

FRAUD
ADVISORY
PANEL
THE YEAR
IN REVIEW
2012/13



The Fraud Advisory Panel is the independent voice of the UK's anti-fraud community. With members drawn from the public, private and voluntary sectors, no other organisation has such a range and depth of knowledge, both of the problems and of the solutions.

We use our truly multidisciplinary perspective to raise awareness of the immense damage fraud does to individual lives, the national economy and society at large and to encourage everyone, in every walk of life, to play their part in reducing it.

We do this by:

ADVISING...

GOVERNMENT, BUSINESS AND THE GENERAL PUBLIC ON FRAUD PREVENTION, DETECTION AND REPORTING.

EDUCATING...

BUSINESS, THE PROFESSIONS AND THE GENERAL PUBLIC.

INFLUENCING...

REFORM OF THE LAW AND PUBLIC POLICY ON FRAUD.

RESEARCHING...

THE EXTENT, CAUSES AND NATURE OF FRAUD.

CONTENTS

04 CHAIRMAN'S OVERVIEW

05 THE YEAR IN REVIEW

- 05 UK to opt out of EU third pillar arrangements?
- 05 New direction for the SFO
- 05 Creation of a national crime agency
- 06 Reporting fraud to law enforcement agencies
- 06 Cuts in police numbers

07 OUR KEY ACHIEVEMENTS 2012

- 07 Advising and informing
- 07 Educating and training
- 07 [Abuse of incorporation used to commit fraud](#)
- 08 Representing and influencing
- 08 Researching and supporting
- 09 [Helping victims to obtain redress](#)

10 CYBERCRIME

12 *PLUS ÇA CHANGE ... IS THERE ANYTHING NEW IN FRAUD?*

14 CROWD ENGAGEMENT COULD HELP SMALL GROUPS FIGHT FRAUD FOR THEMSELVES IN THE YEARS AHEAD

16 ABOUT THE PANEL

- 17 Board of trustees
- 18 Staff and consultants

19 CORPORATE MEMBERS

20 GETTING INVOLVED

- 20 Corporate members

21 THANK YOU

THE CHAIRMAN'S OVERVIEW

WE ARE IN THE DEPTHS OF THE MOST SERIOUS ECONOMIC DOWNTURN ANY OF US HAS EVER EXPERIENCED.

At a time when the national deficit is at an all-time high and our national credit rating has been downgraded, we can ill afford to lose more money to fraud as well. Yet that is exactly what is happening. Meanwhile, the prospects of recovering that money from fraudsters – as we have demonstrated in some of our work over the past year – seem increasingly remote.

Fraud thrives in a recession. But as the economic crisis empowers the fraudster, it does the opposite to the criminal justice system. Spending cuts that eat into law enforcement manpower and services render increasingly remote the prospects of catching fraudsters and recovering losses.

Her Majesty's Inspector of Constabulary, Tom Winsor, has urged police to do more to prevent crime. But as things stand, if society is to have a decent chance of tackling fraud effectively, we must all do much more for ourselves by trying to prevent fraud happening in the first place. To tackle economic crime successfully we all need to know what types of fraud are prevalent and which of them threaten us most. We need to recognise and quantify frauds and prepare for them. But do we?

As far as financial crime is concerned, most of us – particularly those who own or manage a business – could do much more to protect ourselves. It is one of fraud-fighting's more dispiriting facts that, on the whole, business people are complacent about fraud threats. They don't look at fraud as a business risk like any other, so they cannot manage it as efficiently.

Fraud prevention is a central issue for the Panel and it is the focus of much of its work. We can avoid becoming the victims of fraud; we can frustrate the fraudsters. But it takes effort. In particular it takes an increased awareness of the risks, allied to the will and determination to do something about mitigating them.

Of course, even the well organised, diligent and alert can still fall prey. And fraud victims quickly find out how hard it is to recover losses. It is for this reason that we recently turned our attention to investigating ways in which legal outcomes for fraud victims might be improved. We began by conducting research into ways in which fraud victims might be helped to experience more success and less frustration through civil and criminal processes. Our full findings and recommendations were published recently and are available online. We will be developing our ideas further over the coming months.

Elsewhere in this annual review, three expert members of the Panel's board look at burgeoning threats – from cybercrime and investment fraud – and, more controversially, what victims might do for themselves to help prevent the already thread-like 'thin blue line' from breaking under the strain. My thanks go to Dr Stephen Hill, Will Kenyon and David Clarke for these timely and thought-provoking contributions.

My thanks also go to our many volunteers. It is their tireless commitment and dedication that enables us to achieve so much more than our modest financial resources would seem to promise. I would like to thank most sincerely everyone, including our trustees, who has worked so hard this last year. But in particular I would like to say how much we appreciate the hard work and dedication of our staff members, Mia and Oliver.

Rosalind Wright CB QC
July 2013

THE YEAR IN REVIEW

FIVE YEARS OF ECONOMIC STAGNATION HAVE ALREADY DAMAGED OUR NATIONAL FRAUD-FIGHTING CAPABILITY, WITH LITTLE OR NO EVIDENCE OF RECOVERY IN SIGHT. FORTUNATELY, NEW LEADERS AT ECONOMIC CRIME AGENCIES OLD AND NEW PROVIDE SOME CAUSE FOR HOPE. MEANWHILE EURO SCEPTICISM STALKS THE CORRIDORS OF WESTMINSTER AND THREATENS TO MAKE CROSS-BORDER FRAUD-FIGHTING ONE OF ITS EARLY VICTIMS.

UK TO OPT OUT OF EU THIRD PILLAR ARRANGEMENTS?

The government is deciding whether the UK should opt out of some 130 EU police and criminal justice measures created prior to the Treaty of Lisbon. Their loss could seriously harm UK law enforcement and impede cross-border fraud fighting. Measures under threat include schemes for sharing information and expertise in particular areas of cross-border crime as well as the UK's membership of Europol and Eurojust (along with any influence we might have over their work). Among the most significant losses would be: the European Arrest Warrant, which has greatly streamlined the extradition process between member states; instruments under which member states can enforce each other's confiscation orders; and our participation in the Schengen Information System (SIS), which enables police officers to quickly establish whether an arrested person is known to law enforcement in another member state.

NEW DIRECTION FOR THE SFO

The Serious Fraud Office (SFO) has had a chequered history, particularly of late. Now it is sailing into somewhat calmer and more traditional waters but sorely under-resourced and with its budget slashed. New SFO Director David Green CB QC, an experienced and 'old school' prosecutor, has already rejected the 'soft-touch' approach of his predecessor and has vowed

to crack down hard on fraud, money laundering, and bribery and corruption. There will be no more handy hints for fraudsters regarding which crimes the SFO will or will not prosecute.

Unfortunately the constant rumours about plans to abolish the SFO have not been silenced by the arrival of a proactive new director. These serve only to deter first-class investigators and prosecutors from joining the office and to reassure the criminals, perhaps even to embolden them. A secure future for the SFO should be confirmed by government once and for all.

CREATION OF A NATIONAL CRIME AGENCY

The Economic Crime Command (ECC), an important arm of the new National Crime Agency (NCA), will start work officially in October. Its new leader is Jeremy Outen, a forensic accountant from KPMG who was, until his appointment, an incoming member of our management board. The ECC's range is very different from SOCA's. Its national capability reflects the divergent needs of different police areas. It comprises three subgroups – operations, prevention and intelligence – and intends to use its stakeholder groups to maintain a close involvement with the private sector, particularly the banking, insurance and wider financial services industries. ►

REPORTING FRAUD TO LAW ENFORCEMENT AGENCIES

Action Fraud provides a central reporting point for all types of fraud. This year has seen the service rolled out across the country, with 90 people now staffing the phones in Edinburgh and Manchester, supported by a web-based tool for fraud reporting online. Reporting volumes have increased by 40% as a result, but the effectiveness of the service is already being questioned. Action Fraud still cannot deal with bulk fraud reports, discouraging large organisations like banks and insurance companies from reporting some of the biggest crimes.

Given that so much fraud is still very largely unreported, the delayed introduction of bulk reporting by Action Fraud is very disappointing. The more that is done to encourage individuals and businesses to report fraud, the greater the prospect of creating a comprehensive picture of national and local fraud threats that can then inform a police resourcing strategy capable of meeting real needs.

CUTS IN POLICE NUMBERS

The reduction in police budgets under this government has led to fewer police officers, with the number of fraud investigators having fallen by 25% in the last few years. Positive developments in 2012/13 have included the establishment of fraud intelligence units in 10 UK regions. But the future of this resource is uncertain because of an ongoing Home Office review of organised crime policing. The review also has implications for the creation of regional fraud teams – a concept the Panel has strongly supported. About 10 fraud intelligence units were to be based in key areas across the country; each with 10 or so police officers, specially trained and experienced in fraud, supporting and working with local forces. Whatever the ultimate shape of future policing structures, the threat from fraud remains at least as serious as that posed by other forms of organised crime.

The City of London Police is one of the few forces adequately resourced to tackle the fraud on its own patch, the Square Mile. But under its remit, as the lead force for fraud nationally, it also has responsibility for assisting police forces countrywide with their major fraud investigations.

Outside London, the local allocation of policing resources is now in the hands of newly elected police and crime commissioners (PCCs). Many of them will not yet fully appreciate the scale of the fraud threat in their areas. We in the counter-fraud community need to be more active in helping PCCs to understand the threat so that resources can be targeted appropriately. With police resources being reduced, it has never seemed more timely to ask: without police officers to investigate, what encouragement is there to report fraud in the first place?

OUR KEY ACHIEVEMENTS 2012

THE COMBINATION OF THE PANEL'S INDEPENDENCE AND THE UNRIVALLED EXPERTISE OF ITS MEMBERSHIP HAS ONCE AGAIN ENABLED US TO MAKE AN EXCEPTIONAL CONTRIBUTION TO DEVELOPMENTS IN FRAUD-FIGHTING POLICY AND PRACTICE.

ADVISING AND INFORMING

Having brought the problem of fraud against charities to prominence in 2009, we led development of new UK-wide guidance for the general public in 2012. *Giving Safely: a guide to making sure your donations really count* addresses the pitfalls of charitable giving wherever it takes place: on the doorstep, on the street or online. Artwork for this guide, in leaflet and poster form, is freely available online. We also provided expert input to the Charity Finance Group's *Charity Fraud: a guide for the trustees and managers of charities*. Both projects were supported by key stakeholders from the public, private and voluntary sectors. In a separate initiative we produced a new fraud factsheet for internal auditors working for charities.

Five new self-help factsheets were published. Aimed at organisations, they cover civil recovery, fraud investigations, supplier and outsourcing fraud, and fraud in Scotland. An existing email and internet scams factsheet for individuals was updated and reissued. To encourage third parties to distribute our factsheets more widely they can add their logo to each one in a 'distributed by' box.

All publications are available free from our website, www.fraudadvisorypanel.org.

EDUCATING AND TRAINING

A number of practical and participative events were run for anti-fraud professionals from all sectors. A series of workshops looked at how to respond to fraud. Briefing ►

Abuse of incorporation used to commit fraud

The UK limited company regime is worryingly vulnerable to fraud, whether by companies set up for the purpose or by those trading fraudulently while hiding behind nominee directors.

One particular concern is the lack of scrutiny of the information submitted to Companies House. It is a criminal offence under s1112 of the Companies Act 2006 to submit false information to the Registrar, but nobody checks the information for accuracy and we believe that no prosecution has ever been brought. The regime is so lax that criminals have taken to simply cutting and pasting legitimate company accounts into their own fake

returns. Use the Companies House website to check a company's bona fides and you can be reassured by what looks like the multimillion pound results of a legitimate company, audited by one of the big four accountancy firms, when in some cases the truth could not be more different.

We convened an expert roundtable on the matter in May 2012 and published an occasional paper, *The Abuse of Company Incorporation to Commit Fraud*, based on its proceedings. Thirteen recommendations for change have been submitted to the Department of Business, Innovation and Skills.

sessions and best practice forums looked at overseas asset recovery, corruption, managing business information and communication during a fraud investigation.

Joint events were convened in collaboration with the Association of Certified Fraud Examiners, the Chartered Institute of Internal Auditors (CIIA), the Institute of Advanced Legal Studies and the North East Fraud Forum.

Two not-for-profit organisations asked us to provide fraud awareness training for their staff. Five courses on *Fraud Risk and the Internal Auditor* were delivered on behalf of the CIIA in Dublin, Lisbon and London.

A total of 13 external speaking engagements included presentations to various professional, trade and commercial organisations as well as a contribution to the Cambridge International Symposium on Economic Crime.

Regional FAP forums are popular gatherings at which members share knowledge, experiences and best practice in fraud prevention, detection, investigation, prosecution and deterrence. In 2012 we convened 15 of them in Birmingham, Bristol, Edinburgh and London.

REPRESENTING AND INFLUENCING

The FAP represents the interests of its members on: the National Fraud Authority's (NFA) working groups on economic crime prevention and insolvency fraud; the Charity Commission's voluntary sector fraud group (formerly the NFA's charity fraud steering committee); and the economic crime portfolio group of the Association of Chief Police Officers.

We contributed expert responses to three government consultations, on deferred prosecution agreements, governance arrangements for economic crime and the NFA's 2013/14 business plan and stakeholder audit. Our chairman's evidence to the EU subcommittee of the House of Lords was incorporated into its report, *The Fight Against Fraud on the EU's Finances*.

We worked to highlight the ways in which the UK's system of company incorporation, with its limited due diligence checks, can easily be abused by criminals intent on fraud. We made 13 recommendations to government on ways to rectify these shortcomings (see box).

RESEARCHING AND SUPPORTING

As part of our project examining ways in which access to civil justice might be made easier for fraud victims we completed a comprehensive review of existing civil routes to legal redress (see box).

Helping victims to obtain redress

As part of the national strategy to reduce fraud, *Fighting Fraud Together*, the Fraud Advisory Panel was asked to undertake a campaign in support of fraud victims who may wish to recover their money by non-criminal means, including action in the civil courts.

UNDERSTANDING THE PROBLEM

The project began with a comprehensive review of the existing literature on the nature, extent and impact of fraud against individuals and smaller businesses in England and Wales. Importantly, we included in our scope the very large amount of fraud that still goes unreported to law enforcement agencies.

Independent new research was then commissioned to examine the nature, availability and quality of the professional advice and support (public and private) available to fraud victims. A series of case studies enabled us to document the particular experiences of smaller businesses in some detail. A pair of stakeholder forums gave professionals from the public and private sectors the opportunity to explore the obstacles to civil justice that confront fraud victims and to consider how they might be reduced. Meetings with organisations that represent fraud victims helped us to complete a comprehensive and compelling study, which reveals a disturbing picture of questionable professional competence, systemic indifference and the frequent thwarting of victims' reasonable expectations of fairness, transparency and justice.

Our research found that the majority of fraud victims seeking to recover their losses have little or no appreciation of the full range of options open to them, which should include not only criminal

prosecution but also civil actions such as insolvency proceedings and suing the fraudster. A victim's first port of call often has a decisive effect on the quality of their subsequent experience of the justice system. Knowledgeable and unbiased support early in the process could and should make a real difference. In reality advice is often patchy and incomplete, particularly for smaller businesses. Victims typically find it difficult to retain a proper 'fraud expert' or even to find the information they need to make a confident start in identifying one. And even though fraud's consequences are frequently shattering for victims, there is a notable lack of sympathy, particularly if you happen to be a smaller business.

These findings are available in a series of free booklets, *Obtaining Redress and Improving Outcomes for the Victims of Fraud*, which can be downloaded at www.fraudadvisorypanel.org.

DEVELOPING SOLUTIONS

In May 2013 we published a summary of the main themes of our civil justice research, linking them to a set of recommendations for improvements in the support available to individual and smaller business victims. In broad brush terms we believe this can be achieved by improving the availability and quality of information and guidance and by raising public and private-sector professionals' awareness of the range and usefulness of civil justice remedies.

CYBERCRIME

TRUSTEE DIRECTOR AND INDEPENDENT E-CRIME EXPERT DR STEPHEN HILL LOOKS AT THE YEAR THAT WAS IN THE FAST-PACED WORLD OF CYBERCRIME AND CONSIDERS TRENDS TO COME.

Across the globe cybercrime is a serious and growing threat to organisations and individuals. In 2012 we saw many new attempts to steal our confidential information, corrupt our phones and PCs and extort money from our bank accounts, often using sophisticated social engineering techniques. Moreover, new technology further enabled criminal gangs to compromise the expanding mobile and social networks, using spyware to harvest confidential passwords and access codes and launching denial-of-service (DOS) attacks to overload and disable networked systems.

Definitions vary, but in its simplest form ‘cybercrime’ typically refers to any criminal activity in which computers or computer networks are the origin, tool, object or locus of the crime. The sheer complexity of the underlying networked technology makes these crimes fiendishly difficult to tackle. Attackers can strike unseen whether their victims are thousands of miles away or just round the corner.

The inherent vulnerability of modern IT systems to remote attack – by freelance ‘hacktivists’, global hacking groups, organised crime or even state-sponsored agencies – hit the headlines repeatedly in 2012. Security firm Mandiant¹ drew attention to China’s state-sponsored cybercrime programme, with its own dedicated military unit (Unit 61398), stealing hundreds of terabytes of data from English-speaking companies. Hacking groups LulzSec and Anonymous were also in the news. LulzSec is responsible for attacks on SOCA, Sony and *The Times* and *Sun* newspapers. In April 2012 three of its members pleaded guilty to attacks on the NHS and News International. A Briton linked to the group, Ryan Cleary, also pleaded guilty to attacks on the CIA and the Pentagon.

At the beginning of 2012 hacking group Anonymous – known for its ‘Operation Payback’ attacks on Visa, MasterCard and PayPal when they withdrew banking services from WikiLeaks – launched something it calls ‘Operation Tyler’. This distributed and decentralised Wikipedia-style structure, said to be impregnable to censorship, has already been used in DOS attacks on a number of organisations including the Vatican.²

The marked upsurge in cybercriminality comes just as news reports put the annual headline cost of cybercrime to the UK economy at £18bn–£27bn³ and the UK’s National Audit Office laments a serious lack of skilled cybercrime fighters in the UK. A perfect storm some might say.

PwC’s most recent *Information Security Breaches Survey*⁴ found that even though ‘significant’ attacks more than doubled in 2012, one in five companies still spends less than 1% of its IT budget on security. More than half of all small organisations do ‘no security training at all’. The survey also found that 82% of large organisations had reported security breaches by their own staff, 47% having lost or leaked confidential information. The rapidly growing significance of mobile computing and social networking in the overall threat landscape provides another hotspot; 75% of large organisations and 61% of small businesses now allow staff to use smartphones and tablets to connect to their corporate systems. The consequences for a company’s IT security profile are obvious.

So, what’s new in 2013? The McAfee ‘white paper’, *2013 Threat Predictions*,⁵ highlights new vulnerabilities arising out of even greater computing mobility and the introduction of HTML 5 and Windows 8. It also warns us to

¹ <http://edition.cnn.com/2013/02/19/business/china-cyber-attack-mandiant>

² <http://www.nytimes.com/2012/02/27/technology/attack-on-vatican-web-site-offers-view-of-hacker-groups-tactics.html?smid=pl-share>

³ <http://www.bbc.co.uk/news/uk-politics-21414831>

⁴ <http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml>

⁵ <http://www.mcafee.com/uk/resources/reports/rp-threat-predictions-2013.pdf>



expect more hacktivism as well as increased use of botnets, spam and malware. The ‘citadel rain’ trojan (which enables thieves to launch one-off online attacks on individual bank accounts) is a particular concern.

Although only time will tell if the bite of these ominous predictions are a match for their bark, the message is clear nonetheless: all organisations should prepare themselves for new and emerging risks while remaining

vigilant to established threats. Even simple precautions can help to prevent a cybercriminal from taking advantage of your systems. As a minimum, operating systems and critical applications – that means web browsers, antivirus software and firewalls, to name just a few – should be kept patched and up to date. But that really should be just the beginning of any modern cybersecurity programme worthy of the name.

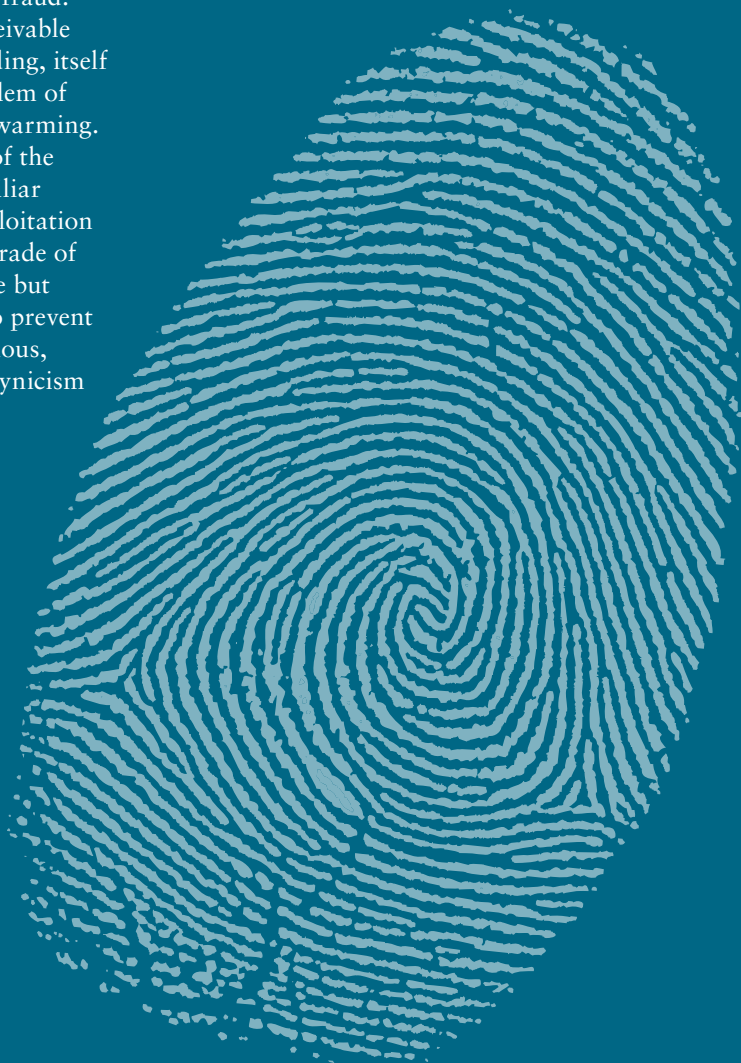
PLUS ÇA CHANGE... IS THERE ANYTHING NEW IN FRAUD?

FORENSIC ACCOUNTANT WILL KENYON ASKS WHETHER ANTI-FRAUD PROFESSIONALS CAN EXPECT TO SEE NEW FORMS OF FINANCIAL AND INVESTMENT FRAUD IN 2013, OR WILL THERE JUST BE VARIATIONS ON OLD THEMES.

In 2010 it emerged that 'spent' and worthless carbon emission reduction certificates (CERs) had been 'recycled' and resold to unwitting buyers in the European carbon offset markets. The fraud took advantage of the absence of a single, common registry of allowances and credits, which would otherwise have picked up the duplications. The CER registration regulations have since been amended.

At first blush this is a very modern fraud. The specifics would have been inconceivable before the introduction of carbon trading, itself a recent response to the pressing problem of greenhouse gas emissions and global warming. But analyse the underlying structure of the scam and you soon recognise the familiar DNA of many much older frauds: exploitation and abuse of an open market for the trade of a commercial necessity with a variable but definable price; inadequate controls to prevent that abuse; unwitting, perhaps incautious, buyers; not to mention breathtaking cynicism on the part of the fraudsters.

What we see here is not a completely new kind of fraud but an opportunity for fraudsters to apply an established criminal mindset to new subject matter. As a coda to the story, 2013 has seen the media reporting that a recession-induced glut of unwanted carbon emissions permits has depressed their value by more than 90% from a 2008 peak. And sure enough, fraudulent trading in CERs is no longer all the rage either. Once the easy money dries up, the great fraud caravan moves on.



The new Financial Conduct Authority does still warn of carbon credit fraud, but it also highlights the emergence of other types:

- Landbanking scams induce investors to purchase parcels of land on the false promise of significantly higher values once planning permission or re-zoning has been secured.
- Rare earth metal scams promise high returns by investing in the raw materials used in the manufacture of electronic devices. Rare in name only (though admittedly difficult to extract), these abundant elements are generally thought a poor investment for retail investors. Not surprisingly, most of the firms offering these schemes are unregulated.
- Overseas land, tree and crop scams offer supposedly lucrative investment opportunities on the premise that because they do not form part of a collective investment scheme (CIS) they are unregulated. In fact the qualifying conditions for a non-CIS include day-to-day management of the asset. An unrealistic prospect for most investors.

The common themes are clear. Fraudsters are both opportunistic and enterprising. They go for the easy kill, where it's available, but they can also be creative and innovative, identifying new targets and vulnerabilities and adopting new tools and techniques. Fundamentally, fraudsters follow the money and we (legitimate businesses, consumers, legislators, law enforcement and regulators) are locked in an arms race against them.

Changes in the *modus operandi* both of fraudsters and anyone trying to combat their predations are driven by changes in technology, business practices and the way we live. As we rely increasingly on mobile technology and the internet, so the virtual world has become a battle ground; its technologies the weaponry of perpetration and prevention. In our networked, digitised world the fraudster's golden ticket is the victim's identity and personal information. As CIFAS tells us in its 2013 *Fraudscape* survey, 65% of all frauds reported to it were identity

theft and facility/account takeover. More than 80% of all identity-related crime is committed (or attempted) using the internet.

As we seize upon the opportunity and convenience offered by technology, so we must be mindful of the ways in which it exposes us to unexpected exploitation and unforeseen consequences. The anonymity of the internet, the low-cost access to the whole world and its expanding role as a marketplace all favour the would-be fraudster. Recent stories about the hacking of accounts holding the virtual currency Bitcoin remind us that all innovations designed to facilitate internet commerce and harness the power of technology – even those designed to subvert the established order – will themselves be subverted before long. There will never be a shortage of fraudsters with the know-how and motivation to exploit weakness, wherever they find it.

But nor should such novelties blind us to the more traditional and/or low-tech threats. The recent spate of frauds involving bogus changes to employee payroll systems and supplier bank account details; the persistence of 419 letters, lottery scams and similarly crude but (sadly) effective email inducements; the more-established boiler room operations selling worthless stocks and shares; credit card fraud; insurance claims fraud; procurement and tendering fraud; all these old foes and more besides continue to cost businesses and consumers dear.

As the business environment changes and new safeguards are put in place, so the bacillus of fraud evolves. There is no way to eradicate it and no foolproof inoculation against it. Only constant vigilance, up-to-date defences and resort to all the necessary precautions will help to contain the disease.

CROWD ENGAGEMENT COULD HELP SMALL GROUPS FIGHT FRAUD FOR THEMSELVES IN THE YEARS AHEAD

AS THE 'THIN BLUE LINE' BECOMES EVER THINNER, DAVID CLARKE, A FORMER CITY OF LONDON POLICE DETECTIVE CHIEF SUPERINTENDENT, ASKS IF 'CROWDFUNDING' BY FRAUD VICTIMS MIGHT OFFER HOPE FOR THE FUTURE OF FRAUD INVESTIGATION.

Police numbers are waning as the demands made upon them continue to grow. Might we yet see a change of heart at the top, with more police resources devoted to the war on fraud? I doubt it, because many in Westminster and beyond already believe that the war is unwinnable.

It's a gloomy notion. No comfort at all to the millions of people in the UK who lost some £6.1bn in 2012 or to the police officers who will never be given the opportunity to investigate the vast bulk of those cases.

The next decade will undoubtedly see UK citizens calling loudly for government to do more to protect them from fraud. They will want more investigations, more help in recovering their losses, and more data (such as the criminals' own details) to be shared more widely with the public. But, even as fraud levels rise, the need to rebalance the economy will surely make it impossible for the government to meet these expectations, leaving individuals increasingly frustrated and exposed to this growing threat. Individuals, just like larger businesses, fall victim to crimes that cover the whole spectrum of fraud – from the downright crude and ridiculous to the highly sophisticated and plausible. Organisations rarely fall for the former (and don't report it even when they do), but individuals seem capable of falling for almost anything. Losses as a proportion of a victim's total assets, especially among the elderly and the poor, may already be staggering, but fraudsters are looking forward to bumper harvests in the decade ahead. Why?

First, Britain is ageing and the elderly, many of them vulnerable and inexperienced investors, are particularly susceptible. The latest figures project an extra 5.5m elderly people in the UK 20 years hence. Second, the explosion of online data and social media usage provides fraudsters with a steady stream of new channels through which to attack victims, making it almost impossible for a novice user to perform

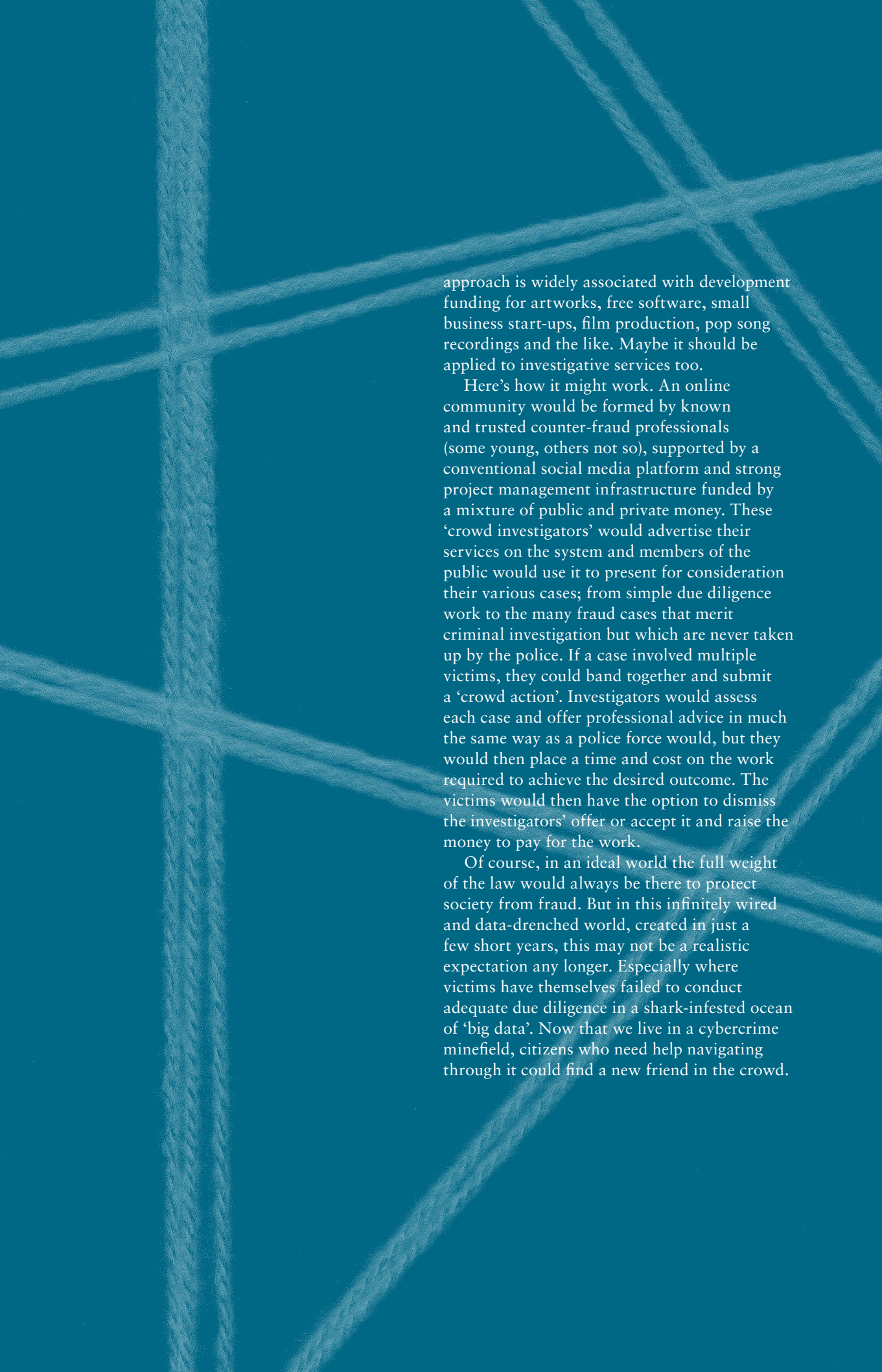
sufficient due diligence checks. IBM estimates that every day we create 2.5 quintillion bytes of data (one quintillion is a billion billion, with 18 zeros); 90% of the data in the world today has been created within the last two years. And third, there is already a shortage of new counter-fraud experts and this shortage will worsen as more and more retire, taking their contacts and expertise with them.

But could relief come in the form of the very mobile computing and social networking technologies that have done so much to open us up to fraud in the first place? And might individual victims exploit that technology by mimicking a funding strategy used successfully for some time now by corporate victims?

During the past decade fraudsters have attacked businesses relentlessly around the globe. In spite of their own formidable IT systems and deep pockets, large firms still recognise that police enforcement and asset recovery skills are essential weapons in their fraud-fighting arsenal. So important, indeed, that when police priorities changed and fraud-focused resources were diverted elsewhere, large organisations began to develop and fund dedicated teams of their own but in partnership with the police.

The Insurance Fraud Enforcement Department (IFED), formed in 2012, is the most recent of these pioneering counter-fraud partnerships. Combining the best investigative talent from the public and private sectors and using state-of-the-art tools, these units do a first-class job for the organisations that fund them. They offer a perfect model for how to marshal exactly the right kind of broadly based expert capability needed to fight an enemy that is not only devious, cruel and innovative but, worst of all, virtually invisible to the untrained eye. Could a similar approach – a method I call 'crowd investigation' – work for individual victims as well?

UK taxpayers rightly expect good police services. But, I believe, many would be prepared to pay a small premium to receive additional services from the police, in the same way as the corporate ratepayers of the City of London and the companies that fund the new IFED. One way to do this would be by crowdfunding. This

The background of the entire page is a solid blue color. Overlaid on this background is a network of thick, light blue ropes. These ropes are woven together to form a complex, three-dimensional mesh or net structure. The ropes intersect at various angles, creating a series of diamond and rectangular openings. The lighting on the ropes gives them a textured, slightly glossy appearance, with highlights and shadows that emphasize their thickness and the way they are intertwined.

approach is widely associated with development funding for artworks, free software, small business start-ups, film production, pop song recordings and the like. Maybe it should be applied to investigative services too.

Here's how it might work. An online community would be formed by known and trusted counter-fraud professionals (some young, others not so), supported by a conventional social media platform and strong project management infrastructure funded by a mixture of public and private money. These 'crowd investigators' would advertise their services on the system and members of the public would use it to present for consideration their various cases; from simple due diligence work to the many fraud cases that merit criminal investigation but which are never taken up by the police. If a case involved multiple victims, they could band together and submit a 'crowd action'. Investigators would assess each case and offer professional advice in much the same way as a police force would, but they would then place a time and cost on the work required to achieve the desired outcome. The victims would then have the option to dismiss the investigators' offer or accept it and raise the money to pay for the work.

Of course, in an ideal world the full weight of the law would always be there to protect society from fraud. But in this infinitely wired and data-drenched world, created in just a few short years, this may not be a realistic expectation any longer. Especially where victims have themselves failed to conduct adequate due diligence in a shark-infested ocean of 'big data'. Now that we live in a cybercrime minefield, citizens who need help navigating through it could find a new friend in the crowd.

ABOUT THE PANEL

The Fraud Advisory Panel is the independent voice and leader of the anti-fraud community in the UK and beyond. Members are drawn from the public, private and voluntary sectors and a variety of professions. By bringing together diverse people and organisations, all with a shared interest and expertise in preventing, detecting, investigating and prosecuting fraud, we seek to make a tangible, practical difference in the fight on fraud.

Established in 1998 through a public-spirited initiative by the Institute of Chartered Accountants in England and Wales (ICAEW), the Panel is now a registered charity and a company limited by guarantee, funded by subscription, donation and sponsorship.

A board of trustee directors governs our activities. The board meets six times a year and is supported by a full-time staff of two.

BOARD OF TRUSTEES



Ros Wright CB QC
Chairman

Complaints commissioner, London Metal Exchange; member of the regulatory board, ACCA. Former director, Serious Fraud Office (1997–2003); past member and chairman of the supervisory committee at OLAF (the European Anti-fraud Office); former non-executive director of both the Insolvency Service steering board and the Office of Fair Trading.



Bill Cleghorn
Deputy chairman

Director, Kinetic Partners LLP (asset management); director, Aver Corporate Advisory Services Ltd (non-asset management), specialising in fraud and financial crime investigation and corporate recovery across all sectors; fellow, Association of Business Recovery Professionals; lecturer on fraud-related matters and money laundering.



Felicity Banks

Head of business law, ICAEW, with lead responsibility for representational work on legal and regulatory issues for professional accountants and specialising in economic crime; represents the profession on the UK government's money laundering advisory committee and the Financial Action Task Force's private sector consultative forum.



David Clarke

Advisory board member responsible for security assurance and risk, Today Translations; specialist in financial crime strategy, Risk Reward. Former detective chief superintendent who served in the UK, Middle East and Eastern Europe; former member of the UK government's Fraud Review team, responsible for designing and delivering new counter-fraud services including the National Fraud Intelligence Bureau and Lead Force for Fraud.



Neil Griffiths

Partner, reconstruction and insolvency group, Dentons, specialising in contentious and fraud-related cases; former vice-chairman, creditors' rights committee, International Bar Association.



Phillip Hagon QPM

Head of corporate security, Sainsbury's, responsible for company security strategy; former officer, Metropolitan Police Service (retired after 33 years with rank of Commander); awarded the Queen's Police Medal in 2005 for distinguished service; City of London Liveryman; sits on the Court of the Worshipful Company of Security Professionals.



Barbara Hart

Retired chartered accountant; charities manager, ICAEW (2007–2008); finance director, CARE International UK (1998–2001) and Mothers' Union (2001–2007).



Dr Stephen Hill
Chairman, cybercrime working group

Managing director, Snowdrop Consulting Ltd; independent consultant and lecturer specialising in fraud, data protection and e-crime; honorary steering committee member, London Fraud Forum; volunteer, City of London Police Support Volunteer Programme; associate, Association of Certified Fraud Examiners; MLIP and CIIP certified.



Monty Raphael QC
Chairman, fraud investigation and the legal process working group

Special counsel, Peters and Peters, specialising in domestic and international business crime and regulation; the acknowledged 'doyen' of UK fraud lawyers; honorary solicitor, Howard League for Penal Reform; trustee director, Transparency International (UK); visiting professor of law, Kingston University; editor, *Blackstone's Guide to the Bribery Act*; lecturer on fraud-related matters.



Will Kenyon

Partner, forensic services group, PricewaterhouseCoopers LLP; founding head of forensic investigations, PwC Germany (1998–2001); specialist in the prevention, detection and investigation of fraud and financial crime across most industries, private and public sector; involved in investigations and recovery actions in relation to some of the most significant fraud and corruption cases of the last 20 years.



Steven Philippsohn
Chairman, asset recovery working group

Founder and senior partner of city solicitors PCB Litigation LLP, specialising in national and international fraud litigation and asset recovery on behalf of international and domestic financial institutions as well as state and commercial organisations; UK representative member, Fraudnet, the International Chamber of Commerce fraud network.



Patrick Rarden

Head of execution products, State Street Global Markets; special police inspector, economic crime directorate, City of London Police; partnership ambassador for FareShare the UK's largest food charity, having founded the FareShare Late sandwich distribution channel for homeless hostels in London; adjutant, Police Detachment, Honourable Artillery Company.



David Skade

Director, global financial crimes risk management team, Bank of America Merrill Lynch, covering the wealth management teams in the EMEA region. Previous MLRO positions held at corporate and investment banks; broad experience across investigations, operational risk, fraud and banking.

Our special thanks go to Alex Plavsic, who was a trustee director until his retirement in 3 July 2012, and Jeremy Outen, who was an active participant on the board between October and February (Jeremy was due to be elected at our 2013 AGM).



Jeremy Outen

Head of KPMG's fraud team with 21 years' experience in KPMG Forensic. Jeremy has led a series of fraud investigations on behalf of private clients and UK law enforcement agencies. From 1 July he will be director designate of the Economic Crime Command of the National Crime Agency.



Alex Plavsic

Head of forensic services, KPMG; during 20 years at KPMG he has worked on many high-profile cases including *Polly Peck*, *Grupo Torras* and the investigation of Jeffrey Archer in relation to the Simple Truth appeal. In the last four years several of his cases have involved bribery and corruption matters, including presenting to the SEC and SFO.

STAFF AND CONSULTANTS



Mia Campbell

Manager and company secretary



Oliver Stopnitzky

Executive



Martin Robinson

Education and training consultant
 Chairman, fraud prevention and detection working group

CORPORATE MEMBERS

Alico Management Services Ltd	ICAEW
AlixPartners UK LLP	Institute of Chartered Accountants of Scotland
AON Ltd	International Compliance Training
Association of Certified Fraud Examiners	Kennedys
Association of Certified Fraud Examiners UK Chapter	KPMG LLP
Association of Chartered Certified Accountants	Kroll
Aviva plc	Law Society of Scotland
AXA Sun Life	Lawrence Graham LLP
Baker Tilly	Lloyds Banking Group
BDO LLP	Moon Beaver Solicitors
Beever and Struthers	National Audit Office
Chantrey Vellacott DFK LLP	National Fraud Authority
CIFAS – the UK’s Fraud Prevention Service	Northern Ireland Audit Office
Control Risks Group	Pinsent Masons LLP
Corporate Research and Investigations	PKF (UK) LLP*
Crédit Agricole Corporate and Investment Bank London Branch	PricewaterhouseCoopers LLP
Deloitte LLP	Proven (UK) Limited (Good Governance Group)
Dentons UKMEA LLP	Prudential plc
Ernst & Young LLP	R-ISC Investigation and Surveillance
Financial Conduct Authority	Royal & Sun Alliance plc
Griffins	RSM Tenon
Haslocks Forensic Accountants Ltd	Smith & Williamson LLP
HSBC	State Street Bank and Trust Company
Haymarket Management Services Ltd	Transport for London
	UBS AG

*On 28 March 2013 PKF (UK) LLP merged with BDO LLP.

GETTING INVOLVED

Individuals and organisations join the Fraud Advisory Panel because they are concerned about fraud and want to do something about it. They find the Panel's activities to be an excellent way to exchange information and insights and to share best practice. You too can show your commitment to stopping fraudsters in their tracks by becoming involved in our highly respected and influential organisation.

Two categories of membership are available: individual and corporate. Either offers a wealth of opportunities and benefits.

- Networking and building relationships with like-minded professionals.
- Exchanging information and best practice.
- Participating in multidisciplinary members' groups and regional forums.
- Preferential rates for our events (some free of charge).
- Influencing public policy and law reform on fraud.
- Regular updates on the latest anti-fraud developments.
- Access to our members' website and LinkedIn group.
- Working in the public interest to address the concerns of business, the professions and the general public.

CORPORATE MEMBERS

Corporate members have up to 20 named employees entitled to all the above benefits and also receive the following additional benefits:

- preferential rates for our events for all employees
- public acknowledgement and company logo on our website
- use of a special 'corporate member' logo on company stationery and websites
- a free professional training session on a fraud-related subject of choice.

All members are required to comply with a code of conduct.

**Join today by calling 020 7920 8637
or email membership@fraudadvisorypanel.org**

THANK YOU

THE FRAUD ADVISORY PANEL WOULD LIKE TO THANK EVERY INDIVIDUAL AND ORGANISATION WHO ASSISTED OUR WORK DURING THE YEAR WHETHER BY VOLUNTEERING TIME AND EXPERTISE, PROVIDING VENUES AND REFRESHMENTS, OR BOTH:

Roy Albutt
Peter Alvey
Professor Jean-Bernard Auby
George Barbary
Barbara Bolton
Clive Bonny
Jane Bewsey QC
Keith Bristow QPM
Louise Brittain
Allison Broad
John Burbidge-King
Robert Burns
John Bush
Joby Carpenter
Penny Cassell
Arun Chauhan
Will Christopher
David Clarke
Allison Clare
Hilary Clarkson
Rod Clayton
Bill Cleghorn
Todd Clements
Chris Cockell
Frances Coulson
Helen Dagley
William Dinan
Alan Doig
Tim Dowdeswell
Anthony Farries
Philippa Foster Back
John Fowler
Jonathan Frost
Andy Fyfe
Laura Gillespie
Sterl Greenhalgh
Phillip Hagon QPM
Matt Hall
Barbara Hart
Tim Harvey
Clive Haslock

Helen Hatton
Jon Hayton
Tony Hetherington
Stephen Hill
Grenville Hodge
David Kearns
Mark Kinsella
Neville Kyrke-Smith
Timothy Lee
Andy Lewis
Kay Linnell
Monica Macovei
Hodge Malek QC
David McCluskey
Kate McMahon
Zimba Moore
Tim Moss
James Nieto
Edward Nkune
David Pester
Steven Philippssohn
Andrew Price
David Prior
David Reynolds
Monty Raphael QC
Elizabeth Rhodes
Martin Robinson
Ryan Rubin
Tom Russell
Nicholas Ryder
Katy Shrimplin
David Springer
Tom Stocker
Perry Stokes
Neill Thomson
Carl Watson
Andrew Webster
Brendan Weekes
Bill White
Simone White
Rik Workman

Charities Internal Audit
Network
DWF LLP
ICAEW
Institute of Advanced Legal
Studies
PKF (UK) LLP
Newcastle University
North East Fraud Forum
Pinsent Masons LLP
Smith & Williamson LLP

Special thanks must also go to the fraud victims and professionals in the public and private sectors who participated in our civil justice project.

Fraud Advisory Panel

Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA
020 7920 8721
info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Registered Charity No. 1108863
Company Limited by Guarantee Registered
in England and Wales No. 04327390

© Fraud Advisory Panel 2013

