Serious Fraud Office – Written evidence (FRS0029)

BACKGROUND

1. The Serious Fraud Office (SFO) is a small independent non-ministerial Government department under the superintendence of the Attorney General. The SFO’s purpose is to investigate and, where appropriate, prosecute cases of serious or complex fraud, bribery and corruption. In addition, the SFO recovers the proceeds of those crimes it investigates and assists overseas jurisdictions in their investigations into serious or complex fraud, bribery and corruption.

2. The SFO will investigate those cases which call for the legal powers and multi-disciplinary approach available to the SFO. In considering whether to take on an investigation, the Director applies a Statement of Principle, which includes consideration of:
   - whether the apparent criminality undermines UK PLC’s commercial or financial interests in general and the City of London in particular;
   - whether the actual or potential financial loss involved is high;
   - whether actual or potential economic harm is significant;
   - whether there is a significant public interest element, and;
   - whether there is a new type of fraud.

3. The SFO has multi-disciplinary case teams of lawyers, investigators, forensic accountants, external counsel and other experts, such as digital forensic investigators, working together throughout the life of a case, led by a case controller, in order to address the particular demands and challenges of serious and complex economic crime. This joint investigatory prosecutorial case-team structure is known as the ‘Roskill’ model. Crucially, it is more than just joint working – it involves professionals embedded and co-located together, each contributing to progressing investigations at pace and, where appropriate, building robust prosecutions.

DIGITAL FORENSICS

4. Whilst the SFO does not rely on traditional forensics such as DNA, Fingerprints etc. it has a dedicated Digital Forensic Unit (DFU) who are responsible for processing the majority of the digital material acquired during the course of investigations. Where data is supplied that does not require forensic processing the SFO has additional processes it can adopt. This has been developed in response to the huge increase in data and material being supplied electronically.

5. To ensure the integrity of digital material acquired during the course of investigations the DFU adhere to the Association of Police Officers (ACPO) (now National Police Chiefs’ Council (NPCC) guidelines on handling digital evidence and the Forensic Science Regulator’s (FSR) codes of conduct.

6. The DFU consists of examiners from a range of technical backgrounds which reflects the huge variety of systems and media the unit encounters. We

---

1 If there was a need to undertake forensics of this manner the SFO would work with partner law enforcement agencies to identify solutions.
currently employ 12 staff in the team but are running a number of recruitment campaigns to bolster this complement. The team is responsible for the handling and processing of digital material obtained during the course of SFO investigations, which includes a wide range of devices including CDs, USBs, hard drives, desktops, Laptops, mobile devices and Servers.

**CHALLENGES**

7. The biggest challenges we currently face are the volume of data and encryption, it is not uncommon for devices to now have the capacity to store gigabytes and terabytes of data which can take time to process. We have a duty to ensure as much data is retrieved as possible in order that the investigation teams can meet their obligations under the Criminal Procedure and Investigations Act. Once obtained this material must be reviewed. Due to the nature of the cases the SFO takes on we often obtain large amounts of data from individuals and companies which may be relevant to an ongoing investigation, it is imperative that we ensure that we have taken appropriate steps to access and review any data held to avoid criticism or challenge.

8. In addition the advancements and availability of different methods of encryption can hinder the acquisition of data. Whilst the SFO will consider all of its available powers to obtain passwords and encryption codes there still can be delays in accessing and acquiring data which impacts on effective investigations. The issues law enforcement agencies face with encrypted devices are well documented, along with the efforts of agencies to engage the Companies responsible for the software to assist in accessing encrypted devices.

**STANDARDS AND REGULATION**

9. There are a number of tools available that can ensure the integrity of digital evidence. These are used across the industry and accepted as the FSR codes of Conduct and introduction of ISO17025 accreditation will ensure consistency across organisations deploying these methods and tools. The validation and quality control of digital forensic processes is key to this as each organisation must review, test and verify both equipment and staff competence. **SFO would support the FSR being given statutory powers to bolster the Codes and accreditation process.**

10. The increased investment into forensic services from a wide range of vendors has had both a positive and negative impact. The digital forensics market is saturated with a number of companies competing for digital forensic work and staff. But this also means there is a great deal of competition for trained and experienced staff and this has had a negative impact on the SFO in respect of recruitment and retention of staff.

11. The SFO trains their examiners to a high standard to ensure it provides adequate support to the investigation and prosecution of complex fraud and bribery cases. They deal with a multitude of devices and provide training that may not be offered elsewhere, making our digital forensic investigators a sought after commodity. The SFO is constantly running recruitment campaigns to attract new and experienced examiners, however the salary gap between the Civil Service and private sector makes a once attractive
career less appealing and we have had difficulty in attracting individuals with the right skills and knowledge.

12. The introduction of expert evidence is likely to increase as evidence is challenged in more detail, therefore the provenance and integrity of material obtained from digital devices is a key area. Ensuring that standards are set and maintained in line with technology is important to retain a level playing field. Expert evidence should therefore have some form of regulation or a mechanism by which agreed criteria or standards are adhered to.

13. SFO staff are not treated as expert witnesses, they will be witnesses of fact providing evidence of what actions they took and the product of that work. The SFO considers the Court is best placed to determine whether a witness can be considered an expert.

RESPONDING TO THE CHALLENGES

14. The SFO has taken significant steps to increase the capacity of the DFU in response to the increasing workload caused by the continuing, exponential growth in the volume of data associated with our investigations. This is a key strategic area for the business and we have taken steps to increase our efficiency by reviewing our processes and systems, expanding the physical size of the lab and increasing the size of the team to meet these additional demands.

15. To give a sense of the scale of the increase, in the first quarter of the 2017/2018 financial year, the DFU released 2.5 million documents per month on average. By the second quarter that had doubled to 5 million per month, and by the third quarter it had doubled again to 10 million per month. The average remained around 10 million per month for the final quarter, and the highest single month was January 2018 where we released more than 15 million documents to our case teams. Since then we have been averaging around 7.5 million per month and expect to maintain or increase this average as the year progresses.

16. These documents are then provided to Case teams for review on an eDiscovery platform. Depending on the number and type of documents this can be achieved using key words and search terms, however search terms can be a blunt tool and change depending on the direction of the investigation.

17. The investigation teams are not only focussed on identifying potential evidence of offences and pursuing all reasonable lines of enquiry, they also must take into account their disclosure obligations and consider what may undermine their case and any additional issues such as material which is covered by Legal Professional Privilege.

18. Taking these considerations into account the review phase can take many months depending on the volume of material and available resources. The management of these reviews is crucial and investigators must have the technical knowledge and skill to use the review platform to maximise efficiency. The traditional knowledge and methods remain at the core of any investigation. However, the abundance of digital material and increased use
of technology to commit crime means that investigators must regularly update their skillset and adapt to the material they obtain.

19. To assist with the review of documents that may be the subject of Legal Professional Privilege (LPP) the SFO has worked with an external company to develop an artificial intelligence tool to assist human reviewers in making determinations of LPP. This was recently deployed on a high profile SFO case which has in excess of 30 million documents subject to claims of LPP. The artificial intelligence tool was able to review documents at speeds up to 2,000 times faster than human reviewers and represented a saving of 80% over using independent counsel only to complete the review.

20. In addition, the SFO has made a significant investment in a new EDIScovery platform which was launched in March 2018 with a number of new analytical tools to enable data in large cases to be interrogated more efficiently. The platform also has the predictive coding capabilities which, although common in the civil investigation and prosecution field, are as yet untested in the criminal sphere.

21. There are a number of ways in which predictive coding could be used in criminal investigations and prosecutions but some of the potential uses would appear to be:
   • To prioritise a review by identifying documents most likely to be of interest or relevant to a particular area of the investigation; or
   • To assist with the identification of specific or highly relevant documents for review or use at early in an investigation; or
   • To assist investigators to make determinations of relevance for the purposes of the CPIA disclosure regime; or
   • To assist in the making of determinations as to which documents satisfy the disclosure test and fall to be disclosed, as set out in the CPIA disclosure regime.

22. The resulting evidence is then produced in evidence alongside any material required for disclosure. This itself can run into gigabytes and in large cases terabytes of information all of which needs to be supplied, hosted and reviewed by all parties within the case.

23. The use of technology has also spread to the presentation of evidence during trials, previously this was limited to producing images on screen for the Court to view, however we are now able to animate, highlight and compare evidence as it is presented. The SFO has recently trialled the use of tablets to assist the Court in dealing with large volumes of material in a more effective manner, in cases where there is a large amount of data: key documents are presented alongside graphics which interact with the documents providing a narrative that is accessible to all parties.

24. It can no longer be suitable or cost effective to generate multiple sets of hard copy documentation when it can be provided on a USB or mobile device. The SFO commonly provides data to third parties in this manner, in fact it is now almost expected as many firms have access to similar document review systems. We are constantly reviewing our processes and policies to continue to deliver value for money and ensure the investigation and prosecution of complex fraud and bribery is managed effectively.
Is enough being done to prepare for the increasing role that digital forensics will have in the future? Does the Criminal Justice System (CJS) have the capacity to deal with the increased evidence load that digital forensics generates?

25. The core methods and principles of investigation still apply but investigators are continuously having to adapt to the crimes being committed via the use of technology. In the case of investment frauds, documentation can be sent to thousands of individuals by the touch of a button. Bribery and corruption can be orchestrated using mobile devices and encrypted communications methods which can be difficult to trace, locate and obtain.

26. The CJS must consider whether it is ready not only for the increased volumes of data available electronically but also whether the current legislation and powers available adequately cover the acquisition of digital material. This includes the availability of appropriate IT systems to receive, store, interrogate and present data but also the increased knowledge and awareness of digital forensics so key points can be presented in a fair and balanced manner.

13 September 2018