

In 2006

The Fraud Review

talked of an anti-fraud culture throughout society based on deterrence, prevention, detection, investigation, sanctions and redress for victims.

Ten years on we ask, has government delivered this promise?

Five steps that will make a difference

- 1. A well-funded and sustained public education campaign.** This is urgently needed: to help people understand and tackle fraud risks online and in the real world; to raise awareness of the subtle warning signs of deception; and to soften unhelpful attitudes to victims. Make it a priority for the newly-announced fraud taskforce.
- 2. A new body with strategic oversight.** The fight on fraud needs someone to stand back from the fray and take the long view: improving the openness, transparency and accountability of fraud initiatives; bringing people and organisations together; identifying gaps, preventing duplications and monitoring outcomes.
- 3. A government-led fraud indicator.** A five-yearly fraud 'census', independent of commercial interests, could provide the broad indication of scale and direction we need but at a much lower cost than the old annual indicator.
- 4. An improved local law enforcement response.** An unintended consequence of Action Fraud has been that too many local police forces no longer feel that fraud is their responsibility. Every local force must have the capacity, experience and resources to deal with the victims of fraud and online crime properly.
- 5. Overhaul of the disclosure regime.** While the criminal justice system tries to limit the length of complex trials to three months, the three years it takes to bring a case to trial goes almost overlooked. The main problem is a one-size-fits-all disclosure regime that is not fit-for-purpose in a complex fraud trial.

Ten years since the Fraud Review

2006

Fraud Review published

Fraud Act 2006 receives royal assent

2007

Government response published

Fraud Act 2006 comes into force

2008

National Fraud Strategic Authority established

City of London Police becomes national lead force

2009

NFSA becomes National Fraud Authority

National fraud strategy published

Action Fraud established

National Fraud Intelligence Bureau established

2010

1st annual fraud indicator published

Action Fraud rolled out

Bribery Act 2010 receives royal assent

A sea change

When the government published the final report of its landmark Fraud Review, in July 2006, we welcomed it enthusiastically and were proud to see so many Fraud Advisory Panel proposals included.

Here, at last, was a comprehensive and serious-minded government acknowledgement of some very uncomfortable truths.

- ◆ Fraudsters were making victims of us all by corroding and distorting the civic, commercial and economic life of our communities and our country.
- ◆ The full, true cost of fraud was enormous and second only to the trafficking of the most dangerous drugs.
- ◆ And yet the criminal justice response was under-resourced, lacked coordination and was no match for the threat.

The review was a brave move by Lord Goldsmith, the then attorney general, with no obvious political pay-back (as he acknowledges on page 2). But it promised to recalibrate public and professional expectations of what a national anti-fraud response could be, and it marked a sea change in official attitudes to fraud. Nonetheless, amid the plaudits, we warned that this must be a beginning, not an end; a ‘springboard for action’.

So here we are, 10 years on. The Fraud Review talked of creating an ‘anti-fraud culture throughout society [based on] deterrence, prevention, detection, investigation, sanctions and redress for victims’. Has government been able to deliver this promise? Did it even try? Does it still? And what happened to those few proposals about which we had significant concerns?

2011

2nd annual fraud indicator published
Fighting Fraud Together national strategy published
 Bribery Act 2010 comes into force

2012

3rd annual fraud indicator published

2013

4th annual fraud indicator published
 National Crime Agency established

2014

National Fraud Authority closes
 Fraud strategy transfers to NCA
 Action Fraud transfers to City of London Police

2016

Action Fraud (version two) launched

Beginnings: An interview with Lord Goldsmith

The Fraud Review was the brainchild of the then attorney general, Lord Peter Goldsmith QC PC. Here he reflects on some of his reasons for launching the review and some of the challenges it presented along the way.

Q. What prompted you to launch the Fraud Review?

- A. It seemed to me that fraud was one gaping area where our response – from the police, investigating authorities and justice system – was inadequate. It was obvious that fraud was costing people a huge amount of money yet very difficult to deal with. Police forces found it much easier to deal with the stealing of milk bottles than with the defrauding of people out of very much larger amounts.

By the time we did the review only a handful of police forces had their own fraud teams. Fraud wasn't a priority and there wasn't an incentive to deal with it. It seemed to take such a long time to get decisions from the fraud prosecuting authorities. And it was a scandal how long the trials would take, with inefficiency and failure often producing inconclusive results.

As one senior judge told me, if he'd wanted to be a criminal he would undoubtedly have turned to fraud.

Q. And yet there was no political gain to be had in conducting the review?

- A. That's right. If anything *[laughs]* there was the opposite of 'gain'. The attorney general is a much less political figure – though politically appointed and close to senior ministers – so political gain wasn't the driving issue as far as I was concerned. My view was really: you do what you think is right, you try to persuade people it is right, and then you see what happens.

Q. The Fraud Review's recommendations have transformed the official response to tackling fraud in this country. What aspect of the review are you most proud of and why?

- A. I hope that's true. I would like it to be true. If the Fraud Review has raised awareness of fraud as a serious social problem – not a victimless crime – then that is what I am most proud of. And that has become even more important today, with the degree of internet fraud that takes place and the cyber security issues. Cyber security wasn't really something we were thinking about at all in the first half of 2005–06.

Q. Why were the police not tackling fraud more vigorously?

- A. There was no incentive because it didn't figure in the relevant key performance indicators, so it wasn't a policing priority. I talked quite a lot to the Home Office about whether I could get fraud on to the national policing priority list. And then there was a lack of fraud expertise. Only a handful of local forces had the necessary fraud skills, and as fraud became more complicated – with computers, the internet and all the rest of it – so this became even more difficult. Fraud is also expensive to deal with.



Q. Were there important lessons to be learned from the US?

A. I looked, as I had on a number of other criminal justice issues, at the experience in other countries, particularly the US. Not to follow the US slavishly, but just to understand what it was they were doing that we weren't. They seemed to be so much better and more effective at tackling fraud in the courts than we were – some may say too effective. I was concerned, as I think we all were, that one of the reasons was because sentencing powers in the US were very, very strong, with the consequence it was often much easier for individuals to plead guilty – perhaps even if they had hesitation about their guilt – so as to avoid some very serious penalties. I thought, let's look at this because maybe we can have the benefits of a more efficient system without the draconian punishments at the end.

Q. There was quite a lot of opposition to non-jury fraud trials. Did the strength of feeling create problems?

A. The short and honest answer is 'yes'.

I thought that having certain fraud trials conducted without a jury was a justified reform to consider – and so indeed did many senior judges – but politically it became extremely difficult. I remember taking the proposals to the House of Lords and an opposition spokesman almost foaming at the mouth with anger. How could I propose this outrageous removal of the birthright of Englishmen? I thought it was a practical measure.

I persuaded cabinet colleagues to allow us to put the proposals forward twice, I think. But they wouldn't countenance another. They were probably right. The prospects weren't sufficiently good to justify a third attempt. The Fraud Review wasn't at the top of anyone else's agenda, but generally the cabinet was supportive.

‘By the time we did the review only a handful of police forces had their own fraud teams. Fraud wasn't a priority and there wasn't an incentive to deal with it. It seemed to take such a long time to get decisions from the fraud prosecuting authorities.’

Lord Peter Goldsmith QC PC

Q. Was that your only difference of opinion with the judiciary?

A. I also believe that it should be possible to have a real idea of what penalty will be imposed if someone pleads guilty. In the US they don't understand how we run a busy docket system without some ability to do this. There was a very strong push-back from the judiciary who felt that sentencing was the job of judges, not prosecutors. Prosecutors are a key part of our justice system; I don't see why you can't trust them to discuss, debate and reach agreements, subject to approval by the courts. It would cut down on cases and make a more efficient system: easier for victims because it is faster, and easier for defendants because they go into a case knowing what's going to happen to them.

Q. So are Deferred Prosecution Agreements a step in the right direction?

A. I think they are an important development. Speaking as a backbencher in the House of Lords, I said I thought there were areas in which the legislation did not go far enough. I was told that the government would look at it again after it had been in operation for a time. So there is, perhaps, more of that to come.

Q. The National Fraud Authority is now disbanded. Are you disappointed by this development?

A. Well, austerity and government cost-cutting have caused quite a number of things I don't welcome. I don't actually know to what extent that was a part of the decision, but I can't believe it wasn't.

I thought it was a very good initiative to have a National Fraud Strategic Authority: first of all, fraud needs to be tackled; secondly, it's not straightforward in terms of how you deal with it – you do need to work with industry, retailers, banks, insurance companies, as well as dealing in the criminal justice system; and you need to make sure that the resources are available. It would be a great shame if the only resources to tackle fraud are concentrated in the Serious Fraud Office. I am a great supporter of the SFO, but there's a lot more fraud that needs strategic thinking.

The way policing is set up in this country, with individual forces, we can lack a national authority to deal with certain things. The City of London Police increasingly took this on in relation to fraud and, I am glad to say, now has that role officially to provide a national resource.

Q. Did the Fraud Review achieve what it set out to achieve?

A. Yes it did. This was no knee-jerk reaction; it wasn't a populist document to grab tabloid newspaper headlines. It was a blueprint created by people who had looked at it carefully and knew what they were talking about. If you are tackling something as difficult as fraud you do need to have an evidence-based approach and that is what the experts who sat on the review were seeking to do. I think they did a very good job, taking a sober, balanced approach and producing very valuable recommendations. I thanked them for it then, and I thank them again. I never expected unanimous or even widespread support for some of the recommendations. I am glad that quite a lot of the report has been carried through into practice.

Is the state still failing on fraud? In 2006 the Fraud Advisory Panel came to the inescapable conclusion that the state was failing in one of its basic duties: to offer citizens a reasonable level of protection against fraud.

The Fraud Review had laid out in detail the sources of this failure.

- ◆ Poor understanding of the nature, extent and harm done because much of the information required wasn't collected or collectable.
- ◆ No shortage of agencies with fraud-related powers, but no national policy or mechanisms for achieving efficient, sustainable, coordinated action.
- ◆ Limited state resources such that people without means were excluded from justice and whole categories of low- and medium-value economic crimes were hardly ever looked into.
- ◆ Weaknesses in prosecutorial and judicial processes, along with flaws in the law, actively obstructed the reliable delivery of justice.

All of which added up to an unacceptably small chance that a fraudster would be prosecuted or, for the 'unlucky' few, penalties so low that they were an insult to victims and no kind of deterrent.

WHERE ARE WE NOW?

In recent years there have been many notable improvements in our ability to fight fraud, with many of them dating back to the Fraud Review.

- ◆ The City of London Police is the national lead force with additional funding to support counter-fraud policing across the country.
- ◆ Action Fraud is the world's first single-point fraud reporting system, with the National Fraud Intelligence Bureau (NFIB) analysing, packaging and distributing the information collected.
- ◆ The Fraud Act 2006 introduced the first offence of fraud, making fraud prosecutions more efficient.
- ◆ More recently, the Bribery Act 2010 – arguably the strictest anti-bribery legislation in the world – created the first corporate offence of 'failure to prevent'.

But, in many of the main problem areas identified by the Fraud Review, progress has been modest, patchy, non-existent or reversed.

Coordination and strategy

With the abolition of the National Fraud Authority we lost the only body specifically charged with creating a coordinated, multi-agency, public-private fraud response working to a strongly evidence-based strategy. Recent government pronouncements on cybercrime (Treasury), banking (Home Office), fraud statistics (Culture, Media and Sport), corruption (the prime minister) and public sector fraud (Cabinet Office) do not suggest a coordinated approach.

Understanding

The only systematic attempt to measure and update the true size and shape of the fraud threat – the annual fraud indicator – was also abolished in 2014. Information on fraud types and sectoral threats remains patchy and fragmented, with no attempt to create common methodologies or raise standards.

Resources

The government's austerity-based response to the 2008 recession has meant sharp cuts to budgets in almost every area of criminal justice and fraud fighting.

Systemic flaws and weaknesses

Most of the criminal justice system problems persist: limited police resources nationwide; few reported frauds investigated; long, drawn-out prosecutions with unpredictable outcomes; too many short sentences; and a poor deal for victims.

Low risk to fraudsters

Even now few frauds are investigated. Police resources are focused on those involving organised crime gangs or linked to the national security threats from terrorism or cybercrime. Since many of these are committed from abroad, very few perpetrators are brought to justice.

But by far the greatest setback to the state's efforts to protect its citizens from fraud has been the explosion of inexpensive, powerful and portable communications and computing devices connected by cheap, fast networks.

‘What is being done for all the people losing small but vital sums every day? Scamming is big, growing and doing enormous harm: equity release, pension release, investment frauds – the opportunities are endless. It's the Wild West out there and it is not enough to leave these people with only an Action Fraud crime number and no hope of seeing a police officer, never mind an investigation.’

David Kirk, chair of the Fraud Advisory Panel

Still searching for a national strategy

The Panel has long argued for the creation of a National Economic Crime Commission, dedicated to building an holistic, long-term approach.

The National Fraud Strategic Authority (NFSA) created by the Fraud Review was intended to be just such a body. We applauded the objective, but had deep concerns from the start; the NFSA was to be made responsible for front-line strategy implementation but given no powers to make that happen. This was a recipe for confused governance, frustration and delay.

Even so, we were disappointed to see the National Fraud Authority (as it had become) disbanded in March 2014. It was particularly dispiriting to see a body set up as an antidote to the traditional ebb and flow of official interest in fraud (and the patchy response inevitably created) dismantled in summary fashion.

Such a body is still needed to sit above the fray and to:

- ◆ create a well-informed understanding of the problems, a common strategy for tackling them, and then to unite the fraud-fighting community in getting on with it;
- ◆ identify and fix the many resource duplications and gaps that inevitably emerge in so complex a fabric of fraud fighting;
- ◆ nag politicians about the continuing need for robust policies and make Whitehall more accountable and engaged; and
- ◆ build public and political support for the effort that a truly effective fraud response would require of us all.

‘The concept of having a strategic body – pulling things together at the centre, being a champion, holding people to account for measured performance – was not always comfortable for some stakeholders.’

Sandra Quinn, NFSA interim and founding chief executive (2007-09)

THE NFA LEGACY

One of the greatest strengths of the NFA was its ability to push forward valuable projects that might otherwise get tied up in red tape. Without it, Action Fraud (for example) might still be trudging through procurement.

It also created a national fraud strategy, *Fighting Fraud Together*, with the backing of 37 separate bodies. It was the first time so many government, industry, voluntary and law enforcement organisations had come together to sign a joint commitment to tackle fraud.

TASK FORCES AND WORKING GROUPS

Recent ministerial announcements point to a government once more taking a close interest in particular types of fraud, but seemingly not paying much attention to the big picture.

- ◆ A new joint fraud task force will bring together banks, payment providers, the police, wider law enforcement and regulators in ‘a new type of partnership’.
- ◆ A new cross-government taskforce will ensure that the so-called Panama Papers are ‘fully investigated’.
- ◆ Talk of a new corporate criminal offence of failing to prevent tax evasion (£14bn in 2012) suggests a greater willingness to tackle public fraud more widely.
- ◆ A new anti-money laundering (AML) action plan includes a seven-strong list of joint ‘lead’ organisations.
- ◆ A new national cyber security plan to protect the ‘Critical National Infrastructure’ will spend £1.9bn over five years and include a new National Cyber Centre.

When all is said and done, can a list of initiatives – with no explicit mechanisms to foster cooperation or to monitor and measure progress and outcomes – ever add up to any kind of strategy?

Today there is a growing suspicion that we are once more lurching from one initiative to another, without the continuity of purpose and stability of institutions and budgets to build real capacity and resilience over the long term.

‘Looking at the government’s announcements, these are praiseworthy; but will the resources be made available to make them work? Money spent on fraud prevention is an investment and the returns can be very large.’

David Kirk, chair of the Fraud Advisory Panel

Joint fraud task force

The home secretary launched the new joint fraud task force with these words: 'For too long, there has been too little understanding of the problem and too great a reluctance to take steps to tackle it.' It was as if the Fraud Review, and all that flowed from it – NFA, annual fraud indicator, lead force, Action Fraud, NFIB, Fraud Act, Bribery Act – had never happened.

The task force is to be welcomed (in spite of what seems to be its narrow focus on banking) as long as the sustained and close engagement of the home secretary is also part of the plan.

But we are concerned that this is less a new vision and commitment, more another process for reinventing the wheel. The key priorities – intelligence gaps and systemic vulnerabilities; fast-track intelligence sharing; better ways to identify victims and targets; raising general awareness and self-defence –

are strikingly similar to those of the NFA's *Fighting Fraud Together*. And, when joint working and intelligence sharing between the banks and the authorities have been on the agenda for many years, it is not unreasonable to ask why it has taken so long to get only this far? Or to wonder when we will begin to see results?

We also question the government's characterisation of the banks as fraud-fighters *par excellence*. Public confidence matters immensely in tackling fraud. Many SMEs and members of the public do not see their banks as entirely dependable partners in this fight. Victims want banks to do more to identify and prevent fraud, to weed out more fraudsters sooner with better 'know-your-customer' safeguards, and to be more cooperative when a fraud is discovered. So we urge government to make sure that these things too are on the agenda of the taskforce.

'When the S-word was dropped from NFSA that was symptomatic of a step away from its proper role. It is very disappointing how the national fraud strategy seems to have just disappeared without trace.'

Sandra Quinn, NFSA interim and founding chief executive (2007-09)

Public education

Even the Fraud Review fell into the trap of thinking that fraud 'should be one of the easiest crimes to prevent' because 'elementary caution and healthy scepticism' would save most people. Metropolitan Police commissioner Sir Bernard Hogan-Howe has now suggested that banks should stop compensating customers for online credit-card fraud because they are being 'rewarded for bad behaviour'.

Attitudes like this gravely underplay the sheer guile and cunning of the fraudster, not to mention the true, baffling complexity of much everyday technology and finance. Before we start to demand more by way of self-defence from internet users we need a well-funded, broadly-based and sustained public education programme to:

- ◆ raise awareness of the warning signs of deception (many are not so obvious when it's you who is caught in the cross-hairs of the con); and
- ◆ soften attitudes to fraud victims so that more are prepared to come forward to share their experiences (we all benefit from the extra intelligence) and get the broad support they often need.

Such a campaign should draw on the best creative talent and it should extend far beyond the temptingly low-cost realm of websites and social media, to include TV, radio, newspapers and posters. Many of the most vulnerable groups in society are not part of the YouTube generation.

Only once this has been done, and done properly, will it be realistic and fair to expect more from everyone.

'It should be in our culture to report criminal matters to the authorities for the greater good; recognising that not every fraud will be investigated, and that the police are not a money recovery service, but that the more we can see of the threat, the better we can design what we do to prevent it.'

Commander Chris Greany, national coordinator for economic crime, City of London Police

Measuring and reporting

The Fraud Review pulled no punches: the criminal justice community had no clear and realistic picture of the true size and shape of the fraud threat. Even the Crime Survey of England and Wales (CSEW) did not include fraud in any systematic way.

The new NFSA created a dedicated unit to make regular estimates of the total cost of fraud using a stable and robust methodology. A new National Fraud Reporting Centre (NFRC) would make fraud reporting quick and efficient everywhere.

- ◆ The measurement unit became the annual fraud indicator, which completed four exercises before being closed down in March 2014. Its final report estimated total fraud losses at £52bn (£15.5bn discovered, £36.5bn hidden or unreported).
- ◆ The National Fraud Reporting Centre (soon renamed Action Fraud) opened in October 2009 with control transferred to the City of London Police in 2014. In 2014-15 Action Fraud received almost a million reports of all kinds, including 246,844 formal crime reports from the general public.

THE PROBLEM OF UNDER-REPORTING

In 2015-16 the Crime Survey of England and Wales (CSEW) will, for the first time, include fraud and cybercrime questions. We welcome this as a step in the right direction. A large-scale field trial of the new questions has already estimated 5.1m frauds in 2014-15, along with 2.5m cyber offences.

But the yawning gap between these figures and the 600,000 or so actual crime reports fed into the NFIB over a similar period clearly indicates that under-reporting persists to a very significant degree. National trading standards research shows that 90% of scam victims never report the crime. Government research suggests that reputational and regulatory concerns prevent the reporting of all but a tiny proportion (less than 2%) of corporate cybercrimes.

For many years the Panel has called for official crime statistics to do a much better job of capturing fraud offences. Incomplete statistics leave fraud victims at a disadvantage because they hide the true level of economic crime, resulting in decisions about police and criminal justice resources being made without a proper understanding of the true amount of fraud and who it is hurting. For some years this lopsided picture also created the illusion that crime in the UK was falling when in fact it was changing shape and increasing. When the new CSEW fraud and cybercrime data was added to the old crime total (6.5m) it more than doubled it, to 14.1m offences.

THE BIG PICTURE

We know there is no 'true' figure for the total amount of all fraud, but we can, and should, develop 'sentinel' data that can tell us something useful about what is actually getting worse, getting better or heading for disaster. A five-yearly fraud 'census' would provide just such a broad indication of scale and direction, but at much lower cost than the old annual fraud indicator. No statistical free-for-all will ever create something like this for us. What's needed is a formal, consistent, sustained measurement effort, performed or supervised by government.

‘We should never be happy with a static picture of fraud. What we should be focused on is what’s changing and the vectors of change.’

Dr Michael Levi, professor of criminology, Cardiff University



Tackling cybercrime – changing behaviour

Online fraud simply wasn't on the Fraud Review's radar 10 years ago. Today the internet has industrialised the way crimes of deception are committed and the radar screen is crowded.

Cybercrime has become a national security threat. Our challenge is to redesign our digital world with security in mind. That's going to take everything we've got because the vulnerabilities are quite literally everywhere.

- ◆ Eager, excitable young minds can be easily drawn into hacking and cybercrime while their parents watch TV.
- ◆ Older internet users are too trusting for the new, digital Wild West.
- ◆ As any hacker will tell you, new software is shipped as soon as possible, with security vulnerabilities 'patched' later (if at all).
- ◆ Consumer technology development models strongly favour functionality over security because so do many consumers.
- ◆ The so-called 'internet of things' – connecting cars and household devices to the global network – will turn software hacks into physical threats.

'People need robust, independent advice about which products are worth having, and which aren't. Could we end up with the mis-selling of cybercrime advice? I think so.'

Dr Michael Levi, professor of criminology, Cardiff University

◆ We take it for granted that internet service providers treat spam and malicious traffic as seriously as possible. But do they?

◆ When companies are reluctant to admit they've been hacked they increase the risks for everyone.

As this short, speculative list shows, building cyber resilience is as much about changing behaviour and culture as it is about strengthening skills. But we have made a start.

- ◆ The government's *Cyberstreetwise* scheme is encouraging better individual online security behaviour.
- ◆ The *Cyber Essentials* certification scheme is trying to spread basic, minimum cyber security controls among SMEs.
- ◆ The new national cyber security plan will also include stronger national infrastructure regulation and more training, mentoring and career opportunities to keep young talent on the straight and narrow.

'The boom in computer-enabled crime is requiring complete cultural change in how we approach policing. But this is a challenge for all of society because the risks are different.'

Commander Chris Greany, national coordinator for economic crime, City of London Police

Policing The Fraud Review echoed the long-standing concerns of the Panel when it found that police resources for fraud investigations were small, declining and often diverted to other tasks.

Fraud was not a priority under the National Policing Plan and a victim's experience of reporting fraud to a police force was seldom a positive one, with little hope of an investigation being launched.

The new policing and reporting infrastructure envisaged by the Fraud Review was created and has mostly survived: the City of London Police is the national lead force with responsibility for supporting local forces and running the National Fraud Intelligence Bureau (NFIB); Action Fraud is now the UK's national fraud and cybercrime reporting centre.

For all the good work of the City of London Police (both as lead force and local force) and the Metropolitan Police online crime and fraud unit, FALCON, the picture remains very different beyond London. The NFIB pushes useful and usable fraud crime information to local forces, but no-one – not the NFIB, not the lead force, not the Home Office – seems able to persuade local forces to use it properly.

Many of us continue to hear of victims prevented from making an urgent report in person, struggling to make the crime fit the Action Fraud website and then receiving little or no meaningful follow-up from officers. Several Panel members, experienced fraud professionals themselves, have had precisely these experiences in recent times.

BAD PRACTICE?

In preparing its recent report *Real lives, real crimes – A study of digital crime and policing* (December 2015) Her Majesty's Inspectorate of Constabulary (HMIC) visited six forces. The inspectors found a depressingly familiar picture of disengaged and ineffectual local fraud policing.

- ◆ A lack of an effective local response to fraud.
- ◆ Too many victims directed to Action Fraud when local officers could have done something quickly to remedy the situation.

- ◆ Very few officers and staff who understand their fraud roles and responsibilities.
- ◆ Continued signs that online fraud doesn't concern police as much as physical crimes like burglary.
- ◆ Insufficient understanding of correct procedures among officers who come into contact with victims.
- ◆ Poor advice and support for fraud victims and little evidence of effective care.
- ◆ Fewer than half of forces regularly including fraud in their strategic risk assessments.

Even the national police coordinator for economic crime has trouble getting a response. In March 2015 he wrote to every chief constable highlighting best practice and asking for a chief officer to be made responsible for implementation. Six months later, the report tells us, 'he had received only 14 responses out of a possible 43.'

The existence of Action Fraud does not change proper police practice when faced with someone in immediate difficulty: the victim should receive a prompt response from their local police, not least because rapid police action might prevent further victimisation or financial loss. They should not be fobbed off and referred to Action Fraud. But the HMIC inspectors found only 'isolated' examples of correct practice alongside a widespread belief that all fraud was now Action Fraud's problem.

Rather than invigorating local fraud policing, Action Fraud seems to be used by local forces to offload fraud victims and hide their own continuing lack of interest in tackling these crimes.

That these problems persist, a decade after the Fraud Review, is deeply dispiriting.



‘Action Fraud 2’

Soon the new Action Fraud system will be launched. It promises better usability and functionality for victims and more efficient, automated information flows from the NFIB to local forces. A web-based interface will be easier for officers to use and make it easier for the NFIB to monitor that use. While these upgrades are to be welcomed, will they make any difference to the many woeful experiences of fraud victims documented by the HMIC report? We certainly hope so.

Protecting the public purse

The Fraud Review rightly called for more vigilance, measurement and risk assessment in public bodies. Yet the National Audit Office has found a continuing lack of good public sector fraud data, with fraud still given a low priority by staff with uneven skills. The government’s own fraud data suggest massive under-reporting; in 2014-15 the figure for detected fraud was 0.02%, against 3-5% in the US and EU.

The Cabinet Office has now begun to create a counter-fraud framework and minimum standards for the public sector – a project to which we are pleased to contribute. Government has an obligation to protect all aspects of the public purse. It also has a duty to lead by example in improving information sharing, building capabilities and demonstrating good practice. The Cabinet Office project is an opportunity to do all of that, and then to share the fruits as widely as possible with the rest of society.

Since 1988 the **Serious Fraud Office** has played a pivotal role in the investigation and prosecution of serious and complex fraud. The Panel was privileged to bring together four of the five most recent directors – George Staple, Ros Wright, Robert Wardle and current director David Green – and to listen as they discussed the past, present and future work of the SFO.

SFO focus

Tackling serious and complex fraud and corruption



CONTINUED RELEVANCE

Green: There are three very good reasons why the SFO should stay. Roskill – there’s no evidence that breaking up the Roskill model would achieve better results – quite the opposite. Independence – we need to be visibly and demonstrably separate from central government influence if we are to investigate the sort of cases we were set up to investigate. Priority – if you make us part of an organisation with multiple priorities, fraud will always be the area that loses out. I think that case is pretty unassailable.

Staple: The other thing is the SFO as a centre of excellence. That was a Roskill objective too. The name itself tells you that this place is something special.

MEDIA AND PUBLIC UNDERSTANDING

Staple: There’s always been a bit of a fog in the public mind – and probably not only the public – about the knowledge and information we possess when these big independent decisions are taken. We live in an age of distrust, but the SFO is set up in such a way that it can be trusted to take them dispassionately.

Green: You make these decisions based on really classy legal advice and the views of a very clever case team. Our job is to put the strongest case we can before a jury. After that, it’s over to them.

Wright: But you can’t explain that. You can’t go to the papers and say, ‘the best legal advice says that ...’

Wardle: I don’t think anyone expects the sheer heat of the spotlight, however much media training they’ve had. The decision to start, or stop, one of these investigations is very complicated and the media aren’t interested in the detail.

Green: You do have to engage though. When Tom Hayes was found guilty I was criticised – including on Radio 4 – for not celebrating enough! Then, when the Libor brokers were acquitted, it was ‘this was a failed case’. And when we dropped the Forex case the response was, ‘this is a crazy decision, how can this be right?’ The media has an over-appreciation of the American model: the ‘perp walk’, the prosecutor’s speech on the court steps, the orange jumpsuit and the massive sentence. I don’t think any of us wants that!

Wright: We had a press officer who actively explained cases to the press and introduced them to the case controllers, so they could get an informed view. But I don’t think you need to explain the outcomes. Trial results are up and down because there are so many variables.

Green: It is complicated: the conviction rate might be low over 12 months but much better over four years or the percentage of cases won can be high, but not so good for defendants convicted.

Wardle: Like the Izodia case – main defendant sees our case and pleads guilty; the second is far too ill to stand trial; so there’s no public interest in the expense of trying number three. It was a very successful prosecution – but only a 33% success rate.

LAW REFORM

Wright: The Fraud Act is a vast improvement. It’s all based on dishonesty now; you look at the circumstances and if there is concealment it doesn’t matter what the victim felt. In the old days you needed a witness who’d say, ‘yes, I was actually deceived, and by X’.

Staple: And the Bribery Act, which has actually defined ‘corruption’. Before, it was what a jury might think was corruption. The section seven offence [failure to prevent] – that’s new for companies and very important.



Green: I've also been lobbying for a wider section seven offence of corporate failure to prevent an economic crime. It's a public confidence thing; the man in the street wants to know how the Americans are so much more effective against companies. Deferred Prosecution Agreements are very useful; a company can now account for criminality without facing the wider consequences of a conviction. But they must self-report and cooperate or we can't convince a judge it's in the interests of justice.

Wardle: I still favour judge-only trials for corporates; no-one is going to lose their liberty, it's part of the regulatory process. To individuals, I would give the option of jury or judge.

Staple: It's just not reasonable to expect jurors to sit for all that time, remember everything said from day one, and then weigh it all up months later. It's too difficult.

Wardle: Unfortunately, there's no appetite for change now.

Wright: It's also disappointing that there's been no progress on the disclosure rules. The CPIA regime is wholly unsuited to big fraud cases, with the prosecution having to 'guess' what unused material might help the defence. And judges lean over backwards to be terribly fair.

Staple: Unless you get a proper defence statement – one they are obliged to stick to – you are never going to contain the problems with disclosure. The English trial is everything; for the defence it's no-holds-barred. It is unfair in one way – to the public and the prosecution – but it will take heaven and earth to change.

ATTRACTING STAFF

Wright: The SFO is like a huge family; I knew every single person by name. Of course, it has doubled in size since I was there. We had City solicitors who were willing to sacrifice a partnership to come to the SFO.

Green: It's the quality of the work that is so attractive; there's intense interest and admiration for it. We offer secondments to City solicitors now. The pay is a fraction of what they are used to but one in four decides they'll stay. I've started with the accountants and insolvency practitioners as well.

Staple: When I returned to private practice I was very aware that people had a great interest in the SFO, particularly the youngsters, who very much admired the work.

FUTURE ROLE

Green: The anti-corruption part of our work will grow and grow, and is now about 50%. But there are vast amounts of suspect foreign money we can't touch and to do so will require the UK as a whole to be more on the ball. We look at corporate corruption overseas, but there's a need for more effort to be put into looking at corruption of individuals as well as what sort of corruption problems we have domestically in the UK.

Wright: It's not that corruption is something new. It's that the Anti-Terrorism, Crime and Security Act 2001 and, more importantly, the Bribery Act 2010 now enables British justice to deal with corruption overseas.

Staple: It's important to remember that the SFO is a creature of the economic cycle. First you have a freewheeling period of prosperity, then the recession strikes – as it does – and the difficult cases come crawling out of the woodwork.

Green: My objective is to leave the SFO properly resourced and politically safe, with a continued ability to expand at short notice, which is important for that very reason.



Prosecuting and punishing At the time of the Fraud Review relatively few fraudsters found themselves in court. Those who did were often accused of Theft Act offences. Fraud trials had become embarrassingly slow, costly and unpredictable.

Maximum sentences for deception ranged from 5 years to 10, but actual custodial sentences were uncommon and short: only 1 in 12 convicted fraudsters went to jail and the average sentence was about six months. The Fraud Review could see that such short sentences had no significant deterrent effect and were an insult to victims.

Nor did the system deliver much by way of victim redress. Many near-identical victims missed out on compensation because those crimes had been severed to make the case manageable. Confiscation proceedings were complicated and rare, with recoveries averaging just 10% of losses.

THE FRAUD ACT

The Fraud Act 2006 introduced the first English statutory offence of fraud. Fraud prosecutions increased and convictions trebled from 2,501 (2007) to almost 8,000 (2011). Sentences of immediate custody increased from 5% (2002) to 18% (2011). Average custodial sentences more than doubled to about 12 months, and in SFO cases they increased from 30 months (2010-11) to 72 months (2012-13).

LOGICAL SENTENCES

The current maximum sentence for theft of any amount is seven years; under the Fraud Act it is 10 years; for handling stolen goods it is 14 years. The Fraud Review wanted consideration given to a 14-year maximum. Today, with sums at risk from a single internet-enabled act of dishonesty snowballing into hundreds of millions of pounds, it is time for maximum tariffs for all types of serious dishonesty to be standardised at 14 years.

VICTIMS AND WITNESSES

Fraudsters are typically expected to serve additional time in jail if they fail to pay a financial penalty. Unenforced penalties harm victims' hopes of recompense, disadvantage the public finances and encourage others to default. But tough action by the courts to enforce fines and compensation orders is becoming rarer. More needs to be done to stiffen enforcement.

The criminal justice system also needs to pay much more attention to how it treats witnesses and victims. The public accounts committee recently warned that the system is 'close to breaking point' and 'failing victims and witnesses'. Witnesses and victims carry the heaviest loads; from the worry, inconvenience and stress of long-delayed proceedings, to the strain of unnecessarily aggressive cross-examinations. They deserve a better deal and a better experience.

CORPORATE OFFENDERS

Piecemeal approaches to fraud fighting throw up anomalies and inconsistencies that help the criminals and harm the rest of us. One such area in economic crime is corporate offences of 'failure to prevent'.

Section seven of the Bribery Act 2010 created the first such offence, making a company criminally liable if it had inadequate procedures for preventing staff from committing bribery.

Without corporate failure-to-prevent offences prosecutors must prove the guilt of a person so senior that he or she can be said to embody 'the company'. It is this requirement – the so-called 'controlling mind' problem – that makes it so much harder to prosecute corporate crime here than in the US.

We are encouraged by the government's plans to introduce a similar corporate criminal offence of failing to prevent tax evasion. But if bribery and tax evasion, then why not money laundering and fraud as well?

It was disappointing to see something that was reported as a prime ministerial commitment to create corporate failure-to-prevent offences for fraud and money laundering turn out, on closer inspection, to be a commitment to consult rather than to act.

Extending failure-to-prevent offences to all economic crimes is one of the great anti-fraud challenges of the day and we urge the government to press on with the job.

SHORTER, BETTER-MANAGED TRIALS

In an attempt to produce shorter, better-managed trials with more consistent outcomes the Fraud Review made two key proposals: more expert fraud judges who would also be better-trained in case management; and an English plea bargain system.

The Fraud Advisory Panel welcomed both proposals but felt that the true root of the problem – the damaging effect of the Criminal Procedure and Investigation Act 1996 (CPIA) and the code of practice it created – had not been confronted. Ten years on it still hasn't.

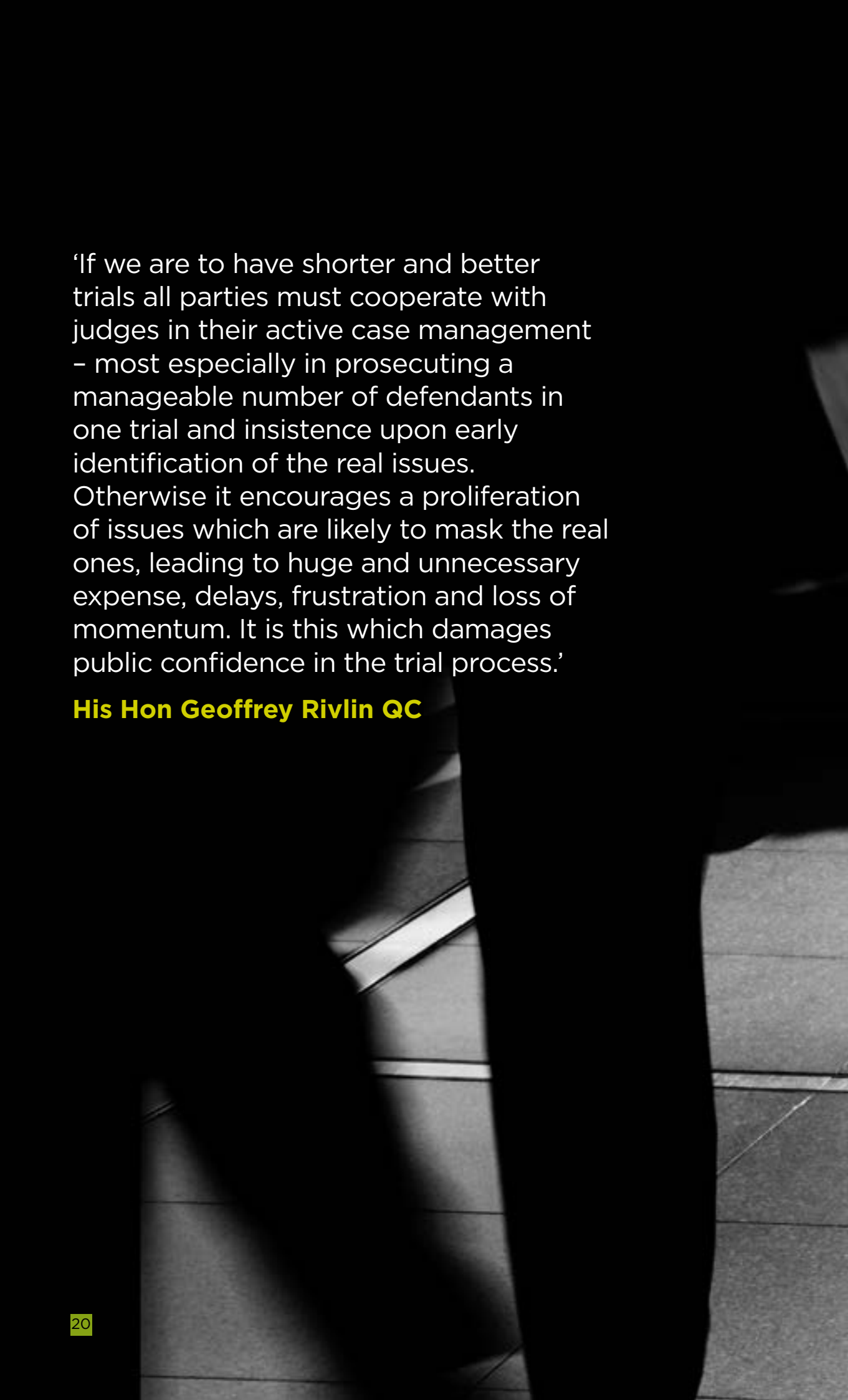
The process of investigation is crucial to the conduct of a prosecution, and the CPIA code damages both.

- ◆ It requires investigators to pursue 'all reasonable lines of enquiry' whether or not they establish guilt ...
- ◆ ... which compels them to widen their investigation far beyond what is needed to make a case ...
- ◆ ... which results in the seizure of extremely large volumes of material, much of which will never be used but must still be carefully disclosed to the defence.

Today this problem is even worse. In a modern serious and complex fraud case, perhaps involving the activities of a large organisation over several years, the unused evidence can run to millions of individual items. The prosecution resources devoted to investigating the facts are frequently dwarfed by the effort needed to sift, analyse and catalogue a mountain of unused material.

Disclosure also creates many opportunities for the defence to delay the trial, or even to derail it completely. In serious and complex fraud cases, abuse of process applications by the defence have now become commonplace.

The disclosure process is so complicated, burdensome and stressful for prosecutors that the risk of a mistake is increased. An accidental failure can be grounds for a conviction to be quashed even when the defendant has pleaded guilty.



‘If we are to have shorter and better trials all parties must cooperate with judges in their active case management – most especially in prosecuting a manageable number of defendants in one trial and insistence upon early identification of the real issues. Otherwise it encourages a proliferation of issues which are likely to mask the real ones, leading to huge and unnecessary expense, delays, frustration and loss of momentum. It is this which damages public confidence in the trial process.’

His Hon Geoffrey Rivlin QC