PARAMETRIC INSIGHTS

ECONOMIC CRIME UPDATES

HELLO!

Welcome to the **sixth** 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!

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

PARAMETRICGLOBAL.CO.UK/

CONNECT

CASE UPDATES

DEUTSCHE BANK BREAKS RULES TO ENABLE TAX FRAUD

An internal investigation found that Deutsche Bank broke its own policies and 'legal or regulatory' rules to facilitate clients to siphon off government revenues amounting to millions of euros. More than 70 current and former employees of the bank are under investigation by German prosecutors. It is connected to the extensive law enforcement inquiry into a multibillion-euro, long-running tax fraud scheme involving leading banks; the ongoing criminal investigation stepped up recently due to a senior banker's arrest by Frankfurt prosecutors.

Deutsche Bank's internal investigation (dating back to 2015) revealed connections to the 'cum-ex' scandal involving banks across Europe. Deutsche generated millions of euros in fees by intentionally delivering investment banking services to clients who specialised in cum-ex trading. The bank also engaged in derivatives trading that exploited illegal loopholes. The internal investigation report includes damning details, such as an indication of lack of controls to ensure bankers would abide by the bank's internal policies. Further, business managers concluded that the risks around providing leverage to potential cum-ex purchasers, were acceptable.

BANK OF AMERICA IN SETTLEMENT TALKS OVER UNAPPROVED DEVICE USAGE

The SEC are looking into whether Wall Street banks have satisfactorily recorded work-related communications during the period of the pandemic when work-from-home was widespread. They began investigating record-keeping practices regarding personal devices in 2021 as part of a broad inquiry into how Wall Street banks track employees' digital communications, and the CFTC also began examining the issue. In late July, the Bank of America said that it was involved in settlement talks with the SEC and CFTC over staff communications on unapproved devices. The banking giant has set aside around $200 million for expected fines from the probe into unauthorised use of personal phones by bank staff.

BARCLAYS INCLUDED IN U.S MESSAGING PROBES

Barclays recently joined other European banks impacted by a U.S. global investigation into breaches linked to use of unapproved electronic messaging channels for business communications. The issue has gained traction since the pandemic led to more bankers working from home. So far, various banks and Wall Street giants have set aside cash to cover expected fines. Barclays reported that they reached an agreement with the SEC and CFTC late in July, with the penalties expected to be $200 million in total.

PWC FINED OVER FRAUD AUDIT FAILURES

UK's accounting regulator FRC has fined PwC almost £1.8m for failing to properly inspect BT's accounts after a £500m accounting fraud was uncovered at the company's Italian operation. PwC failed to act with the "requisite professional scepticism" and did not obtain "sufficient appropriate audit evidence" in its work on the financial statements. FRC rebuked both PwC and Richard Hughes, the firm's audit engagement partner. Their audit documentation was said to have been difficult for even an "experienced auditor, having no previous connection with the audit", to understand. However, the breaches were deemed not to have been "intentional, dishonest or reckless", and early admissions resulted in a 30% discount to financial penalty.

THE DEEP DIVE

THE ART OF COOPERATION WITH GOVERNMENT INVESTIGATIONS

There has been a steady trickle of corporate resolutions in the U.K. and the U.S. following corporate misconduct.

The fortunes of an organisation can be severely dented by protracted and costly investigations by law enforcement and regulatory authorities. Strategic and effective cooperation can truncate the length of an investigation and focus the attention of all parties on a suitable resolution.

Cooperation that comes too late and lacks depth may deprive the organisation of some of the cooperation credit due. It may also mean that the organisation loses the opportunity to avoid a criminal conviction, thereby tarnishing its reputation and possibly impacting its ability to do business in some jurisdictions.

The decision to cooperate with law enforcement or regulatory investigations isn't one that can be made by external advisors to an organisation. It is the job of those advisors to present the available options and set out the consequences of each path, but ultimately the decision is for the most senior within the organisation to make.

To genuinely and effectively cooperate, the leaders of an organisation must be persuaded that it is in the best interests of the company to do so. They must also grapple with the fact that the investigation is now out of the organisation's control. It does not get to dictate the pace, scope, or remit of that investigation. Its role is now primarily reactive, but the one area in which it can play a proactive role is in relation to the cooperation that it provides to the investigating authority.

It may not always be in the organisation's best interests to cooperate (for a variety of reasons), but care must be taken to fully acknowledge the consequences of that strategy.

The organisation may genuinely believe that it is the victim of political machinations, or its leaders be fully persuaded as to the relative innocence of their organisation in respect of the alleged criminality. However, the organisation must grasp the reality of what it means to set itself on a collision course with the investigating authority and consider that even if it wins, will it really win? It must determine what the variations of success may look like, and chart a course in that direction if it chooses not to cooperate.

Law enforcement and/or regulatory investigations are a serious distraction, diverting attention from the key priorities of the organisation. They are a drain on the organisation's human and financial resources. They are hard work!

Non-cooperation is not for the faint hearted. However, there is also a high bar for the extent of cooperation that is expected by the law enforcement and regulatory authorities.

Early engagement with the investigating authorities to establish what they require from the organisation is crucial. Organisations are expected to be proactive and genuine in their approach to cooperation. There is no time to waste. This should be followed by consistent engagement as the investigation progresses.

There should be a clear and coherent strategy for the desired resolution which is endorsed and supported by the senior leaders in the organisation.

The organisation should establish its position on issues such the disclosure of material that is properly subject to legal professional privilege and ensure that this position aligns with its strategy for a resolution.

There are best practice expectations of what cooperation should look like. However, it isn't prescriptive and will ultimately depend on the nature of the investigation and the investigating authority.

Organisations should be alert to the fact that what may have been a sufficient level of cooperation in one matter, whilst providing some steer, may not be enough in respect of the investigation into their affairs. There is often an uncertain and arduous path to navigate in cooperating with a government investigation. A clear strategy for cooperation is vital as it may be the path that bears most fruit, enabling the organisation to move forward and past its misdemeanours.

****** KEY TAKEAWAYS: Have a clear strategy for cooperation. Ensure that senior leaders are aligned on the desired but realistic resolution. Proactive and genuine cooperation is an expectation. ******

TECH SPOTLIGHT

'TRUST TECHNOLOGY' & WHISTLEBLOWING

Whistleblowing can help tackle corruption, protect a business' reputation, and encourage good ethical practice. It is important that organisations protect those raising concerns and make whistleblowing as easy as possible.

Trust technology - "Trust Tech" - refers to technology that improves and spreads trust throughout different settings. It can manifest in the form of internal reporting platforms, which play an important role in facilitating whistleblowing. There are growing options available that make whistleblowing easier, protect anonymity more securely, help firms handle misconduct reports internally, and convert complaints into data that enables harmful pattern detection. Furthermore, Trust Tech provides a variety of ways in which reports can be made, which is reflective of our times. The FCA's "Whistleblowing quarterly data 2022 Q1" demonstrates that they received most whistleblowing reports between January and March 2022, via the online reporting form.

How can Trust Tech make it easier for people to speak up?

- It can significantly increase the number of reports being made and reduce resolution time.
- Workplace trust and confidence are key to organisational success, yet many potential whistle-blowers fear retaliation, insecure reporting channels, and dismissal of concerns. Trust Tech can help to alleviate concerns about confidentiality and the processing of reports made.
- Without belief in confidential systems and appropriate case processing, necessary information may be withheld.
- Whistleblowing platforms can limit traceability of reporters, as many are embedded with strict data security and privacy measures. They can ensure that integrity of reported information and identities are protected. They can also provide more accessible ways to communicate with whistle-blowers.
- Organisational culture and values are increasingly important to employees. Investing in whistleblowing technology can help organisations to develop more ethical and sustainable cultures and business practices. It promotes a good corporate culture where people can see that complaints are heard and acted upon, and ethics and transparency are taken seriously.
- Whistleblowing platforms can enhance quality and expediency of reports received, better structure the complaints process, provide support and resilience by protecting channels, and provide insights into trends. They can offer various features - such as report management protocols to ensure anonymity, coordination of information on centralised platforms between teams investigating reports, and real-time tracking of investigation status.

- Delays between incident occurrence and reporting impact an organisation's ability to deal with/prevent misconduct from occurring. Enhancing data visibility during the whistleblowing process is therefore vital. Whistleblowing technology can increase data accessibility for analysis and trend-watching. The data from such platforms can limit litigation costs, minimise reputational damage and provide actionable insights.
- With hybrid and remote working reducing on-site visibility, online reporting platforms have become even more essential.

Considerations:

- Confidence in reporting systems is often wrecked when whistle-blowers become targets after system failures. It is important to prioritise platform security.
- Reporting platforms cannot solely solve issues around how complainants are treated. Technology and organisational culture must work together for maximum impact. The systems will be ineffective otherwise.
- Training is crucial. Staff should be trained on using the systems and made aware of whistleblowing security and protections available. There should be adequate guidance made widely accessible across the organisation. It is particularly vital that those responsible for triaging concerns are fully trained, and able to maximise the use of the technology.

Check out next month's issue for further developments in this space, and a quick guide to whistleblowing platforms for your organisation to consider!

****** KEY TAKEAWAYS: Consider whether the whistleblowing platform that you use facilitates ease of access for those who may wish to use it. If you are a large organisation, does your platform allow external parties to report concerns? Is your triage process robust, and are those responsible for managing the process adequately trained? ******

THE INVESTIGATORS' MINDSET

THE TRIAGE PROCESS: STEP ONE – REACT!

Having a triage process as part of your investigation methodology is extremely helpful when assessing how issues will be handled, especially in the context of complaints and reports. It is all about having a stable system in place.

Working out *what* triage system to use is an important consideration. Although it is different for every organisation, at Parametric Global Consulting, we recommend our 'three Rs': the "React; Respond; Remediate" triage system.

Over the next few issues, we will focus on the three Rs, and what organisations should do at each step.

1 - React:

An organisation's reaction to concerns is all-important. It sets the tone for how adequately a report will be handled and can make or break trust in an organisation's culture and approach to handling misconduct.

The organisation should be swift but considered in acknowledging the complaint, as failure to do so may mean employees are forced to escalate their concerns outside the organization. The chances of external reporting are increased if the complainants are of the view that business leaders will not even acknowledge the existence of their concerns, regardless of validity. In addition to damaging workplace trust and confidence, this can lead to huge reputational risks and external scrutiny.

Reacting does not always mean starting a full investigation; it will depend on the severity of the report. Nevertheless, it means always providing reassurance to those who speak up, to ensure they feel heard. This will encourage employees to come forward boldly, reduce fear of retaliation, enhance business integrity, and avoid long-term concealment of issues.

****** KEY TAKEAWAYS: Do you have a clear framework for your investigation process? The initial reaction to a complaint or allegation can either instil confidence or dismantle trust in the process. The failure to react in a considered and timely way can quickly escalate the situation. ******

POLICY UPDATES

DOJ CERTIFICATION REGIME FOR CHIEF COMPLIANCE OFFICERS

The U.S. Department of Justice (DOJ) has introduced compliance officer certifications in corporate enforcement actions. Chief Compliance Officers (CCO) will have to certify representations about their companies' compliance programs in corporate resolutions and settlement agreements with the DOJ. CEO certifications have been part of the DOJ's previous practice, but what does this new process mean for CCOs, and what potential liability may be attached to such a certification?

Background

- In March 2022, Assistant Attorney General of the DOJ's Criminal Division, Kenneth Polite, announced that for corporate resolutions going forward, prosecutors should consider requiring CCOs to certify that the company's compliance programs are 'reasonably designed and implemented to detect and prevent violations of the law' and are 'functioning effectively'.
- Since then, this requirement has been reiterated by other DOJ officials. It was also confirmed in June by the Assistant Chief of the DOJ's Fraud Section, Lauren Kootman, who said that companies can expect the requirement to be included in corporate resolutions going forward.
- The CCO certification process was put into practice in May 2022, in the DOJ's resolution of FCPA violations by Glencore. The mining firm agreed that its CCO would execute the relevant certifications at the end of the resolution's term.

Expectations

- At the end of resolutions, CCOs of companies should expect to certify that the compliance program is 'reasonably designed' to detect and stop relevant criminal violations.
- The CCO becomes responsible for making certifications regarding resolution elements - such as reporting requirements - on the company's behalf.
- CCOs must individually confirm the effectiveness of the company's compliance program as part of DOJ resolutions, and personally approve the company's remediation efforts.
- In some resolutions, monitors may not be imposed, and companies will have to provide the annual self-reports on their compliance programs. In such cases, the DOJ will consider requiring certification that all compliance reports submitted during the resolution's term are true, accurate, and complete.
- CCOs expose themselves to the risk of prosecution and will have to certify under penalty of perjury.

Purpose

- This additional certification is not intended to be punitive.
- It is designed to 'empower' CCOs and boost their voice, independence, and 'authority and stature', ensure their involvement in corporate decision-making, enhance their access to relevant compliance-related information, and help them effectively share concerns with the DOJ before certification.
- The DOJ envisions that certification will help ensure that CCOs are reporting directly to the Board about what has or has not happened while fulfilling the company's obligations.
- The requirement incentivises CCOs to ensure their compliance programs are up to the required standard before signing the certification.

Criticisms

- The new certifications ought to empower CCOs to be involved in critical compliance-related decision-making. Nevertheless, there may be consequences counterproductive to the stated purpose.
- CCOs will personally bear their company's responsibilities to remediate compliance deficiencies and communicate honestly with the DOJ.

- There is no guidance to help determine when a compliance program is 'reasonably designed'. This standard could have different interpretations. The language is very subjective.
- For multinational companies, certifications based on personal knowledge will be problematic as CCOs must rely on representations of company employees in key positions.
- There is risk of individual criminal liability for the CCO; however, there is little certainty around the circumstances in which such liability may be triggered.
- There are concerns about the certifications potentially being used to ensnare CCOs with criminal liability for corporate failings. They may even become the scapegoat if a dispute arises between the DOJ and the company over the adequacy of its compliance programme.

What next?

- The new requirement raises the stakes for CCOs, and will have a significant impact on their oversight responsibilities in relation to corporate resolutions.
- The certifications should be expected in future DOJ resolutions. Companies should ensure their Chief Compliance Officers have the power to make them.
- The certifications should be carefully considered, and steps taken to ensure accuracy and clarity when attesting to the 'reasonably designed' standard.
- CCOs will be personally exposed to the risk of prosecution for false representations.
- CCOs should carefully document their company's efforts to introduce well-designed compliance measures to reduce likelihood of violations.

****** KEY TAKEAWAYS: Does the CCO have the authority, stature and independence within the company? Does the CCO have access to all the relevant data and information relevant to the compliance program? CCOs should ensure that there is a clear paper trail in place and that they are empowered to make the relevant certifications. ******

DATES FOR YOUR DIARY

THE ESSENTIALS OF REMOTE INTERVIEWING SKILLS

ACFE | 20-09-22 | Register

Conducting interviews remotely is here to stay, even post-pandemic, and it is vital that investigators develop the necessary skills to conduct these types of interviews effectively and successfully. This session, delivered by Lloydette Bai-Marrow, will focus on techniques and strategies for maximizing the outcomes of remote interviews, and how to help the investigation progress.

INVESTIGATING CORRUPTION: DIFFERENT JURISDICTIONS – DIFFERENT WAYS

ACi | 13-09-22 | Register

This webinar will examine the legal areas that need consideration during a corporate investigation into allegations of corruption: The alleged provision of undue benefits to foreign public officials.

ECONOMIC CRIME PREVENTION & COMPLIANCE: LONDON 2022

ACi | 28-09-22 - 29-09-22 | Register

Money laundering, sanctions, cyber, ransomware, and bribery are developing in ways and forms that have not previously been imagined. The Economic Crime Prevention & Compliance in London will help attendees learn how to design and implement actionable “catch-all” compliance programs, manage government and internal investigations, and stay ahead of enforcement.

HUMAN RIGHTS IN SUPPLY CHAINS – ADAPTING TO NEW ENFORCEMENT RISKS AND CONDUCTING EFFECTIVE DUE DILIGENCE

Covington & Burling LLP | 21-09-22 | Register

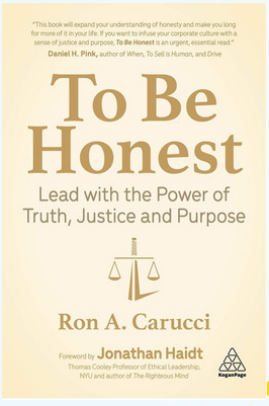
Companies are facing a host of new and fast-evolving enforcement risks related to forced labour and other human rights issues in supply chains. This webinar will give an overview of key trends and developments in the United States and Europe, and provide practical advice on steps companies can take to conduct due diligence that is effective in practice and consistent with the expectations of regulators.

USEFUL RESOURCES

BOOK: TO BE HONEST: LEAD WITH THE POWER OF TRUTH, JUSTICE AND PURPOSE

Access: Amazon

By: Ron A. Carruci (Author), Jonathan Haidt (Foreword)



Based on 15 years of research, To Be Honest explains how four factors affect honesty, justice and purpose within a company. It shares stories of leaders who have acted with purpose, honesty and justice, even when difficult. In-depth interviews with CEOs and senior executives from exemplar companies reveal what it takes to build purpose-driven companies of honesty and justice, and interviews with thought leaders offer rich insights on how leaders can become more honest and purposeful. Filled with real-life examples, the book offers actionable steps, practical tools and approaches that any leader or manager can use to create a culture of purpose, honesty and justice.