The threat of fraud in the financial services sector has probably never been higher, and the risks to both banking institutions and their customers are many and various. At the same time, there is a strong public perception that the financial institutions themselves have been guilty of criminal misconduct. There are threats across a wide front: a major, and constantly emerging and evolving, cause of criminal activity in the financial sector is 'cybercrime'; even in 2016, the strains and problems caused by the 2007/8 financial crisis still persist; and at the same time, more old-fashioned forms of dishonesty are commonplace.

The capacity of regulators and law enforcement to stem this tide of criminality is constantly under challenge. The FCA, and its predecessor, the FSA, have both adopted a policy of 'credible deterrence' in dealing with threats to the integrity of the financial markets, taking the view that, while strong regulatory action remains the regulator's main weapon against breaches of regulation, criminal prosecution will have a deterrent effect against a range of misconduct. In response to these threats the FCA Enforcement and Market Oversight Division (EMO) can take a variety of actions. Where it decides to take criminal action, it can prosecute market abuse and misleading statements1 and investment frauds - indeed, following the Supreme Court decision in R v Rollins2, the FCA can prosecute almost any offence as part of its 'credible deterrence' policy; it can take regulatory and other civil actions to prevent and discourage criminal conduct; or it can refer cases to other investigators and prosecutors, including the Serious Fraud Office (Libor, Forex, for example) and the City of London Police. In addition, the FCA can work together with the Economic Crime Command, putting together teams of experts to share intelligence and to investigate the organised crime gangs which increasingly work in the financial sector.

The recent revision of statutory definitions of criminal offences of fraud (Fraud Act 2006), money laundering (Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007) and bribery (Bribery Act 2010) has changed the landscape of economic crime offences, but the impact of these changes against the mainstream UK regulated financial sector is hard to assess. If one included sharp practice and unethical conduct in the mix, the numbers would increase exponentially, but the extent of deliberate and dishonest criminal misconduct is less easy to identify.

The extent to which the financial sector has been the subject of prosecutions for fraud, arising either out of the causes of the global financial crisis, or out of longer term types of misconduct, is relatively low. The criminal investigations into Libor and Forex manipulation, referred by the FCA to the Serious Fraud Office from 2012 onwards, are one exception to this, but such prosecutions as have taken place for what might be referred to as 'old misconduct' by banks, have taken years to resolve, and have had mixed results. The overall impression created by the fact that many of the major banks engaged in benchmark manipulation over a lengthy period of time is that the banking sector is fundamentally lacking in proper standards of honesty and integrity. Payment Protection Insurance mis-selling may be said to come into a similar category. The combination of profit and ease of sale was clearly so tempting that management ignored, deliberately or otherwise, the obvious truth that their firms were indulging in mis-selling on a grand scale. As with Libor and Forex, the fact that almost everyone was doing it, and had been for some years, probably lent it some sort of bogus respectability, but in truth it was on the borderline between sharp practice and misrepresentation that is hard to patrol.

The fact that large parts of the population regard bankers as little better than rogues and cheats is a major issue. The Parliamentary Commission on Banking Standards (PCBS) clearly shares this view, and has been instrumental in promoting legislation to punish such misconduct, and to improve standards. At the same time there has been increased vigilance around anti-money laundering (AML) and anti-bribery and corruption (ABC), with FCA thematic reviews exposing poor systems and controls across the sector, and regular – and enormous – fines being imposed by both the UK and US regulators, particularly for AML failings (and sanctions, in the case of the United States). This has undoubtedly led to a greatly increased focus by banks on ABC and AML risks and compliance.

[1] Section 397 Financial Services and Markets Act 2000
[2] [2010] UKSC 39

Meanwhile the PCBS noted, as have many others, that senior management has tended to avoid the consequences of their firms' misconduct, and proposed some solutions to this problem. Evidence of knowledge at board level of the dishonest activities of bankers at lower echelons in firms has not tended to find its way into the hands of investigators, and the chain of incriminating e-mails dries up somewhere in middle management according to the Director of the Serious Fraud Office.

Pressure from the PCBS has led to new criminal offences being drafted which, it is hoped, will have the beneficial effect of making bankers who occupy senior management positions think twice before embarking on, or permitting the continuation of, risky or dishonest conduct. For example, section 36 of the Financial Services (Banking Reform) Act 2013, created an offence 'relating to a decision causing a financial institution to fail'. The offence can be committed by a senior manager, who either takes a decision that might lead to the failure of the institution, or fails to prevent such a decision being taken, knowing that there is a risk, and the decision leads to the failure of the institution. The section is intended to apply to senior management in circumstances similar to those which led to the failures of Royal Bank of Scotland and HBOS.

Section 91 of the Financial Services Act 2012 amended section 397 of the 2000 Act (misleading statements) to create an offence of manipulating benchmarks, so that in future it should be easier to prosecute such conduct.

The risky banking and benchmark offences both carry a maximum 7 year sentence. The existence of such specific offences will dispel any doubts there might have been about whether such conduct is dishonest, and is clearly intended to discourage risky and unethical banking.

However, there is an element of closing the stable door after the horse has bolted. It might also be said that the section 36 offence will be unprosecutable, and may simply encourage avoidance strategies that will not be difficult to devise.

Section 7 of the Bribery Act 2010 creates a corporate offence of failing to prevent bribery. There are future legislative plans (the Criminal Finance Bill) to create similar corporate offences relating to economic crime, tax evasion and money laundering.

Because senior management has largely escaped prosecution, a new senior managers regime and a system of attestations has been introduced by the FCA for banks, insurers, and some other firms, and although this will lead to regulatory sanctions, it may also have the effect of bringing senior management into the frame for criminal misconduct because a direct line of accountability will exist between managers and board.

While there has been intense pressure to bring bankers to account at the top end of the financial services sector, with a view to preventing a repetition of the banking crisis, at the other end of the scale a war is being fought against those who use and abuse the financial services sector to defraud individuals. Boiler rooms and other investment scams relating, for example, to pension release and equity release, target vulnerable victims who are tempted by the offer of much better returns on their cash than more traditional investment can achieve. The extent of this form of criminal activity is enormous, and the resources to fight it are stretched, even though investigators and prosecutors are working hard together to meet the challenge by pooling skills and intelligence across agencies and borders.

Unauthorised business cases are dealt with in a variety of criminal and non-criminal ways. The majority of cases are subject to winding up petitions and asset freezing orders, but the more egregious cases, with repeat offenders and large losses, are selected for criminal investigation. A number of prosecutions in the Crown Court have been successful, with significant custodial sentences passed against those convicted. Offenders include not only the operators of the investment frauds, but also their lawyers and accountants. Professional 'enablers' are recognised as a prime target for investigators.

One reason for pursuing such criminal activity is that it may be closely related to terrorist funding; or that it is linked to organised criminal gangs. The government has made the pursuit of such activity a priority.

STRESSES AND STRAINS

The combination of these threats, both from within and from outside the financial services industry, presents challenges for the regulator. Quite apart from the austerity measures that have had an adverse impact on the UK

economy, and its public services, conduct issues that contributed to the crisis are still troubling Enforcement teams. Not only are they dealing with the criminal fall-out from such conduct, but they had to face severe criticism for their supervision of governance, management and systems and controls failures in the run up to the crisis,

Examination of the FCA's own systems and controls has led to a re-evaluation of intervention standards, with a fresh emphasis on early intervention, and prevention rather than cure.

Reliance on office based assessments by Supervisors of tick-box returns has been significantly replaced by site visits where the underlying culture of a business can be experienced at first hand. This new approach may well lead to quicker and better recognition of financial crime, which will soon be introduced as a specific measure. While this development is greatly to be welcomed, it requires levels of skill and judgement that are much less easy to acquire and deploy than counting ticks in boxes. Because the line between regulatory and criminal misconduct is often narrow, that assessment of the integrity of individual firms, and the appropriate response to the uncovering of regulatory and other breaches, becomes more complex.

Investigating and prosecuting misconduct, whether it be market abuse or money laundering, is much more complex and time-consuming than taking a regulatory case before the RDC, even if it is contested to appeal stage in the Upper Tribunal or the Court of Appeal. The resources available to EMO to tackle criminal cases have to be balanced against other needs. The £14m allegedly spent on the Tabernula market abuse investigation and prosecution between 2008 and 2016 can be justified in terms of the deterrent effect of prosecuting some senior banking figures, but there is clearly a limit to the FCA budget for such cases. The prioritisation of cases for criminal prosecution is a delicately balanced decision-making process. The guidance set out in chapter 12 of the Enforcement Guide is comprehensive, but it does not take account of stretched resources.

Part of the reason for the huge expense and difficulty of bringing criminal cases to trial is that the system is subject to a number of obstacles. While it will be argued that such obstacles are essential to a proper and fair criminal justice system, there are ways in which improvements could be made without compromising the quality of justice:

One major hurdle in bringing criminal cases to trial is the disclosure process under the Criminal Procedure and Investigations Act 1996 (CPIA). It is not uncommon in a large FCA criminal investigation for a team of 6 lawyers to be employed for a year to carry out a thorough disclosure exercise. Even when great care, expense and skill is applied to compliance with CPIA, there is always a risk that a disclosure problem will cause a trial to be aborted.

Another hurdle is the management of digital material collected in the course of an investigation. There will often be mega-bytes, if not tera-bytes, of such material, and not only does it have to be securely stored, it must also be sifted for relevance, disclosure and privilege. The cost of the analysis of seized evidence is huge. The systems that are used to conduct this work are expensive, and are frequently in need of up-dating.

Trial management is also a challenge. Fraud cases will often involve several accused, and a wide array of possible charges involving many individual transactions. Crown Court judges will usually insist that the case will not last longer than 3 months, and this instruction almost always involves prosecutors in a number of difficult choices, including whether to sever the case between defendants and/or to reduce the number of counts on the indictment. While the logic of this approach is unassailable, and it can often be said that a pared down case is less likely to fall victim to difficult legal and evidential challenges, it is a frustrating exercise.

Complex fraud trials usually require expert evidence both to prove technical points and to explain matters to the jury. The choice and instruction of an expert is a notoriously difficult exercise. When an expert is successfully challenged by a defence advocate, it can have a seriously adverse impact on the success of a prosecution.

The FCA often shares intelligence with, and will sometimes refer cases to, other investigators and prosecutors, but although there is a coordinated effort to crack down on savings, investments and pensions fraud, and to break up boiler rooms, investigating these serious criminal cases requires a degree of skill and persistence and budget that cannot always be available.

The FSA and the FCA have by and large met all these challenges, and the regulator is generally regarded as an effective investigator and prosecutor. Like all prosecutors, it does not win all its cases, but it may be said that this means that it is tackling the most challenging cases rather than the gathering low hanging fruit.

FUTURE INFLUENCES

There have been a number of attempts to reform the trial of fraud cases. Trial management is high on the agenda. Non-jury trial in complex fraud cases has been considered, although it is not currently under consideration following the failure some years ago to obtain an affirmative resolution of both Houses to implement a provision in the 2003 Criminal Justice Act. The House of Lords is implacably opposed, it seems, to any interference with the right to jury trial. However, this issue will probably be debated again before long, particularly if there is a perception that the complexities of financial matters have developed so far as to make it impossible to present a case to a jury. The difficulty of bringing complex fraud cases to trial is a significant inhibition to any attempt to investigate and prosecute. Any improvements in this area should be welcomed.

Another possible development will be the introduction of a range of quasi-criminal charges, similar to regulatory breaches, which will not attract prison sentences, but will result in fines and prohibitions and confiscation. Forms of 'alternative dispute resolution', of which the recently introduced Deferred Prosecution Agreements are an example, may also be brought into play. It remains to be seen how far such initiatives will go in dealing with individual offenders, bearing in mind that the force behind the 'credible deterrence' policy is that the threat of imprisonment has a higher chance of deterring misconduct than financial and other non-custodial sentences. This may be a correct assumption, and it may also chime in with a public thirst for revenge against deviant bankers, but consideration should also be given to the fact that significant financial penalties, both in the form of fines and confiscation, reputational damage, and prohibition are all severe punishments that undoubtedly have a deterrent effect.

In terms of the types of offences that will become prevalent, it is often said that developments in technology will assist fraudsters far more than they will assist those seeking to combat their activities. Cybercrime will develop new capacities and formats, taking advantage of digital activity, and of our reliance on the internet for banking and shopping. As is already the case, tracking down those responsible for criminal actions in this sphere will be extremely difficult, and will inevitably become more so.

New banking arrangements, crowd funding and other forms of alternative finance, new currency models and many other developments in financial markets will create ever increasing fraud opportunities. The margin between authorised and unauthorised business will become ever harder to define. The regulator's capacity both to assess the integrity of the new products, and to police them when they are introduced, will be challenged. At the same time, the level of understanding of more complex financial media will be a mystery to a large section of the population, creating ever increasing opportunities for fraudsters.

The global reach of fraudsters, whether engaged in boiler rooms, land banking or phishing, or other new and improved forms of scamming, making assaults on our bank accounts, savings, investments and pensions, and their capacity to operate from anywhere in the world, and hide behind a range of off-shore trusts and beneficial ownerships, makes it easy to commit serious crimes without any real risk of being apprehended. Funds might be recovered if speedy action is taken, but bringing a cybercriminal to justice will always be a challenge. Whether in future law enforcement agencies will have sufficient resources and skills to pursue such cases may be open to doubt. However, there has been a serious investment in intelligence capacity, and pressure to share intelligence between agencies, both nationally and internationally, and this investment should pay dividends. There are also systems in development that are designed to provide intelligence links between financial activity, and which may have the capacity to redress the balance between criminals and law enforcement.

There is also a serious issue with the reporting of fraud. Our personal, corporate and public sector finances have built in an increasing acceptance of a level of fraud as the price we pay for the convenience of utilising complex banking systems in everyday life. There is discussion about the level of fraud that goes unreported. At one level this must lead to complacency about the threat. At another level, it permits some serious criminals to operate with impunity. But for most of us, the fact that we will often be reimbursed by our bank for losses suffered when our accounts are hacked, means that we are not interested in curing the source of the problem by pursuing the matter through a report to the police, unless a crime report reference is required for insurance purposes.

The current focus on anti-money laundering and bribery across the business world will continue to have a major impact on the financial sector. The massive increase in the compliance effort that firms have installed in their

systems and controls will probably have the effect of reducing, or keeping in check, the level of this type of criminal activity. The increased attention of governments and NGOs will sustain this downward pressure on the banking sector.

However, it would be foolish to be complacent. Law enforcement changes its priorities, and government interest is easily diverted. Generous funding at the outset of a new project all too quickly disappears after two or three years. New priorities are identified, and resources are moved to a new initiative.

Banks can easily divert their energies away from expensive compliance regimes to profitable new enterprises whose risks and consequences are not properly assessed until it is too late. Shareholders will soon become impatient with the low returns on investment of safe and steady retail banking, and will welcome the introduction of riskier models. Even government might prefer to see tax revenue, and the profitability and status brought to the City of London as a global financial centre, flowing from more 'innovative' banking products which are not weighed down by the negative caution of a compliance department.

Early intervention is clearly the right approach when doubts are raised about the integrity of a course of conduct or a new product, but if the assumption is that this will always identify and bring to an end criminal or quasi-criminal misconduct before severe damage has been caused, there will be serious disappointment. One only has to look back over the last decade to see the consequences of failures to act decisively and early: consider the eagerness with which all concerned embraced toxic debt, and the length of time it took to recognise that PPI was a deeply flawed form of insurance. The failure, in spite of specific and credible warnings, to uncover the Madoff Ponzi showed that sheer neck is a good defence against discovery. There are many other examples. An examination of each one will demonstrate the problems involved in identifying and intervening and resolving such cases before the damage is done – and before, therefore, there is clear evidence of wrong-doing.

CHALLENGING ASSUMPTIONS

Making any assumptions about how the financial world will conduct itself in the decade up to 2030, and how law enforcers and regulators can respond to any consequent misconduct, is dangerous and probably impossible. Existing problems, particularly in the cybercrime sphere, will continue to challenge law enforcement, and at the same time the pace of change, and the outside influences – the consequences of Brexit and the future constitution of the EU, the increasing power of the economies of China and India (or the reverse), Middle East conflict, another global financial meltdown – might create additional opportunities for criminal detriment, at the same time as promoting unethical behaviours.

It would therefore be unwise to predict that there will be fewer financial disasters over the next decade. The problems will be a mix of the innovative and the well-established. The Emperor's new clothes will be as effective in concealing deceit as new-fangled trading strategies.

Two main questions arise from this: first, can the criminal law be used to act as an effective bulwark against the increasingly sophisticated activities of those engaged in trying (and often succeeding) to steal our assets? Second, is the criminal law the right tool to use to pursue and punish unethical or improper conduct in the banking sector?

Existing fraud offences (principally POCA 2002, the Fraud Act 2006, the Bribery Act 2010) provide a reasonable framework for tackling traditional fraud offences. In particular, it is highly unlikely that any changes will be made to the Fraud Act and the Bribery Act, which have both been regarded as 'the gold standard', in the foreseeable future. Indeed, it is not easy to see how the criminal law could accommodate radical departures from these Acts.

The offences set out in POCA, and its predecessors and successors, are testimony to the assumption that attacking money laundering is an effective way of tackling the existing range of financial and organised criminal activities, as well as any future problems. The Criminal Finance Bill represents a small step in improving the process. The National Crime Agency's priority of proactively identifying and closing down Organised Crime Groups, and spotting professional enablers and other supporters of OCGs, should lead to a reduction in the levels of such crime. However, whether POCA, and the anti-money laundering regime, are the panacea for all ills, as some believe, may be doubted, but in any event what is needed in order to give it extra power is a step change in resources and capability.

What part can a financial regulator play in this rethink? The tried and tested means of attack – systems and controls failures and a raft of regulation aimed at the full range of financial services industries – assist in containing the problems, but is there a sharper way of making the banking system more bullet-proof? The answer probably, and inevitably, lies in cleverer technology, backed up by specialist training.

There is, however, a broader question: has all the focus on AML since 1993 paid the kind of dividends that we have been promised? London's unenviable reputation, whether deserved or not, of being a global money laundering centre, coupled with few prosecutions and a lamentably low level of recovery of the proceeds of crime, suggests that the answer to that question is a firm 'no'. Given the huge expense incurred by the private sector in trying to comply with the rules and regulations, not to mention the significant inconvenience to every member of the public when they try to open a bank account or enter into any significant financial agreement, has the time come to rethink the whole system?

Changes to the SARS regime set out in a recent Home Office 'Action Plan', and also being consulted on in the Criminal Finance Bill, suggest that law enforcement does not believe that the current structures of law enforcement, legislation and criminal justice are working in relation to the use of the UK banking system to combat economic crime, terrorist financing or cybercrime. The planned new measures are designed to make better use of the resources, both public and private, that are now devoted to this challenge, particularly by targeting organisations that conduct money laundering, as opposed to looking at individual transactions. There will also be provisions to improve the capacity of investigators and the criminal justice system to identify and, more importantly, recover criminal assets. All this may mark a move away from reliance on an intelligence format that gathers information indiscriminately, and depends on firms and organisations to provide that information, towards a more focused and law enforcement driven analysis of high risk activity.

Turning to the second question, how far can or should we rely on the criminal law to deal with unethical conduct by banking professionals, only time will tell. The impact of the reckless banking and benchmark offences is more likely to be cautionary than implemented. The possibility that any senior banker will be successfully prosecuted under section 36 of the Financial Services (Banking Reform) Act 2012 seems, as stated above, very remote, but the existence of the offence may deter reckless conduct. The next banking crisis will throw up new challenges for regulators (how quickly should they react, what form should retribution take, should the media and public thirst for revenge drive the agenda?), and once again it is likely that law enforcement and regulation will be judged to have been wrong-footed.

Benchmark manipulation is unlikely to recur in relation to Libor and Forex, and therefore the amended section 397 Financial Services Act 2000 may not be called into use. The Libor prosecutions by the Serious Fraud Office, using existing offences, have worked reasonably well, but at a very considerable cost to the criminal justice system. However, the Forex investigations had to be terminated without charges and trials, due to insufficient evidence, but also one suspects because of the sheer difficulty and expense of pursuing the complex allegations.

The bad behaviour that will be left exposed in the wake of the next financial crisis will be different, and by the time it is exposed, the damage will have been done. The means of countering it will have to be created after the event, and law enforcement will be left scratching their collective heads in deciding how best to respond.

Therefore, difficult decisions have to be taken in deciding whether the criminal law is the right forum for adjudicating improper behaviour in highly complex situations, or whether regulatory fines and prohibitions are a sufficient, and more cost-effective, deterrent. It will also be essential to ensure that the law enforcement response to fraud, money laundering and bribery will keep pace with the threats posed, but it is highly likely that resources will be stretched both because of the high cost involved in pursuing such cases to the criminal standard, and because the skills needed to respond are not easy to acquire.

The FCA will face a challenge in deploying its resources to counter the threats of fraud in the financial services sector, but it can and must take a leading role in ensuring that overall banking and other financial sector standards are sufficiently robust to minimize the damage to consumers, business, and the UK economy caused by financial crime

CONTACT

David N. Kirk

Partner

+44 20 7632 1685
dkirk@mcguirewoods.com

11 Pilgrim Street
London EC4V 6RN