ONBORD – Written evidence (FDF0013)

Paragraph numbers refer to the question numbers in the Call for Evidence

1. Digitalisation has allowed for industrialised fraud attempts as well as new avenues for fraud. While affording many business advantages, digitalisation has also meant that traditional sniff tests (through meeting and conversing with people) have disappeared. For want of a better phrase, technology has democratised fraud. This relates not just to external attacks but internal ones too. The ability to conduct internal fraud (or be a party to it) has increased at businesses. Whereas, in the past, most fraudsters had to face their mark, now fraud can easily be perpetrated remotely (even from a different jurisdiction) and perpetrators may perceive it as quasi-victimless, if a bank or insurance company is covering the losses.

   Digital fraud has manifested itself and is likely to continue to manifest in the following ways:

   a) (individuals) phishing (for financial details), fraudulent investment schemes and push payment fraud

   b) (government) procurement and false claim fraud

   c) push payment, internal fraud, identity theft of business or individual, delivery to a fake client, accounting fraud

2. Digital fraud is where intelligent criminals should be allocating their resources, as it can be executed remotely and anonymously. Additionally, it may not be reported and, even if it is reported, it may not be prosecuted. It can be hard to trace and harder to prosecute. The victim may feel shame and there may be an initial bias to believing that they were partly to blame. How things will evolve in the future cannot be accurately predicted, however, we can say with certainty that fraudsters will evolve and try to profit from technological change. Philosophically, we should assume that:

   - the number of fraudsters will increase,
   - their behaviour will evolve,
   - they will leverage technology,
   - and seek out the weakest links.

   Technology developments including Web3 and Crypto are going to create more opportunities for fraud just as dating apps, market places and social media have. Tech is both the biggest threat and the best solution. In order, to reduce the impact of fraudsters, it is essential that scams are reported and acted upon quickly.

3. Currently, there is no meaningful cooperation between different parts of the ecosystem. Cifas is the best resource but membership is expensive and only available to larger financial institutions. There is anecdotal evidence that fraud crimes on businesses under £50k to £100k will not be investigated by the police. Even with more sophisticated scams involving larger sums, it often appears in the media that the UK is not aggressive at prosecuting white-collar crime (whether it be accounting fraud on AIM or

misrepresentation within the financial markets). It is important for a myriad of reasons that, in relation to fraud, justice is not only done but that justice is seen to be done.

4. The SFO has given evidence that it lacks extra-territorial powers. Britain can't solve international fraud schemes on its own. It requires international cooperation. One potential solution would be to leverage the work of FATF in countering laundering and terrorism financing. The UK could take the lead in lobbying to get FATF to have a dedicated fraud arm. There is little point in creating a new international organisation as the cooperation protocols are in place and there is some overlap with both the protections needed and the actors involved in laundering and terrorist activity.
5. It has to be recognised that it is a very tough task to keep up with fraud advances. All agencies are playing catch-up and the crime scene is constantly evolving. Lessons from the tech field should be employed to combat digital fraud:
    - Stay as agile as possible
    - Learn quickly
    - Iterate

    The City of London Police were the obvious lead on this and they should be given the resources to execute on their mandate. The overall structure is likely not the issue. Hiring more talent from the Infosec space would likely benefit law enforcement. Rather than thinking about changing the high-level structure, it is likely that the major weaknesses lie in a lack of clear reporting and escalation protocols and the resourcing required to investigate and prosecute. One idea to benchmark performance could be an annual fraud census (say choose 10k businesses and 100k individuals) to make the assessment more scientific and informed by real world events.
6. The SFO has not secured the convictions it believes it should have. It is best placed to explain why. From the outside, it is unclear why that it is and it may be purely down to a lack of talent, budget and resources. While victim support is useful, prevention and prosecution should be prioritised. Victim support doesn't deal with causes or reduce economic effects and most victims would take solace from knowing the culprit was caught and appropriately punished. Indeed, a focus on victim support could end up acting as a distraction from other failures.
7. There isn't really a method in place for the private sector organisations to warn each other about fraud (away from perhaps large financial institutions and even there it is not that effective). Silos (even within a particular business) can allow fraud to go undetected that joined-up thinking would catch quickly. Currently, fraud is likely only shared when it is proven and not suspected. One solution could be a suspicious activity reporting protocol like for laundering to a regulated entity, passing: name, IP address, phone number and email address of suspicions of fraud.
8. GDPR issues can be dealt with by reporting suspicions to a regulator with limits to the scope. This would create a database that could be searched

for a match but couldn't be downloaded. Particularly, if it is made a legal requirement to report suspicions of fraud at regulated entities.

9. It is difficult to educate the public when fraud is constantly evolving but fraud should be more publicised. Using technical jargon is also unhelpful. Scams need to be explained simply and clearly. Individuals need to take personal responsibility for protecting themselves. It cannot be that banks unilaterally underwrite any losses in a bank account when they had nothing to do with the fraud either through negligence or even enabling it. A code of conduct which says any business will make best endeavours to ensure their systems are not used to enable fraud would be a good thing but we would favour that this should be a voluntary code of conduct rather than legislation at this point.
10. The Fraud Act 2006 defines fraud very broadly in Common Law so this is not the issue - it covers everything needed. The only obvious issues are the corporate controlling mind and extra territoriality. In fact, attempting to create specific crimes for emerging subtypes of digital fraud would be a mistake, as getting off on technicalities would likely increase.
11. This is a problem of detection, prevention and enforcement; not of legislation.
12. The system is not working in terms of the amount of convictions versus the likely amount of fraud activity in the economy (which is most definitely under reported).
13. The incentive to commit fraud needs to be understood as a probability calculation for potential fraudsters:

    Gain x Probability of success > Loss x Probability of successful prosecution

    The focus should be on the probabilities versus increasing the potential loss as this will have a greater impact on deterring fraudsters.
14. The US is the world leader in enforcement - their strategies should be adopted - better whistle blower rewards, more aggressive investigative work and more deals to get criminals to testify against each other.
15. Fix the controlling mind issue when prosecuting organisations. The CEO should be the assumed controlling mind and should be personally guilty of any corporate crime unless the CEO can prove otherwise and place the control elsewhere.

    A register of suspected fraudsters could be an idea (operating at a lower standard than a formal prosecution). This would not be a statement that you are definitely a criminal but rather that a competent regulator with no ulterior motive suspected you might be. No doubt there would be legal pushback on this but it should be possible with the right legislation.

19 April 2022