively manage the disclosure process and led to mistakes being made.

Guidance

- There was absence of guidance in the Operational Handbook and other internal policies on how to deal with non-legal representatives. I did not encounter such a situation during my time as an SFO prosecutor, and the possibility of dealing with any party other than legal representatives would have been an alien concept.

Compliance

- Whilst there were a number of policies relevant to the life cycle of a case, the Review found limited compliance with those policies, especially by senior leaders who perceived that they were "above the guidance".

A lack of trust

- The Review found that there was a "culture of distrust" between the case team and senior management based on several factors. These included the dismissal of the Case Controller, and the agency appearing to bow to pressure from the DOJ in relation to the Ahsanis.
- This distrust was further exacerbated by the senior managers dealings with Tinsley, which members of the case team had strong views on. "To be blunt, we thought that anyone with an ounce of investigative nous would have seen right through him."

The Director's endorsement of Tinsley

- It appeared to be the case that Tinsley had been given the "seal of approval" by the Director. This impacted the way in which the case team dealt with Tinsley and hindered their ability to make the right judgement call in respect of their engagement with him. "His relationship with our senior managers…was one of the causes of the pressure and expectation to engage with him and the inability to shut him down."
- Tinsley was not a legal representative of any of the parties being investigated and the case team was of the view that he should not have had any role in the agency's investigation.
- No one in a position of authority within the agency, that was aware of the contact with Tinsley, questioned the interactions with this third party or considered the wider implications of such engagement.

The Review set out 11 recommendations and they have been accepted by the SFO and the Attorney General. Some of the recommendations have already been implemented - including an anonymous reporting tool for staff to raise concerns directly with the Chief Operating Officer.

The ramifications of this Review will lead to a stronger and more resilient agency. The damage that has been done can be repaired over time. It will be important for the SFO to rebuild its reputation, and most importantly, regain the trust of those within the criminal justice process.

TECH SPOTLIGHT

USING FORENSIC IMAGING IN CORPORATE INVESTIGATIONS

What is forensic imaging?

"Digital forensics" is about documenting, identifying, preserving, and analysing digital evidence. Its use in corporate investigations has become more critical with the prevalent use of electronic devices. "Forensic imaging" describes the processes and tools used to copy the contents of an electronic device, such as mobile phones, or internal disk drives of a computer. In some instances, forensic imaging can recover deleted data. This is extremely helpful during an investigation, as digital data is often crucial to the evidence-gathering process.

It is important that the original evidence on a device is preserved and remains unmodified by investigators. "Forensic images" are an exact duplicate of the device and all accessible data stored upon it. They are an essential source of evidence in many investigations, and it is imperative that the images are obtained in a forensically sound manner. This ensures that they can be used in any legal proceedings that may follow. However, not all imaging or backup software can create forensic images and there are many specialised forensic software tools available to create complete and accurate copies.

How is forensic imaging used during an investigation?

Gathering, preserving, and examining all potential evidence is vital. Various sources of evidence can be found in electronic data. Therefore, at the outset of an investigation it is crucial to consider the electronic evidence that may be available, and the ways it can be secured to prevent deletion or modification.

Forensic imaging preserves evidence and enables electronic document review and e-discovery. Where an individual's personal or company-issued electronic device needs to be reviewed during an investigation, it is best practice for the device to be forensically imaged before any interrogation of the device occurs. Digital evidence in particular is easy to transform accidentally. Forensic imaging functions to protect such data during an examination, so that it cannot be inadvertently changed. An investigator should work from the image rather than the device itself. This is useful from a practical perspective - employees will likely require their devices back to continue working.

To index the data, the forensic images can be loaded onto an e-discovery program. Investigators can use key word searches to identify potentially relevant material needed for an investigation. Help can be sourced from an in-house IT team, or an external third-party resource to image the devices and ensure the forensic integrity of the process.

Data privacy issues

The primary objective of forensic imaging is data integrity and there are data privacy issues to consider when forensically imaging devices during corporate investigations. Although it is normal for investigators to need access to private information when examining digital devices, privacy can be threatened whilst such data is handled and processed.

In some organisations, employees may be encouraged or permitted to use personal devices for work, rather than company devices. This could present serious privacy issues for investigators wishing to access these devices during an investigation. Companies should ensure that there is an acceptable use policy applicable to personal devices, including access rights for specified reasons. Otherwise, staff can refuse examination requests which can impede the progress of an investigation.

Does the whole device need to be imaged?

Depending on the imaging method used, it is possible to capture only specific parts of the image. Unlike a full 'physical' image, 'targeted' collection will allow investigators to selectively copy specific information related to the case – such as documents. It can lessen the volume of data collected considerably but there should be clear and documented reasons for proceeding on this basis. The more data that is gathered, the longer it takes to examine, and the more costly the process. It is also possible to narrow material down after full forensic imaging has been conducted. Given the overwhelming growth in corporate data, managing the volume of data collected is a pivotal factor in maintaining costs across the investigation workflow.

*****KEY TAKEAWAYS: Forensic imaging ensures that original digital evidence is preserved and unmodified. The imaging process can assist with recovering deleted data. Watch out for data privacy issues and access rights!*****

THE INVESTIGATORS' MINDSET

USING PERSONAL DEVICES AT WORK: ISSUES AND CONSIDERATIONS

Many organizations have adopted Bring Your Own Device (BYOD) policies to encourage own-device use, due to cost savings and increased flexibility. Some employees may simply prefer their own equipment, for various reasons. However, there are several associated issues to consider when it comes to allowing use of personal devices for work purposes. It is an overlooked, thorny blind spot for many organisations.

Problems around utilising 'own-devices' for work tend to arise in relation to data theft, data leaks, and overall network security. These may expose a company to third-party liability. There is also the risk of unauthorized use of company data for personal purposes.

Another key concern is about accessing personal devices during internal reviews – which includes audits, investigations, and reviews conducted by retained law firms and forensic professionals. Without an acceptable use policy establishing that the same policies applying to organisation-issued devices also apply to personal devices used for work purposes, staff have every right to refuse access. Restricted permission can make investigations very difficult.

BYOD policies should set out what companies expect of employees in various scenarios, and the rights the company has in those circumstances. They can also include the ability to immobilize (and take possession of) personal devices, in the event of a serious breach or suspected criminality.

*****KEY TAKEAWAYS: Do you have an acceptable use policy that covers the use of personal devices? Does your acceptable use policy include accessing personal devices for investigations and reviews? *****

LEGISLATION UPDATES

U.S. ENABLERS ACT PASSES ITS FIRST HURDLE

- In mid-July, the U.S House of Representatives approved the Enablers Act. It is included in the annual national defence bill, the National Defense Authorization Act.
- If passed by the Senate, it will be a step forward in the legislative U.S.' approach to money laundering and will cure a "blind spot" in anti-money laundering laws.
- Scott Greytak, advocacy director at Transparency International U.S., has described the Act as "…the single most important anticorruption measure the United States Congress can adopt right now to prevent corrupt Russian officials and future kleptocrats from hiding and growing their dirty money in the United States."
- The Act targets the presently overlooked professional service providers and industries involved in corruption and money laundering.
- Banks were once the usual go-to for laundering illicit funds, but as AML laws around them strengthened, service providers outside the banking sector (which are less controlled) became the preferred method. Whilst banks must scrutinise clients and wealth sources closely, other U.S. 'financial gatekeepers' have not been required to undertake such due diligence.

If approved, what key changes will the Act bring about?

The Act will ensure that AML procedures are adopted to prevent money-laundering by professional service providers. Professional service providers, including those offering company, trust, financial, or third-party payment, will have to pay more attention to detecting corrupt and criminal funds. Implementing strong AML, KYC, and due diligence procedures will become essential.

Some of the new requirements may include the following:

- Identifying and verifying corporate clients;
- collecting and reporting relevant information;
- establishing internal anti-money laundering programs and due diligence policies, and;
- filing suspicious activity reports to help monitor and track kleptocrats' funds movement.

To support information collection and enforcement, the Act promotes multi-agency coordination and collaboration, deployment of additional resources, and utilisation of technology. Therefore, companies that may be impacted by these reforms should begin to consider their current AML procedures and how they can be strengthened.

SANCTIONS UPDATES

OFSI RED ALERT ON FINANCIAL SANCTIONS EVASION TYPOLOGIES

In July, OFSI (Office of Financial Sanctions Implementation), the NCA (National Crime Agency), the NECC (National Economic Crime Centre), and JMLIT (Joint Money Laundering Intelligence Taskforce), collectively issued a "Red Alert" (the "Alert"). It centres on typologies that may be used to circumvent UK financial sanctions restrictions. It aims to "complement existing knowledge and support on-going improvements to … business processes and procedures". It is designed to promote "awareness" and aid "preventative action".

Key points:

- The Red Alert provides information from law enforcement and the legal and financial services sectors, on common techniques designated persons ("DPs") and associated "enablers" are suspected to use to evade sanctions measures. This includes using "associates" to transfer and sell assets and retain influence via "proxies".
- The Alert lists thirty-four indicators identified through the NCA's casework, open source or risk monitoring by the private sector, that might indicate attempted sanctions evasion. The indicators are classified under three key headings:

1.indicators of frozen asset transfers;
2.indicators of UK enablers; and
3.indicators of suspicious payments.

- Where activity arises involving these indicators, OFSI encourages businesses, particularly in the regulated sector, to report this to the authorities, and seek guidance before proceeding with transactions.
- The Alert also sets out six industry recommendations for spotting financial sanctions evasion, with an emphasis on contacting OFSI for guidance if in doubt. These include:

1. Documenting and not taking transactions at face value.
2. Undertaking appropriate due diligence.
3. Assessing complex corporate structures carefully.
4. Being mindful of complications around aggregation of ownership.
5. Conducting enhanced due diligence and following up with OFSI to confirm appropriate ownership transfer of companies linked to DPs.
6. Carrying out legal assessments to determine transfer of ownership.

What next?

- Businesses should remain vigilant as the risk of evading sanctions is higher than ever. The new strict civil liability test for financial sanctions breaches removes the knowledge/reasonable suspicion requirement, making it harder to escape liability.
- It is crucial to understand the indicators, undertake sufficient due diligence, and remain alert to the risk of sanctions evasion.
- A proactive approach is vital since the risk of breach and therefore enforcement action is now much greater. Sanctions compliance processes and procedures should be reviewed, to ensure that approaches to assessing higher-risk transactions and counterparties reflect the warnings and due diligence recommendations.
- The indicators, which are potential red flags of sanctions breaches, place responsibility on businesses to demonstrate that they took them into account when assessing customer or transaction risk.
- Those in regulated sectors, such as financial services, should be especially mindful of the indicators when conducting sanctions risk assessments.
- The Alert meets the demand for further compliance guidance after the increase in sanctions. It is a step forward in much-needed collaboration between government bodies and the private sector.

*****KEY TAKEAWAYS: OFSI provides clarity on indicators of sanctions evasion. Review your sanctions compliance processes and ensure alignment with the indicators and recommendations.*****

DATES FOR YOUR DIARY

DETECTING MISREPRESENTATION AND FRAUD DURING M&A DUE DILIGENCE

ACFE | 02-08-22-04-08-22 | Register

Time constraints and the pressure to get deals completed in M&A can lead to failures to identify false information, misrepresentation, and fraud in the due diligence process. This course will prepare participants to incorporate specific approaches to detecting misinformation and fraud during M&A due diligence.

INVESTIGATING CONFLICTS OF INTEREST

ACFE | 18-08-22 | Register

Conflicts of interest can present fraud risks for corporations, government agencies, fiduciaries, customers and suppliers. It is one of the most difficult areas of fraud to investigate and obtain appropriate evidence for. Improper investigations can create counterclaims and civil actions against organizations and fraud examiners. This seminar will explore both how and why conflicts of interest arise, and how to spot warning signs. It aims to help attendees gain a better understanding of issues specific to such engagements and teach ways to protect an organization from conflicts of interest.

BENCHMARKING INTERNAL INVESTIGATIONS

Today's General Counsel | 11-08-22 | Register

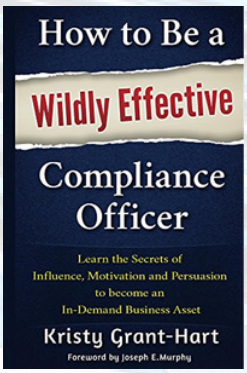
With increasing compliance requirements and growing liability concerns, organizations must be able to conduct internal investigations thoroughly and swiftly. To achieve this, legal teams need to understand best practices and benchmark their processes against their peers. In this webcast, experts will speak on recent survey results benchmarking internal investigation processes and how to use these findings to manage internal investigations more effectively. Attend to learn about how 70 legal departments are conducting internal investigations, best practices from experts on streamlining your process, and the role technology must play to automate the process.

USEFUL RESOURCES

BOOK: HOW TO BE A WILDLY EFFECTIVE COMPLIANCE OFFICER

Access: website

By: Kristy Grant-Hart (Author), Joseph E. Murphy (Foreword)



This book teaches compliance professionals the secrets of influence, persuasion and motivation so they can become in-demand business assets. It is a powerful guide to help practitioners move from the “check-the-box” mentality of a paper program to become dynamic business leaders. This book is recommended for those who want to be successful compliance professionals and is said to describe the “missing link” in the compliance profession – interpersonal skills, and influence.