



Report on Wilton Park Conference 917

IMPROVING INTERNATIONAL EFFORTS TO COMBAT FRAUD

Monday 9 – Wednesday 11 June 2008

1. Fraud, in all its manifestations, poses a threat to individuals, financial institutions and other businesses and markets. Serious international fraud can affect the reputation of countries and have a detrimental impact on the health and well-being of consumers. International acknowledgment of fraud has lagged behind measures taken to deal with drugs trafficking and other transnational organised crime. There are few accepted standards and definitions and levels of resources devoted to the problem are often low. There can be disagreement between public and private sector institutions on the best way to tackle fraud and roles and responsibilities are unclear. Political will may be lacking in all countries, including developed ones, and in some cases the political elite may be involved in fraudulent activity themselves. It is important to consider what can be done nationally and internationally to address these problems and the threat that fraud poses to society.

2. In discussions on fraud, there are often difficulties with terminology and definition. For example, there are few international standards relating to the general definition of fraud, other than bribery and corruption. This can hamper co-operation and understanding of the problem on the global scale. Fraud, although recognisable when encountered, is not the same to all people. However, common definitions are vital to ensure a better understanding of both the scale of the problem and how to deal with it. In addition, sensible measures of fraud are impossible in the absence of precise terminology. Legal definitions of fraud have often failed to keep pace with developments, particularly in technology, with the increased use of the internet. Reality often outruns legal constructs based around previous activities. A modern trend is to move to offender-focused legislation, where obscure legislation relating to theft and deception has been removed and replaced by statutory definitions of

fraudulent behaviour, such as those contained in the Fraud Act 2006 in the United Kingdom. However, this approach can go too far – criticism has been levelled at the UK legislation for effectively criminalising lying.

3. Beyond legal definitions, fraud means different things to those affected by it. Fraud affects both business and individuals. However, whilst understanding the concept and impact of identity theft, many people may not describe it as ‘fraud’.

4. The theft of data is an interesting case in point. It does not fit the normal concept of theft in that the data is usually duplicated and not entirely removed from the original owner. Theft of data does not automatically result in fraudulent activity, although it is often spoken of in that way. Indeed, highly publicised cases such as those in the UK involving the loss of millions of individuals’ details from both public and private sector bodies, may not result in any crime at all, if the data does not fall into criminal hands. The ratio of compromise to fraudulent use of data is a measurement of efficiency of a criminal market.

5. Businesses are often more aware of fraud than individuals and have increasingly comprehensive anti-fraud measures in place. This may be driven by their own awareness of the effect of fraud on their bottom line (and reputation) or, in regulated industries, by the requirements of regulators. Internal fraud is a major problem in many industries and not just from more junior level staff – senior executives also commit fraud and are positioned to cause significantly more damage and loss.

6. There is still a high degree of complacency about fraud amongst both individuals and businesses. However, there is an unfortunate tendency to regard the victims of fraud as either greedy, stupid or both. Fraudsters deliberately target the vulnerable. Sophisticated persons and businesses can be taken in by sophisticated scams. There can be an element of denial or an unwillingness to accept that they have been defrauded on the part of victims that can lead to repeat victimisation and can mean that frauds are not taken seriously by the judicial system.

6. There may be cultural or other issues, such as legal, financial or tax implications, to take into account. Businesses may prefer to classify fraud loss as 'bad debt' rather than admit to their shareholders or regulators that they have been subject to a significant level of fraud. As a further example, in some cultures fraud losses in lending may not even be classified as bad debt, but rather be counted as 'pending collection'. The time lag in identification of fraudulent behaviour in these cases can make true measurement difficult. Compensation of losses may also impact on the definition of fraud – in some cases a compensation scheme, paid for by the regulated institutions, will cover fraud losses to consumers.

7. Fraudsters are sophisticated and can target international weak points: they are often aware of the difficulties of international co-operation in information sharing and investigation. Major organised frauds often have an international dimension and this can impact badly on the reputation of a country and its government. The classic example is the use of the term 'Nigerian' or '419'¹ frauds. There is a common assumption that advance fee scams originate in Nigeria. This has been the case in the past and to an extent is still true, but efforts by the Nigerian authorities have resulted in large scale displacement and many of these scams are now based outside the country. Other nationalities are frequently found to be involved. 'Canadian' lottery scams are another example of mass- or tele-marketing frauds that have become commonly associated with a particular country, when in fact they are practised by crime groups in many different jurisdictions.

8. Given the difficulties in defining fraud, it is no wonder that measurement of the scale of the problem has proved problematic. Data sources such as police information (both reported cases and investigative intelligence), corporate fraud surveys, reviews of government department spending, and private sector victim surveys can be used to identify the scale of the problem in terms of direct monetary losses. However, it is much harder to measure the indirect harm of fraud. There are strong suggestions of links between fraud and other crimes such as drugs trafficking, people smuggling and terrorism. On the other hand, some of these assumptions are based on anecdotal evidence. Whilst these associations can be useful to raise awareness and to encourage the various actors to respond to fraud, the amount of

¹ So called after the relevant article of the Nigerian penal code

fraud that supports terrorism, for example, as a proportion of the whole is relatively small. Other indirect effects of fraud can include serious physical and mental health problems, especially for elderly or vulnerable victims of fraud, which in extreme cases can lead to suicide. It can also bring about a loss of confidence in legitimate investment.

9. How then to tackle the problem of fraud and ensure an international response when its scale and impact are difficult to measure and quantify? The investigation of fraud by law enforcement and prosecution of offenders through judicial systems can only be components of the response, albeit very important. Other efforts by public and private sectors, working both on their own and in partnership, must also focus on preventing and disrupting fraud. Public/private partnership, either in information sharing or other ways, is vitally important, but must not be seen as the panacea for all fraud ills – each sector must also take their own responsibilities to heart.

10. Much is made of public/private partnerships and the need for effective information sharing in particular. It is interesting to note that both parties tend to believe there is a disadvantageous asymmetry in information relating to fraud, thinking that the ‘other side’ hold more information than they are letting on and the belief that if only ‘they’ were more willing to share it, so much more could be done. This may actually represent the state of knowledge on fraud generally rather than an unwillingness to share information. In any case, sharing information is not the goal. The focus could be on the effective use of shared information to produce tangible results that reduce the harm from fraud. This is more difficult to achieve but a consideration of the potential outcome can shed light on the required nature and quality of information shared. There needs to be a balance between safeguarding civil liberties and personal information and the need to share sufficient data to enable progress in detecting and preventing fraud.

11. The anti-money laundering standards and requirements established over the last twenty years or so have significantly changed the expectations of financial institutions and their relationships with their customers. The creation of a series of obligations, such as identification of clients, record keeping, monitoring and reporting has resulted in a large scale sharing of citizens’ information, mainly by financial institutions with the public authorities. This is done primarily through suspicious

activity reports (SARs) made to Financial Intelligence Units (FIUs). It is clear that this compulsory sharing of information can lead to positive outcomes such as prosecution or asset recovery. However, this can be at great cost both in terms of the resources devoted to it and the altered relationship with the customer, with the institution acting almost as an agent of the state monitoring activities and reporting in secret. There has been no real cost benefit analysis of this change, it generally being held that money laundering is such a public evil that these measures are necessary.

12. These standards and requirements were originally introduced to deal with crimes such as drugs trafficking, where both public will and international co-operation are easy to gain. Often, but not always, these obligations now extend to predicate crimes such as fraud, where the financial institutions may be the victims as well as the facilitators. Increasingly, financial services regulators press, or compel, institutions to do more to prevent fraud than they would do left to their own devices, even where they are required to make good the losses suffered by their customers. This may lead to institutions spending on compliance for compliance sake, rather than focusing resources on the areas that their commercial analysis would identify as having most benefit.

13. Increasingly regulators and international bodies such as the Financial Action Task Force (FATF) talk about the 'risk based' approach to financial crime, a development broadly, but perhaps suspiciously, welcomed by the private sector. It can be accompanied by suggestions that private institutions are best placed to identify and mitigate their own risks. Institutions need reassurance that they are on the right lines, requiring greater expertise in line supervisors than is currently available, in cases where financial crime oversight is delegated to the prudential supervisor; or greater sharing of knowledge and co-ordination where there are specialist financial crime supervisors, such as the FIU. In any case, it cannot be demonstrated that individual institutions reacting to their own risks and vulnerabilities necessarily results in a strong combined defence to fraud at the national and international level. Threat assessments drawing on both public and private information and a gap analysis of counter-measures are required to provide this assurance. The focus on suspicious activity reporting (and the potential criminal sanction on institutions for failing to comply with it) should not be allowed to get in

the way of information sharing at a broader level, such as reporting on market activity in both legitimate and criminal markets.

14. The public and private sector partnership must go beyond information sharing. The two sectors can come together with a shared vision to develop strategies and systems to tackle fraud nationally and internationally. They could share experiences and, where appropriate, resources through regular meetings and networking. Partnership working relies on all partners having the right skills and experience to manage relationships, as well as the required counter fraud experience.

15. Public awareness and education provides a specific area for effective joint working. Information campaigns can do much to demonstrate the overall menace of fraud as well as the roles and responsibilities of individuals to combat it. Consumers could be educated to ensure that they are taking steps to protect themselves as well as to understand the wider impact of fraud. This would do much to overcome the widely held perception that fraud is a victimless crime. This view is compounded by the fact that most people are compensated for losses, without realising that they pay the price through, for example, higher insurance premiums.

16. The inter-action between public and private sector may also be misconstrued through the use of common terminology . 'Partnership' normally implies a common interest and benefit, whereas in this context it may be about ways in which different sectors work together and the rules of engagement for their interaction. Some of this can be compelled through law and regulation, but success depends on a common understanding of the benefits to society. Public/private information sharing may be unbalanced, with most information flowing from financial institutions, however, this is recognised and understood by those institutions. In return they seek feedback, both specific and generic, and also a clear articulation of the authorities' needs (within the 'need to know' principle). Greater understanding of the requirement can lead to the supply of better quality of information. Public authorities can also assist financial institutions understand and implement the intelligence process.

17. Regardless of the need for public/private partnership in all its manifestations, each sector must also recognise and take on its own responsibilities. The law enforcement agencies can legitimately query why they should devote time and

resources (and potentially put officers in harm's way) when an institution has taken a commercial decision not to tackle a problem in the first instance. On the other hand, the private sector may have cause to complain about the resources they devote to countering financial crime when they do not see an equivalent commitment from the public sector.

18. It is important that commitment and political will is demonstrated at the highest level, preferably with the appointment of someone at ministerial level who has responsibility for combating fraud or financial crime more widely. The international focus on anti-money laundering may well result in a department (often a finance ministry) having this particular responsibility, but fraud matters may be split between justice, trade and finance departments. A national strategy, with clear accountability, is a first step to effective co-ordinated action, but it is important to note that a strategy alone does not achieve anything. Implementation is the key to tangible results. Political will and leadership will encourage a culture where a fraud problem is acknowledged and addressed, rather than ignored and hidden.

19. Whilst national co-ordination involving the public sector agencies and representative bodies from the private sector is clearly desirable, issues may arise around independence and operational autonomy. For example, United Nations (UN) conventions require 'independent' bodies to deal with corruption matters; FIUs, particularly administrative ones based in government departments, may not be able to fulfil this role. On the other hand, there is often a question over the degree of independence afforded to investigating bodies, particularly given the need to interface with other official bodies during investigation. Ultimately, overt political interference in the decision making process is a clear indication of lack of independence.

20. A component of a national strategy may be that of the reporting requirements which, in theory, allow for better measurement of the scale of the problem and assessment of the effectiveness of counter-measures. However, this can be fraught with difficulties, with the potential not only for double counting, but also the imposition of further requirements on financial institutions, which will already have to comply with money laundering requirements. It may be an unfortunate accident of history that these requirements have historically focused on anti-money laundering, rather

than financial crime. The distinction may be clear in theory: SARs should not be used to make reports of crime. However, this becomes blurred in practice when the institution may be the victim and, unlike the situation with other predicate crimes, the laundered money is already in the system. The question arises of when the fraud ends and the laundering begins – having a joined up approach would remove this potential confusion. In any case, without a clear strategy and defined roles and responsibilities, anti-money laundering structures, focused around an FIU, may not deal efficiently with SARs relating to fraud, even if they have the ability to spot them.

21. Technology has a role to play in fraud detection, but can only ever be one tool. It is most useful in situations where large amounts of data are available, such as in financial institutions and FIUs, and where it is backed up by the human resources required to deal with alerts generated. The worst kind of assistance for developing or low capacity countries is technology without the appropriate training, resources and support in its use. However, if sufficient data is available, good outcomes can come from network analysis, in conjunction with traditional rules based systems (which attempt to codify an investigator's 'feel' for cases), data matching and data mining. Modern systems have the ability to search across free text as well as structured data, identifying network structures that could never be isolated manually, and can output this information in graphical ways that can make cases easier to present to investigators or, ultimately, to a court. Investing in such systems allows firms not only to investigate current and historic fraud, but also improve their detection and prevention efforts, and identify new and emerging fraud trends. Sharing of this information both with other private sector bodies and the public authorities can be a major component of a counter fraud system, but the firms will look for a *quid pro quo* in a reciprocal resource investment from the public sector and take up of those cases they identify as being sufficiently serious to warrant investigation by law enforcement.

22. Another element of a national strategy could be the creation of specialist bodies, or squads within existing agencies, to deal with fraud or aspects of fraud such as bribery and corruption. Such structures could provide career progression for those involved, as fraud (and financial crime) is a specialist area, requiring years of training for investigators. Ring-fencing resources in this way is another demonstration of political will. A review of legislation may highlight deficiencies that

can be rectified by introduction of new Acts, creating new offences to deal with current and future threats, and giving the investigative agencies the powers they require to effectively investigate fraud. Plea bargaining powers may prove effective tools, but only if the sanctions for fraud conviction are sufficiently high to make them appear attractive. 'Whistle blowing' can also be a useful source of valuable and early information, but is most effective when informants are provided with some statutory protection and firms are required to take internal reports seriously.

23. Of course, financial crime will not be stopped simply by the creation of new units and the introduction of laws. Those units must enforce those laws effectively, free from government interference, and in a targeted and prioritised way. 'Kingpin' offenders who are accustomed to operate with impunity can be targeted, steps taken to investigate top management at banks involved in outright fraud or in the complicit laundering of proceeds and corrupt public officials arrested. Such high profile action can have knock on effects in bank reform, public sector governance and displacement of criminal activity.

24. Partnership is also required between law enforcement investigative agencies and prosecutors to investigate fraud successfully. Success in an investigation should not be narrowly defined as the prosecution and conviction of the offenders – if this measure is taken most fraud will never be successfully investigated. There is simply too much reported fraud (let alone un-reported fraud) to be investigated by agencies with scarce resources and other priorities. Success could also include disruption or problem solving, and identifying ways to prevent or minimise the impact of frauds in the future.

25. Law enforcement clearly needs to prioritise efforts when they lack adequate resources. The decision over what cases to take on and the strategic drivers of case acceptance could be based, in part, on dialogue with the communities affected by fraud. This is particularly important with the commercial sector, where effective dialogue over emerging threats (for example from new financial products) can ensure the strategy remains up to date. Strategies should also be developed, in conjunction with prosecutors, on individual cases and the correct resources devoted to them in light of the desired outcome and the powers and constraints available to the investigation team. Traditionally fraud investigations have been lengthy affairs,

sometimes involving millions of documents, but a proper case strategy can focus an investigation, resulting in a shorter timescale and an easier case to present to a court. 'Success' should also be defined for each case, which will inform the enquiry's priorities and strands (for example, focusing on prevention aspects for dissemination to industry). It is tempting to overload indictments with many counts to reflect the nature of the fraud (telemarketing fraud may have many thousands of victims, for example). However it is important to seek focused charges which are fully supported by the evidence, capture the nature of the offence as linked to appropriate punishments, but which are easily presentable to the court and will not lead to over-lengthy trials. Good trial management is an important aspect of successful prosecution, as is complete and proper disclosure, even of facts adverse to the case.

26. Persistence and creativity are hallmarks of successful investigations. Bureaucracy and delays in obtaining information can be disheartening, but good fraud investigators find ways to deal with these frustrations. Co-operation with other agencies is vital and public/private partnership is important even in this investigative activity. The private sector, often the victim in frauds, may have useful information and investigative resources themselves. Imaginative use of international business contacts can often be a quicker way to obtain information from foreign jurisdictions.

27. Many major frauds have international components. Indeed, some frauds by their very nature will cross national boundaries, for example VAT 'carousel' frauds. However, law enforcement agencies and FIUs in different countries will not only have different priorities, but also different levels of experience and skill in investigating fraud, which may be defined differently in their jurisdiction. Different legal systems will also have to interact. Some systems may not traditionally involve prosecutors or magistrates at an early stage; in others a magistrate may be involved with the investigation from the outset. Best practice is to involve prosecutors from the early stages of an investigation, even if they have no formal control or role. This can go against deeply held principles that the prosecutor and investigator should be independent. Increasingly, special prosecutors are used to provide experience and knowledge of fraud investigations and in some places there are special tribunals with trained judiciary.

28. Even the most well run and successful investigations can only aspire to address a small minority of fraud activity. Other strategies must be developed to deal with the problem of fraud. For example, agencies should give consideration to developing offender focused investigations as well as offence based ones, becoming proactive rather than reactive. Such approaches must be predicated on a good intelligence picture of the major fraud offenders, which in turn requires well developed information sharing between public sector agencies, as well as public/private co-operation, and must also recognise that some classes of very significant fraud are essentially opportunistic in nature (such as 'rogue traders').

29. Other, more holistic, approaches could also be developed. Efforts to deal with large scale telemarketing frauds, such as those adopted in the Netherlands, could include all sectors involved, including telecommunications providers and financial institutions and adopt a prevention strand as well as focusing on offenders and victims. By examining money flows from victims abroad, not only is it possible to freeze numerous accounts, but also to identify changes in criminal behaviour, such as the use of money transfer systems rather than bank accounts. Understanding the use and procurement of false identities by criminals can enable the authorities to tighten controls and also to provide financial institutions with access to appropriate data to check documents produced at account opening. A successful tactic used in Nigeria is to target telephone lines and email addresses used to conduct 'advance fee' fraud. By providing the police with power to cut off such communication facilitation on reasonable suspicion of involvement in fraud, disruption can be achieved in addition to evidence gathering. Given the international nature of fraud and the globalisation not only of financial markets, but also the communications industry, the best results are achieved when international partners have similar powers, can act quickly and in concert, and share information effectively. Relying on mutual legal assistance treaties, with their slow and bureaucratic systems, can frustrate the aims. Personal contacts and networking are vital to follow criminal transactions across borders, with appropriate checks and balances to remain within legal constraints.

30. This approach can be extended to broader non-traditional techniques in the public sector. Rather than focus on up to 100 different typologies of fraud, analysis can reveal a small number of key fraud enablers, such as false identities, technology

and communications, access to data, corruption and use of accommodation addresses. Tackling issues relating to these enablers can reduce the threat and harm of fraud. Information can be shared with the relevant private sectors through alerts or outreach using dialogue teams to engage with them. Some jurisdictions have introduced vetted groups where sensitive strategic information can be shared with individuals from the private sector with appropriate clearances. This type of activity can be limited by the recipients' ability to respond in a cost effective way and care must be taken not to provide a commercial advantage for particular institutions. Short-term benefits may not be immediately apparent, but this model of information sharing may hold a key to future success.

31. In conclusion, successful national and international efforts to combat fraud must include political will and a co-ordinated approach between public sector agencies as well as public/private partnerships. International co-operation must be improved to take account of the nature of organised fraud and relationships developed between jurisdictions, whilst taking account of the problems developing countries face in implementing international standards. At the same time, new thinking must be developed to tackle fraud enablers, recognising that the best that can be hoped for is the minimisation of fraud, not its eradication, and technology has a key role to play. Investigative, intelligence and other tools can be used to tackle all types of financial crime, not fraud and money laundering separately, and precise analysis of the threat can lead to responses appropriate to particular jurisdictions.

David Artingstall
June 2008

Wilton Park Reports are brief summaries of the main points of a conference. The reports reflect rapporteurs' personal interpretations of the proceedings - as such they do not constitute any institutional policy of Wilton Park nor do they necessarily represent the views of rapporteurs.